9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Challenges and strategies for tackling NP-hard problems

Mahdi Imanparast[1]
Department of Computer Science, University of Bojnord, Bojnord, Iran

Abstract

The classification of a problem as NP-hard comes from its inherent complexity, structural features, and relationships with other hard problems, which lead to significant computational challenges. Many real-world problems are NP-hard, meaning that as the input size increases, it becomes computationally infeasible to find known exact and efficient solutions to solve them for all cases. Understanding why some problems are NP-hard can inform the methods we adopt to tackle them. It also helps to recognize the limits of what can be efficiently computed and to choose strategies for solving computationally complex problems in practice. In this article, we study the main factors that lead to the hardness of NP-hard problems in the real-world, and the challenges of solving them in computing.

Keywords: NP-hard problems, Computational complexity, Theory of computation.
Mathematics Subject Classification [2010]: 68Q15.

1 Introduction

The theory of computation is a branch of computer science and mathematics that deals with the nature of computation and the capabilities and limitations of computational processes. In the early 20th century, mathematicians such as Kurt Godel and Alan Turing established the foundations of modern computer science with their work on formal systems, computability, and undecidability. Kurt Godel presented his incompleteness theorems, which showed the limitations inherent in formal systems and created the groundwork for later theories of computation. In 1936, Alan Turing introduced the concept of Turing machines, which established fundamental concepts in computation and decision making that led to the discovery of decidable and undecidable problems and became the basis for understanding computation and complexity [1, 2]. In the 1950s and 1960s, researchers began to formalize concepts around the efficiency of algorithms and their complexity. Although an explicit classification of problem hardness was still new, in 1971 Stephen Cook published a groundbreaking paper entitled "The Complexity of Theorem-Proving Procedures" and introduced the concept of NP-complete [3]. He proved that the Boolean satisfiability (SAT) problem is NP-complete and lays the foundation for further exploration about NP problems. He showed that many problems could be converted to the SAT and provided a basis for classifying problems according to their hardness. Richard Karp extended Cook's work in 1972 by identifying 21 NP-complete problems, including traveling salesman problem (TSP), Hamiltonian path, and graph coloring problem and so on [4]. Researchers began to develop different algorithmic techniques to deal with NP-complete problems, including approximation, heuristics, and special case algorithms. The 1980s saw significant advances in approximation algorithms, especially for NP-hard problems. This included developing algorithms for the knapsack problem and scheduling problems. Researchers explored randomized algorithms as a tools to more effectively tackle NP-hard problems. The introduction of Las Vegas and Monte Carlo algorithms allowed possible approaches to find solutions. In this paper, we examine the factors affecting the difficulty of NP-hard problems in real-world, and also study the approaches that can be used to overcome difficult NP-hard problems.

[1] speaker

2 NP, co-NP, NP-complete and NP-hard problems

NP-hardness is usually discussed in the context of decision problems (problems with a yes/no answer), but it can also be applied to optimization problems. Regarding decision problems, we have the following classes. Class P is the set of decision problems that can be solved in polynomial time (or in a finite amount of time). The class NP is the set of decision problems with the property that if the answer is yes and there is a solution to it, then we can verify the yes answer in a polynomial time. The class co-NP is the opposite of NP. If the answer to a problem in co-NP is no, then we can verify the answer in polynomial time. It is clear that every decision problem in P is also in NP because if there is a problem in P, we can verify the yes answer in polynomial time. Similarly, every problem in P is also in co-NP. Hard problems which are often classified as NP-complete or NP-hard, appear in various domains in computer science, mathematics, and real-world applications. From the perspective of the theory of computation, NP-hard (Non-Deterministic Polynomial-time Hard) problems are a class of problems that are at least as difficult as the hardest problems in NP. In other words, NP-hard problems may not necessarily be in NP. This means that they may not have solutions that can be verified quickly (in polynomial time) [5, 6]. As can be seen in Figure 1, there are some differences between NP-complete and NP-hard problems. NP-complete problems are in both NP and NP-hard problems and can be solved by a non-deterministic Turing machine in polynomial time. NP-complete is exclusively a decision problem, but NP-hard is not a decision problem. The Hamiltonian cycle and Boolean SAT are examples of NP-complete problems. On the other hand, an NP-hard problem can be solved if and only if there is an NP-complete problem that can be reduced to this problem in polynomial time. Some classic examples of NP-hard problems are: Satisfiability (SAT), traveling salesman problem (TSP), Hamiltonian cycle, steiner tree, subset sum, maximum independent set, clique and vertex cover.

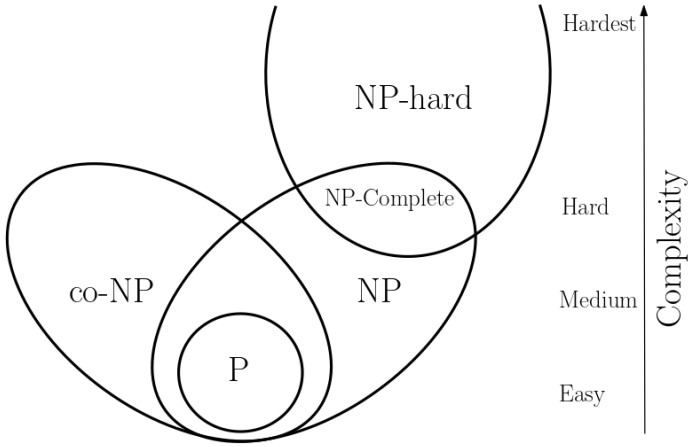


Figure 1: Complexity classes under assumption that P≠NP.

There is no known polynomial time algorithm that solves NP-hard problems in general. If every NP-hard problem can be solved in polynomial time, then all NP-hard problems can also be solved quickly. This is known as the P versus NP (P $\neq$ NP) question, which is one of the most important open problems in theoretical computer science. This meant that is whether the complexity classes P and NP are really different. Intuitively, it seems that P $\neq$ NP, but a more delicate but still open question is whether the complexity classes NP and co-NP are different. In fact, even if we could quickly verify every yes answer, there is no reason to believe that we could also quickly verify every no answer. Hence, it is generally believed that NP $\neq$ co-NP, but no one knows how to prove it. Many natural problems fall into the NP-hard category, meaning they cannot be solved in polynomial time unless P = NP. This inherent hardness makes dealing with them challenging. Exploration of these problems continues by both academic research and applications in real-world, making it an unstable area of research in computer science and mathematics. Many real-world problems and phenomena in nature lead to very difficult problems, especially those involving complexity, uncertainty, and combinatorial structures. Table 1 lists some key real-world categories in which NP-hard

problems arise.

Table 1: Some real-world categories where NP-hard problems arise.

Category	Examples
Combinatorial optimization	traveling salesman problem (TSP), knapsack problem
Graph theory	graph coloring, Hamiltonian cycle, Steiner tree
Scheduling	task scheduling, resource allocation, bandwidth allocation
Decision and search	satisfiability (SAT), subset sum problem
Machine learning and data mining	clustering, feature selection
Network design	routing problems, telecommunication networks, social network
Bioinformatics	sequence alignment, protein folding and structure prediction
Cryptography	integer factorization, discrete logarithm problem
Operations research	facility location, inventory management
Logistics and transportation	vehicle routing, supply chain management
Planning	project management, air traffic control
Ecology and environmental science	species distribution modeling, resource management
Artificial intelligence	game theory, constraint satisfaction problems (CSP)
Manufacturing and production	flexible production systems, quality control
Scientific research and simulation	climate modeling, quantum physics

3 Factors affecting on hardness of real-world problems

Many natural problems are classified as NP-hard problems due to the combination of factors that contribute to the complexity and difficulty of finding optimal solutions. Here is an overview of the primary factors that make these problems particularly challenging:

Exponential growth

Many NP-hard problems involve searching a large space of potential solutions. The larger and more complex space of the problem, makes it more difficult to find the optimal solutions. For example, in combinatorial problems, the number of possible combinations can grow exponentially with the size of the input, leading to computational challenges. Many real-world problems, such as scheduling, routing, and resource allocation, are combinatorial in nature. Problems that require evaluating all permutations or combinations of a set, and selecting subsets from larger sets (such as TSP) often cannot be solved exactly by increasing the input size, because as the input size increases, the number of possible combinations and permutations can increase exponentially.

Interdependence between variables

Many NP-hard problems involve interdependent variables or components. Natural systems (e.g. ecosystems, weather patterns) and social systems (e.g. economy, traffic flow) are usually complex and involve many interacting variables. In these cases, several interdependent variables can create a situation where changing one variable affects others, leading to a complex network of interactions that complicates the search for a solution. It does because changes in one part of the problem can affect many others. The interdependence between these variables can create non-linear behaviors that make them difficult to predict and analyze, and finding solutions is significantly more complicated than linear relationship scenarios.

Incompleteness of information and uncertainty

Real-world problems often involve incomplete or uncertain information. On the other hand, many problems are uncertain and stochastic in nature, whether due to unpredictable human behavior, environmental factors, or incomplete data. Issues that involve uncertainty or variability (e.g., unpredictable demand in supply chain management) can complicate solution strategies and increase difficulty, which complicates the decision-making process. In fields such as medicine, diagnostic processes may involve incomplete patient data, making it difficult to determine the best treatment plan. In cancer treatment, the variability in individual patient responses to treatment, along with the complexity of cancer biology, makes finding universally effective treatments challenging. On the other hand, real-world scenarios are usually dynamic, meaning that conditions change over time. Issues that involve changing conditions create additional layers of complexity.

For example, in weather forecasting, while we can create models to predict the weather, the chaotic nature of the atmosphere makes it impossible to predict the future with perfect accuracy.

Human factors

Human decision-making may not always follow logical patterns and introduce variability and uncertainty into models. People may resist change due to fear of the unknown, loss of control, or disruption of fixed routines. Issues such as public opinions, beneficiaries' benefits, and ethical considerations can influence policy decisions and make them more difficult to navigate. Social and behavioral aspects can complicate problem solving in real-world scenarios. In fields such as economics or social sciences, human behavior can be unpredictable, adding layers of complexity and random elements to modeling and prediction. Beneficiaries may have conflicting interests. For example, policy decisions often require balancing economic growth, social equity, and environmental sustainability. Social, cultural, and institutional inertia can prevent the implementation of new solutions, even if they are theoretically sound.

Complex relationships and constraints

The NP-hard problems often have complex relationships between elements that must be satisfied simultaneously. This complexity can significantly increase the solution space and the difficulty of finding the optimal solution. Many NP-hard problems require finding optimal solutions under severe constraints, leading to a very complex landscape of feasible solutions. The interaction of these constraints makes it harder to find solutions that work under all conditions. Problems are often associated with various hard and soft constraints (such as capacity and time constraints) that can complicate the search space for practical solutions. In some cases, the constraints change in time (e.g., traffic conditions), which requires adaptive solutions that are difficult to calculate. In systems with feedback loops, small changes can have large effects due to the interconnected nature of the components.

High dimensions

High-dimensional data spaces complicate optimization and search algorithms. They lead to the "*Curse of Dimensionality*", where the volume of the space increases rapidly as data points become more sparse, making it difficult to find patterns or effectively optimize functions. In machine learning, model tuning parameters often involves traversing high-dimensional spaces, which makes finding optimal settings challenging. Optimizing parameters in high-dimensional models (such as machine learning algorithms) involves searching large spaces, which complicates the optimization process.

Absence of efficient algorithms

For many NP-hard problems, no known efficient (or polynomial time) algorithm can efficiently solve all instances of the problem, while some special cases may have efficient solutions. While the problem may be solvable in a reasonable time, the general case remains unsolved.

Multiple objectives and constraints

Real-world problems often include multiple objectives and constraints, such as balancing cost, time, and quality in project management, which may conflict with each other, making it difficult to find a satisfactory solution and increasing the complexity.

Limitation of resources

Some problems may be theoretically solvable but are impractical due to constraints such as time, money or technology. For example, while algorithms exist to optimize traffic flow, in real-world applications it is often face limitations due to infrastructure, public behavior, and environmental factors.

4 Strategies to overcome of NP-hard problems

While some problems may be theoretically intractable in the conventional sense (e.g., NP-hard problems), several approaches and strategies can lead to practical solutions or improvements. As research advances and technology evolves, several key perspectives can be presented to overcome the limitations of NP-hard problems. The following are some important strategies for overcoming the NP-hard problems. A summary of these strategies is given in Table 2.

Advances in algorithms

The study of approximation algorithms emerged as a practical approach to dealing with NP-hard problems. For many NP-hard problems, researchers have developed approximation algorithms that can provide

Table 2: Some strategies to overcome NP-hard problems.

Strategy	Description	Potential Applications	Advantages
Advances in Algorithms	Development of approximation, randomized, and heuristic algorithms for near-optimal solutions.	Logistics, resource management	Reduces computation time, practical solutions
Distributed and Parallel Computing	Utilizing multi-core processors and cloud computing for extensive simulations and computations.	Large-scale optimization problems, data analysis	Faster processing through simultaneous task execution
Fixed Parameter Tractability (FPT)	Focus on specific parameters for efficient algorithm design in NP-hard contexts.	Network design, scheduling	Efficient for larger instances with fixed parameters
Potential of Quantum Computing	Using quantum algorithms for faster resolution of certain NP-hard problems.	Cryptography, complex optimization	Possible speedups over classical computing methods
Machine Learning and AI	Using models that learn from data to optimize decisions without explicit problem solving.	Logistic, robotics, game development	Adaptable solutions, real-time optimization
Interdisciplinary Approaches	Collaboration across various fields to develop innovative solutions for complex problems.	Climate modeling, healthcare, transportation	Diverse perspectives lead to holistic solutions

near-optimal solutions within the guaranteed range of the optimal solution. These algorithms can significantly reduce the computation time. These developments enhance decision-making in various fields, from logistics to resource management. The introduction of randomized algorithms allowed researchers to tackle NP-hard problems using probability. Techniques such as Monte Carlo algorithms provide methods for finding approximate solutions more quickly. Heuristic algorithms use practical techniques based on experience and trial to explore large solution spaces effectively. They can often find solutions that are good enough in a reasonable time. Special algorithmic approaches like genetic algorithms, simulated annealing, particle swarm optimization, and tabu search can be especially effective for combinatorial optimization problems.

Advances in distributed and parallel computing

Continued growth in processing power, including advances in multi-core processors, GPUs, and specialized hardware, enables more extensive computations and simulations that can help effectively solve NP-hard problems. Cloud computing and distributed systems can use massive computing resources to tackle large-scale NP-hard problems and enable parallel processing that may enable exhaustive search in some scenarios. Parallel computing allows problems to be broken down into smaller tasks that can be solved simultaneously. This can dramatically decrease the computation time for some NP-hard problems and offers new opportunities for handling complex computations.

The ability of fixed parameter tractability (FPT)

In the theory of algorithms, fixed parameter tractability (FPT) is a concept used in the study of computational complexity, particularly in relation to problems that can be solved efficiently when certain parameters are fixed. FPT provides a powerful toolkit for addressing complex problems by allowing researchers to focus on specific parameters of interest, enabling efficient algorithms even in the face of NP-hardness for larger instances.

The potential of quantum computing

Advances in quantum computing have created new perspectives on NP-hard problems. Quantum computers have the potential to solve some NP-hard problems more efficiently than classical computers. Quantum algorithms, such as Grover's search algorithm, offer potential speedups for certain types of problems and provide interest in exploring NP-completeness concepts [7]. As quantum technology matures, we may see practical applications where quantum computing addresses previously intractable problems.

Use of capabilities machine learning and artificial intelligence

Advances in machine learning make it possible to develop models that can learn from data and make predictions or decisions without explicitly solving the underlying problem. Machine learning can facilitate the

development of models that learn from data patterns to optimize solutions for complex problems, potentially changing the way we approach NP-hard problems, especially in areas such as logistics and network design. Research continues on the application of deep learning methods to combinatorial optimization problems using neural networks, which can yield new insights and faster solutions. Artificial intelligence can also adapt to complex environments and dynamically optimize processes. This technique is promising in finding solutions to problems such as gaming and robotic navigation, where traditional optimization methods may have difficulty.

Interdisciplinary approaches

The complexities of NP-hard problems often require interdisciplinary collaboration, integrating insights from mathematics, computer science, operations research, and fields such as biology or economics to develop innovative solutions. As industries face increasing complexity, applying computational theory and techniques to real-world problems (such as climate modeling, transportation, and health-care) becomes critical and creates a partnership between theoretical developments and practical implementation. Collaboration across disciplines can lead to innovative solutions. Insights from fields such as biology, sociology, economics, and engineering can provide strategies for tackling complex problems.

5 Conclusions

The fundamental challenges that make some real-world problems difficult to solve or implement quickly are rooted in issues including complexity, uncertainty, human factors, resource limitations, and dynamic interactions in systems. The future prospects of computing in the face of NP-hard problems are promising yet complex. While some hard problems remain challenging and may not have precise and efficient solutions, ongoing research, technological advances, and innovative methods offer hope for notable progress. While significant challenges remain, advances in technology, algorithms, and interdisciplinary collaborations are paving the way for new solutions. Using a combination of approximation, heuristics, artificial intelligence, advanced computing power, cloud computing, quantum computing, and interdisciplinary collaboration, helps to effectively solve complex real-world problems and achieve meaningful results even when traditional approaches fail to find significant results. However, many problems in the real-world either cannot be solved due to limitations, or do not have efficient algorithms.

References

[1] M. Davis, R. Sigal, E. J. Weyuker, *Computability, complexity, and languages: fundamentals of theoretical computer science*, 2nd edition, Morgan Kaufmann, (1994).

[2] S. B. Cooper, *Computability Theory*, 1st edition, Chapman Hall/ CRC, (2003).

[3] S. Cook, *The Complexity of Theorem Proving Procedures*. In Proceeding of the 3rd Annual ACM Symposium on Theory of Computing (STOC), (1971), pp. 151-158.

[4] R. M. Karp, *Reducibility Among Combinatorial Problems*, In Proceeding of a Symposium on the Complexity of Computer Computations, (1972), pp. 85-103.

[5] J. E. Hopcroft, R. Motwani, J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, 3rd edition, Pearson, (2006).

[6] M. Sipser, *Introduction to the Theory of Computation*, 3rd edition, Cengage Learning, (2012).

[7] M. Imanparast, *The prospect of cryptography and computing with quantum computers*, In Proceeding of the 8th International Conference on Combinatorics, Cryptography, Computer Science and Computation, (2023), pp. 379-384.

Email: m.imanparast@ub.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

A new heuristic algorithm for the unit disk cover problem

Mahdi Imanparast[1]
Department of Computer Science, University of Bojnord, Bojnord, Iran

Abstract

This paper introduces a new heuristic algorithm for the unit disk cover (UDC) problem, which is an NP-hard problem. The UDC problem involves determining the minimum number of unit disks required to cover a given set of n points on the plane. The proposed heuristic algorithm combines the point rounding techniques and the Delaunay triangulation for solving the unit disk covering problem and has an $\mathcal{O}(n \log n)$ expected time and a memory complexity $\mathcal{O}(n)$, when n is the number of input points.

Keywords: Computational geometry, NP-hard problem, Unit disk cover problem, Heuristic algorithms.

Mathematics Subject Classification [2010]: 68W25, 68W40.

1 Introduction

The unit disk cover (UDC) problem is a classic problem in computational geometry and combinatorial optimization. It involves determining the minimum number of unit disks needed to cover a given set of points in the plane. The problem of covering points with geometric shapes dates back to early work in optimization and computational geometry in the 1970s and 1980s. Researchers were interested in efficient algorithms for various geometric covering problems, including those involving circles, squares, and other shapes. The UDC problem was formally introduced in the context of computational geometry, primarily influenced by applications in wireless communication, sensor networks, and geographic information systems. The problem quickly gained attention due to its connection to NP-hardness; it was established that finding the minimum number of unit disks needed to cover all points is NP-hard, making it computationally challenging [1]. Researchers focused on developing polynomial-time algorithms that could yield near-optimal solutions. Greedy approaches and local search techniques emerged as popular strategies for tackling the problem effectively in practice, despite the theoretical difficulty. Various heuristic and approximation algorithms have been proposed in the literature [2, 3, 4]. The UDC problem has important applications in network design, particularly in the deployment of sensor networks where coverage and connectivity are crucial. This gave rise to further interest in variations of the problem, such as the minimum connected dominating set problem and the maximum coverage problem, further expanding the research landscape. The UDC problem also remains relevant in various fields including robotics, environmental monitoring, and urban planning. Its principles are applied in real-world scenarios where coverage, efficiency, and resource allocation are critical. In this paper, we present a new heuristic algorithm for the UDC problem that combines the point rounding technique and Delaunay triangulation to achieve good results for this problem.

[1] speaker

2 The proposed heuristics algorithm

In this subsection, we propose a new heuristic algorithm for solving the UDC problem. The details of the algorithm are as follows.

Algorithm 1: A HEURISTIC FOR UNIT DISK COVER

Input: a point set $\mathcal{P}$ of n points in the plane.

Output: a solution for the UDC problem.

1: Define a regular square grid with side length $\sqrt{2}$ on the points;
2: Round the points to the center points of the grid cells;
3: Determine the center points of the circles that cover the points and store them in a list $\mathcal{L}$;
4: Create a Delaunay triangulation for the points stored in $\mathcal{L}$;
5: Find the center points of each triangle in the Delaunay triangulation and add them to the list $\mathcal{L}$;
6: **while** $(\mathcal{P} \neq \phi)$
7: **begin**
8: Find a circle $\mathcal{C} \in \mathcal{L}$ that covers the maximum number of points of $\mathcal{P}$;
9: Put points in $\mathcal{C}$ in the set $\mathcal{P}_{\mathcal{C}}$;
10: Put circle $\mathcal{C}$ in the solution list $\mathcal{S}$;
11: Set $\mathcal{P} = \mathcal{P} - \mathcal{P}_{\mathcal{C}}$;
12: **end of while**
13: Output $\mathcal{S}$;

To better understand the algorithm process, we present the steps of its implementation in an example. Figure 1 shows a set of points and a grid with side length $\sqrt{2}$ defined on it. After rounding, we find circles which cover points.

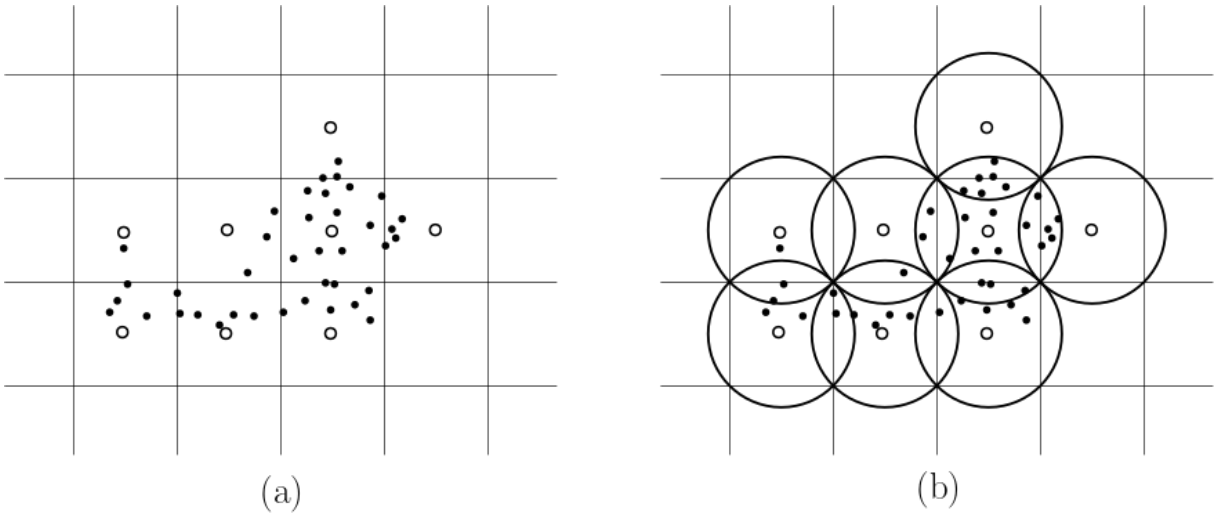


Figure 1: (a) Rounding points to the center of the grid cells (b) Determining the circles that cover the points.

After this step, for the rounded points, we create a Delaunay triangulation of the centers of the circles in the list $\mathcal{L}$ and calculate the centers of the triangles and add them to the list of circles in the circle candidate list $\mathcal{L}$ (see Figure 2). Finally, by performing the iterative process from steps 7 to 12, we can find the set of solution circles as shown in Figure 3.

3 Runtime Analysis

In this section, we analyze the execution time of the proposed algorithm. Define a regular square grid with side length $\sqrt{2}$ on the points, involves determining a grid based on the given points. If there are n points, creating the grid can be done in $\mathcal{O}(n)$. Rounding each point to the nearest grid center also takes $\mathcal{O}(n)$.

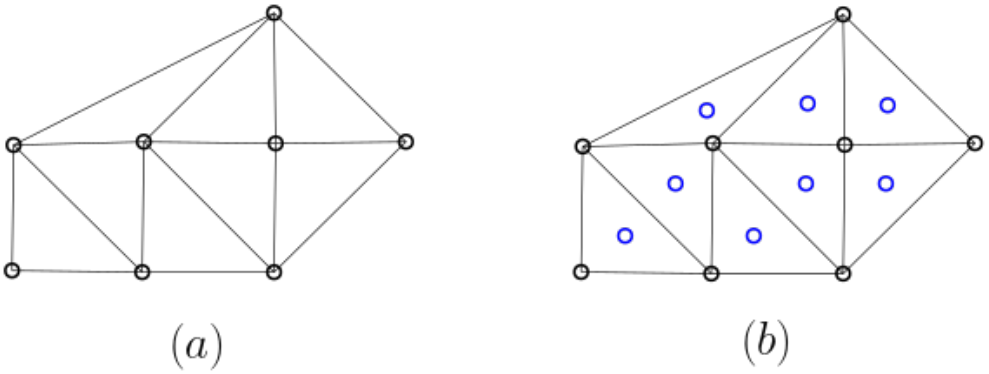


Figure 2: (a) Computing the Delaunay triangulation for the center points of the circles in list $\mathcal{L}$ (b) Finding the center points of each triangle.

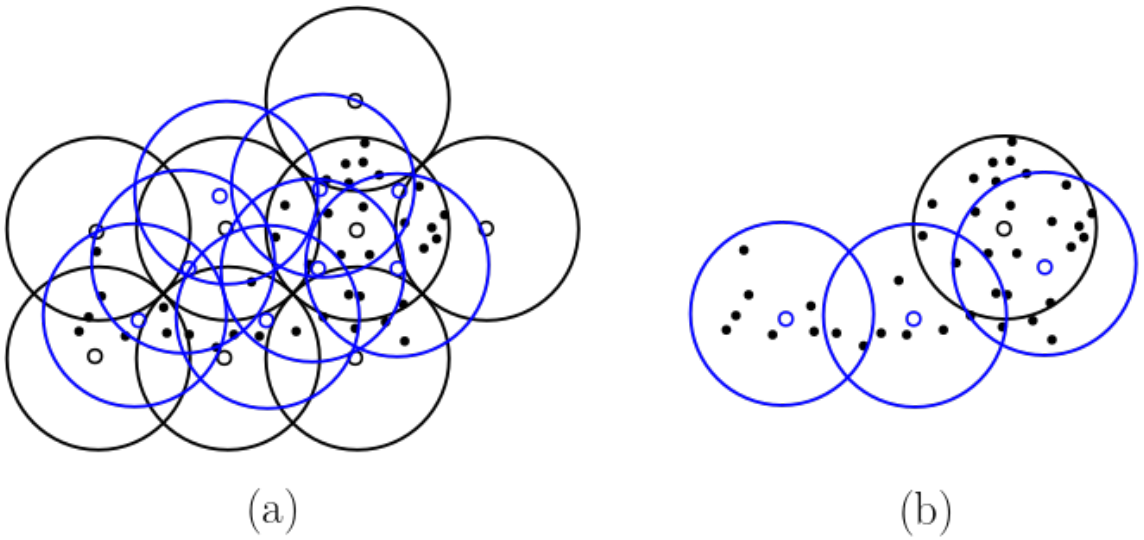


Figure 3: (a) The entire set of circles in list $\mathcal{L}$, including the initial circles and the circles resulting from the centers of triangles within the Delaunay triangulation. (b) The final solution.

Determine the center points of the circles that cover the points and store them in a list $\mathcal{L}$, is likely involves determining an initial set of covering circles based on the rounded points, taking $\mathcal{O}(n.m)$ time, where m is the number of points in $\mathcal{L}$. Constructing a Delaunay triangulation needs to $\mathcal{O}(m \log m)$ expected time, where m is the number of points in $\mathcal{L}$. Extracting the centers of triangles can be done in linear time relative to the number of triangles, which again is dependent on m. Thus, this step can be considered $\mathcal{O}(m)$. Finding the best covering circle involves checking coverage against remaining points. In the worst case, if we check all remaining points for each circle, this could take $\mathcal{O}(n)$ per iteration, potentially leading to $\mathcal{O}(n \cdot k)$, where k is the number of iterations until all points are covered. The number of iterations depends on the distribution of points and how many circles are needed. In the worst case, if each circle covers just a few points, this can lead to $\mathcal{O}(n \cdot k)$. Combining all these steps, the total time complexity is $\mathcal{O}(nm + m \log m + m + nk)$. Since m (the size of list $\mathcal{L}$) and k (the number of iterations) are generally much smaller than n, the time complexity of this heuristic algorithm is $\mathcal{O}(n^2)$ in the worst case.

4 Improving the running time

As mentioned in the previous section, the part that takes the most time in the algorithm is related to calculating the number of points inside the circles for the set of points in the list $\mathcal{L}$, which takes $\mathcal{O}(n)$ time for each circle because we have to check all n points. In order to reduce the execution time, we can use a spatial data structure like a kd-tree. A kd-tree (k-dimensional tree) is a binary tree used for organizing

points in a k-dimensional space. In this case, since we are working in a 2D plane, it will be a 2D kd-tree. In this case, for n points, a kd-tree can be created in $\mathcal{O}(n \log n)$ time and $\mathcal{O}(n)$ space. Then, for each circle $\mathcal{C}_i$, instead of checking all n points, we can use the kd-tree to check only a square with side length 2 and the center of that circle, which takes $\mathcal{O}(\sqrt{n} + k_i)$ time, where k_i is the number of points inside the square corresponding to the circle $\mathcal{C}_i$. So, considering the last steps of the algorithm, it is clear that the sum of k_i's will be n, so the required time for the last steps will be $\mathcal{O}(\sqrt{n} + n) = \mathcal{O}(n)$. So, implementing a spatial data structure like a kd-tree can significantly speed up searching for covered points within potential covering circles. Therefore, taking into account this improvement as well as the average time required to construct the Delaunay triangulation, the overall execution time of the algorithm is $\mathcal{O}(n \log n)$ expected time.

5 Memory Consumption Analysis

The memory usage of the heuristic algorithm for the UDC problem utilizing Delaunay triangulation can be analyzed based on several components involved in the algorithm. We need to store the coordinates of the n points on the plane. This typically requires $\mathcal{O}(n)$ space, as each point is usually represented with its x and y coordinates. The list $\mathcal{L}$ which stores potential circle centers derived from the grid or triangulation will also require memory. In the worst case, this could again be up to $\mathcal{O}(n)$ if every point leads to a different center being added, although practical scenarios might yield fewer. The memory required to store the Delaunay triangulation depends on the number of triangles formed, which is generally around $\mathcal{O}(n)$ for n points. Each triangle consists of three edges and three vertices, so additional space is needed to store this information, leading to extra overhead. Overall, this part still remains linear, i.e., $\mathcal{O}(n)$. If we use kd-tree to optimize point lookup and coverage determination, they also add to the memory. These structures typically require $\mathcal{O}(n)$ space. Therefore, the total memory complexity of the algorithm is $\mathcal{O}(n)$.

6 Conclusion

This paper presented a new heuristic algorithm for the UDC problem that addresses the challenge of determining the minimum number of unit disks needed to cover a set of points in a plane. While the proposed algorithm may not always match the precision of exact methods, its enhancements in speed, scalability, and practical applicability make it a strong candidate for solving the UDC problem effectively, particularly in large-scale applications. Future work could explore further refinements to the algorithm, investigate additional problem variants or extensions.

References

[1] R. J. Fowler, M. S. Paterson, S. L. Tanimoto, *Optimal packing and covering in the plane are NP-complete*, Information Processing Letters, 12(3), (1981), pp. 133–137.

[2] B. Fu, Z. Chen, M. Abdelguerfi, *An almost linear time 2.8334-approximation algorithm for the disc covering problem*, In Proceeding of the 3rd International Conference on Algorithmic Applications in Management (AAIM'07), (2007), pp. 317–326.

[3] A. Biniaz, P. Liu, A. Maheshwari, M. Smid, *Approximation algorithms for the unit disk cover problem in 2D and 3D*, Computational Geometry: Theory and Applications, 60, (2017), pp. 8–18.

[4] M. Imanparast, S. N. Hashemi, *A simple greedy approximation algorithm for the unit disk cover problem*, AUT Journal of Mathematics and Computing, 1(1), (2020), pp. 47–55.

[5] M. de Berg, O. Cheong, M. van Kreveld, M. Overmars, *Computational Geometry: Algorithms and Applications*, Springer Berlin Heidelberg, (2008), pp. 95–115.

Email: m.imanparast@ub.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

On some properties of self-similar action of a group on a k-graph

Ebrahim Tamimi[1]
Velayat University, Iranshahr, Iran

Abstract

In this paper, we study the basic properties of the notion of a self-similar action of a group G on a k-graph. Also, by considering a self-similar k-graph over a certain group, we prove some hereditary properties through of so called restriction mapping on k-graph.

Keywords: Self-similar action, k-graph, G-hereditary, G-strongly connected, restriction map

AMS Mathematical Subject Classification [2010]: 46L05

1 Introduction

Let G be a discrete (countable) group, and (E, r, s) be a finite directed graph with no sources. In [3], Exel-Pardo introduced a notion of a selfsimilar action of G on E, which naturally generalizes the notion of selfsimilar groups (see, e.g., [5]). For investigate and to study a certain C^*-algebra, Exel-Pardo in [3] associated the self-similar action (G, E) an inverse semigroup $S_{G,E}$.

In this paper, we study the properties of the notion of a self-similar action of a group G on a k-graph. We know that for higher-dimensional cases, in general the construction of the inverse semigroup $S_{G,E}$ in [3] mentioned above does not apply, and so unlike [3] one can not apply the machinery in [1, 2].

2 Main results

Definition 2.1. Let Λ be a k-graph, and G be a group acting on Λ. Then the action is said to be self-similar if there exists a restriction map $G \times \Lambda \to G$, $(g, \mu) \mapsto g\,|_\mu$, such that

(i) $g.(\mu\nu) = (g.\mu)(g\,|_\mu\,.\nu)$ for all $g \in G, \mu, \nu \in \Lambda$ with $s(\mu) = r(\nu)$.

(ii) $g\,|_\nu = g$ for all $g \in G$, $\nu \in \Lambda^0$;

(iii) $g\,|_{\mu\nu} = g\,|_\mu\,|_\nu$ for all $g \in G, \mu, \nu \in \Lambda$ with $s(\mu) = r(\nu)$;

(iv) $1_G\,|_\mu = 1_G$ for all $\mu \in \Lambda$;

(v) $(gh)\,|_\mu = g\,|_{h.\mu}\,h\,|_\mu$ for all $g, h \in G$, $\mu \in \Lambda$.

Moreover, Λ and G are called a self-similar k-graph over G and self-similar group on Λ, respectively [4].

[1] speaker

Definition 2.2. Let Λ be a self-similar k-graph over a group G, and H be a subset of Λ^0. Then H is said to be G-hereditary if $s(H\Lambda) \subseteq H$ and $G.H \subseteq H$. Notice that H is hereditary in the usual sense, and that it naturally induces a self-similar action of G on $H\Lambda$ [4].

Definition 2.3. Let Λ be a self-similar k-graph over a group G. Then Λ is said to be G-strongly connected if $(G.\nu)\Lambda\omega \neq \varnothing$ for all $\nu, \omega \in \Lambda^0$.

Clearly, if Λ is strongly connected, then it is G-strongly connected [4].

Theorem 2.4. *Let Λ be a self-similar k-graph over a group G. Then*

(i) $(g+g') \mid_\mu .s(\nu) = (g+g').s(\nu)$ *for all* $g, g' \in G$, $\mu, \nu \in \Lambda$ *with* $s(\mu) = r(\nu)$;

(ii) $(g+g') \mid_\mu .s(\mu) = (g+g').s(\mu)$ *for all* $\mu \in \Lambda$;

(iii) $((g+g') \mid_\mu)^{-1} = (g+g')^{-1} \mid_{(g+g').\mu}$ *for all* $g, g' \in G, \mu \in \Lambda$.

Proof. (i) By hypothesis we have

$$\begin{aligned}(g+g').s(\nu) &= (g+g').s(\mu\nu)\\ &= s((g+g').(\mu\nu))\\ &= s((g+g') \mid_\mu .\nu)\\ &= (g+g') \mid_\mu .s(\nu).\end{aligned}$$

(ii) This is a special case of (i).

(iii) We obtain

$$\begin{aligned}((g+g') \mid_\mu)((g+g')^{-1} \mid_{(g+g').\mu}) &= ((g+g')(g+g')^{-1}) \mid_{(g+g').\mu}\\ &= 1_G = ((g+g')^{-1}(g+g')) \mid_\mu\\ &= ((g+g')^{-1} \mid_{(g+g').\mu})((g+g') \mid_\mu).\end{aligned}$$

□

Let Λ be a k-graph. Set $\Lambda^e := \Lambda^{e_1} \cup \Lambda^{e_2} \cup \cdots \cup \Lambda^{e_k}$. By the next theorem we extend an action of G on $\Lambda^0 \bigcup \Lambda^e$ with a restriction to a self-similar action of G on Λ.

Theorem 2.5. *Let Λ be a k-graph, and G be a group. Suppose that G acts on the set $\Lambda^0 \bigcup \Lambda^e$, and that there is a restriction map $G \times (\Lambda^0 \bigcup \Lambda^e) \to G$, $(g, x) \mapsto g \mid_x$, satisfying the following properties:*

(i) $G.\Lambda^n \subseteq \Lambda^n$ *for all* $n \in \{0, e_i : 1 \leq i \leq k\}$;

(ii) $s((g+g').\mu) = (g+g').s(\mu)$ *and* $r((g+g').\mu) = (g+g').r(\mu)$ *for all* $g, g' \in G, \mu \in \Lambda^e$;

(iii) $(g+g') \mid_\mu .s(\nu) = (g+g').s(\nu)$ *for all* $g, g' \in G, \mu \in \Lambda^e, \nu \in \Lambda$ *with* $s(\mu) = r(\nu)$;

(iv) $((g+g').\mu)((g+g') \mid_\mu .\nu) = ((g+g').\alpha)((g+g') \mid_\alpha .\beta)$ *for all* $g, g' \in G, \mu, \nu, \alpha, \beta \in \Lambda^e$ *with* $\mu = \alpha\beta$;

(v) $(g+g') \mid_\nu = (g+g')$ *for all* $g, g' \in G, \nu \in \Lambda^0$;

(vi) $(g+g') \mid_\mu \mid_\nu = (g+g') \mid_\alpha \mid_\beta$ *for all* $g, g' \in G$, $\mu, \nu, \alpha, \beta \in \Lambda^e$ *with* $\mu\nu = \alpha\beta$;

(vii) $((g+g')h) \mid_\mu = ((g+g') \mid_{h.\mu})(h \mid_\mu)$ *for all* $g, g', h \in G, \mu \in \Lambda^e$.

Then there exists a unique self-similar action of G on Λ with the restriction map $|$ from $G \times \Lambda$ into G extending the given action and the given map $|$.

Proof. Let $\mu \in \Lambda$ with $|\mu| = 2$. We set $\mu = \mu_1\mu_2$ with $\mu_1, \mu_2 \in \Lambda^e$. For $g, g' \in G$, set

$$(g + g').\mu := ((g + g').\mu_1)((g + g') \mid_{\mu_1} .\mu_2)$$

and

$$(g + g') \mid_{\mu} := (g + g') \mid_{\mu_1} \mid_{\mu_2}.$$

We can see that both $(g + g').\mu$ and $(g + g') \mid_{\mu}$ are well-defined. Inductively, we extend the given action and restriction to Λ. One can see that they satisfy Definition 2.1 $(i) - (v)$ are satisfied. Thus the extensions follows a self-similar action of G on Λ. □

Remark 2.6. Let Λ be a self-similar k-graph over a group G. For $g, g' \in G$ and $x \in \Lambda^\infty$, we define

$$((g + g').x)(p, q) := (g + g') \mid_{x(0,p)} .x(p, q) \qquad forall \qquad (p, q) \in \Omega_k,$$

and

$$(g + g') \mid_x (p) := (g + g') \mid_{x(0,p)} \qquad forall \qquad p \in \mathbb{N}^k.$$

Then $(g + g').x \in \Lambda^\infty$ and $(g + g') \mid_x$ is a function from $\mathbb{N}^k$ to G.

By the following proposition we give some basic properties of $(g + g').x$ and $(g + g') \mid_x$.

Proposition 2.7. *Let Λ be a self-similar k-graph over a group G. The following statements are hold*

(i) for $g, g' \in G$, the map $\Lambda^\infty \to \Lambda^\infty$, $x \to (g + g').x$ is a homeomorphism;

(ii) $\sigma^p((g + g').x) = (g + g') \mid_{x(0,p)} .\sigma^p(x)$ for all $g, g' \in G$, $p \in \mathbb{N}^k$ and $x \in \Lambda^\infty$;

(iii) $(g + g').(\mu x) = ((g + g').\mu)((g + g') \mid_\mu .x)$ for all $g, g' \in G$, $\mu \in \Lambda$ and $x \in s(\mu)\Lambda^\infty$.

Proof. The proof of (i) is straightforward.

(ii) Suppose that $p \in \mathbb{N}^k$ and $(s, t) \in k$, repeatedly using Definition 2.1 (5) follows that

$$\begin{aligned}
\sigma^p((g + g').x)(s, t) &= ((g + g').x)(s + p, t + p) \\
&= (g + g') \mid_{x(0,s+p)} .x(s + p, t + p) \\
&= (g + g') \mid_{x(0,s+p)} .\sigma^p(x)(s, t) \\
&= (g + g') \mid_{x(0,p)} |\sigma^p(x)(0, s).\sigma^p(x)(s, t) \\
&= ((g + g') \mid_{x(0,p)} .\sigma^p(x))(s, t).
\end{aligned}$$

The proof of (iii) is straightforward. □

Acknowledgment

The author express their deep thanks for the comments.

References

[1] R. Exel, *Inverse semigroups and combinatorial C^*-algebras*, Bull. Braz. Math. Soc. (N.S.) 39 (2008), 191–313.

[2] R. Exel and E. Pardo, *The tight groupoid of an inverse semigroup*, Semigroup Forum 92 (2016), 274–303.

[3] R. Exel and E. Pardo, *Self-similar graphs, a unified treatment of Katsura and Nekrashevych C^*-algebras*, Adv. Math. 306 (2017), 1046–1129.

[4] H. Li and D. Yang, *Self-similar k-graph C^*-algebras*, International Mathematics Research Notices. 15 (2021), 11270–11305.

[5] V. Nekrashevych, *Self-similar groups*, American Mathematical Society, Providence, RI, 2005, xii+231.

e-mail: e.tamimi@velayat.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Flag-transitive block designs and almost simple groups

Mohsen Bayat[1], Nasrin Soltankhah
Department of Mathematics, Faculty of Mathematical Science, Alzahra University, Tehran, Iran

Abstract

The main aim of this talk is to present some recent studies on nontrivial block designs admitting a flag-transitive and point-primitive automorphism group G.

Keywords: Flag-transitive, point-primitive, block design, almost simple group.

Mathematics Subject Classification [2010]: 05B05, 05B25, 20B25

1 Introduction

A block design $\mathcal{D}$ is a pair $(\mathcal{P}, \mathcal{B})$ with a set $\mathcal{P}$ of v points and a set $\mathcal{B}$ of blocks such that each block is a k-subset of $\mathcal{P}$ and each two distinct points are contained in λ blocks. We say $\mathcal{D}$ is nontrivial if $2 < k < v - 1$, and symmetric if $v = b$, where b is the number of blocks of $\mathcal{D}$. Each point of $\mathcal{D}$ is contained in exactly $r = bk/v$ blocks which is called the *replication number* of $\mathcal{D}$. The *complement* of a block design $\mathcal{D}$ is a block design with parameters set $(v, b, b - r, v - k, b - 2r + \lambda)$ whose set of points is the same as the set of points of $\mathcal{D}$ and whose blocks are the complements of the blocks of $\mathcal{D}$, that is, incidence is replaced by non-incidence and vice versa. An *automorphism* of a symmetric design $\mathcal{D}$ is a permutation of the points permuting the blocks and preserving the incidence relation. The full automorphism group $Aut(\mathcal{D})$ of $\mathcal{D}$ is the group consisting of all automorphisms of $\mathcal{D}$. A *flag* of $\mathcal{D}$ is a point-block pair (α, B) such that $\alpha \in B$. For $G \leqslant Aut(\mathcal{D})$, G is called *flag-transitive* if G acts transitively on the set of flags. The group G is said to be *point-primitive* if G acts primitively on $\mathcal{P}$. A group G is said to be *almost simple* with socle X if $X \trianglelefteq G \leqslant Aut(X)$, where X is a nonabelian simple group. We adopt the standard notation as in [2, 3] when we deal with almost simple groups with socle finite classical simple groups. We here write A_n and S_n for the alternating group and the symmetric group on n letters, respectively, and we write "n" for a group of order n. By Aschbacher's theorem [1], the maximal subgroups of finite classical groups belong to one of the eight geometric $\mathcal{C}_i$ families $(i = 1, \ldots, 8)$ or a $\mathcal{S}$ family containing almost simple groups satisfying some irreducibility conditions. In this paper, we follow the same terminology as in [4] and if H belongs to the family $\mathcal{C}_j$, for some j, then we sometimes say that H is a $\mathcal{C}_j$-subgroup. Moreover, we use the symbol $\hat{}H$ for the structure of the pre-image of H in the corresponding linear group. Further notation and definitions in both design theory and group theory are standard and can be found, for example, in [2, 4, 5]. We use GAP [6] for computational arguments.

[1]speaker

Flag-transitivity is one of the most interested condition that can be imposed on the automorphism group G of a block design $\mathcal{D}$. It is well-known that flag-transitive designs are also point-transitive and block-transitive. However, transitivity on flags does not necessarily imply primitivity on points. In fact, except for linear spaces, flag-transitive designs may possess imprimitive automorphism groups, and we know that there are only finitely many block designs with a flag-transitive and point-imprimitive automorphism group [7]. Moreover, Delandtsheer and Doyen [8] showed that the examples of flag-transitive and point-imprimitive block designs are somewhat exceptional, that is to say, most flag-transitive designs are point-primitive. By these reasons, we are interest to studying flag-transitive and point-primitive block designs.

Table 1: Some flag-transitive and point primitive block design $\mathcal{D}$.

Line	v	b	r	k	λ	G	Class	Ref
1	8	14	7	4	3	$PSL_3(2)$	$\mathcal{C}_3$	[11]
	Base block: { 1, 2, 3, 5 }							
2	8	28	14	4	6	$PSL_3(2):2$	$\mathcal{C}_3$	[15]
	Base block: {1, 2, 3, 5 }							
3	8	28	21	6	15	$PSL_3(2)$, $PSL_3(2):2$, $PSL_4(2)$, $PSL_4(2):2$	$\mathcal{C}_3$	[15]
	Base block: {1, 2, 3, 4, 5, 6 }							
4	8	42	21	4	9	$PSL_3(2)$, $PSL_3(2):2$	$\mathcal{C}_3$	[15]
	Base block: {1, 2, 3, 4 }							
5	8	56	21	3	6	$PSL_3(2)$, $PSL_3(2):2$, $PSL_4(2)$, $PSL_4(2):2$	$\mathcal{C}_3$, $\mathcal{S}$	[15]
	Base block: {1, 2, 3 }							
6	8	56	35	5	20	$PSL_4(2)$, $PSL_4(2):2$	$\mathcal{S}$	[15]
	Base block: {1, 2, 3, 4, 5 }							
7	8	70	35	4	15	$PSL_4(2)$, $PSL_4(2):2$	$\mathcal{S}$	[15]
	Base block: {1, 2, 3, 4 }							
8	56	56	45	45	36	$PSL_3(4)$, $PSL_3(4):2_1$, $PSL_3(4):2_2$, $PSL_3(4):2_3$, $PSL_3(4):2^2$	$\mathcal{S}$	[12]
	Base block: { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37, 39, 40, 41, 44, 45, 46, 48, 53, 54 }							
9	56	420	90	12	18	$PSL_3(4)$, $PSL_3(4):2_1$, $PSL_3(4):2_2$, $PSL_3(4):2_3$, $PSL_3(4):2^2$	$\mathcal{S}$	[15]
	Base block: { 1, 2, 3, 5, 7, 8, 10, 12, 15, 16, 21, 22 }							
10	56	420	90	12	18	$PSL_3(4)$, $PSL_3(4):2_1$, $PSL_3(4):2_2$, $PSL_3(4):2_3$, $PSL_3(4):2^2$	$\mathcal{S}$	[15]
	Base block: { 1, 2, 3, 18, 25, 29, 30, 35, 37, 43, 47, 51 }							
11	56	3360	720	12	144	$PSL_3(4):2_2$, $PSL_3(4):2_3$, $PSL_3(4):2^2$	$\mathcal{S}$	[15]
	Base block: { 1, 2, 3, 4, 5, 8, 10, 15, 17, 22, 43, 50 }							
12	144	468	39	12	3	$PSL_3(3)$	$\mathcal{C}_3$	[15]
	Base block: { 1, 2, 10, 20, 21, 43, 48, 56, 79, 85, 95, 114 }							
13	144	936	78	12	6	$PSL_3(3):2$	$\mathcal{C}_3$	[15]
	Base block: { 1, 2, 4, 9, 42, 50, 66, 78, 88, 94, 118, 128 }							

Notes: The first row in each line consists of v, b, r, k, λ, G, Aschbacher's class of point stabilizer G and appropriate references. In each line , the full automorphism group of $\mathcal{D}$ occupies the last possibilities of the G.
The second row in each line consist of the base block for $\mathcal{D}$.
The block design in line 6 is the complement of line 5.

The block designs $\mathcal{D}$ admitting a flag-transitive and point-primitive almost simple automorphism group G have been widely studied by several authors. For example, in 1990, a classification of those with $\lambda = 1$ and $G \not\leqslant A\Gamma L_1(q)$ was announced by Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck and Saxl in [9]. Since then a special attention was given to the case $\lambda > 1$. A classification of the flag-transitive and point-primitive block design with $\gcd(r, \lambda) = 1$ and almost simple group

G has been announced by Alavi, Biliotti, Daneshkakh, Montinaro, Zhou and their collaborators in [10]. The purpose of this talk is to present a contribute part of the proof of the classification of flag-transitive and point-primitive block design $\mathcal{D}$. Let now that $\mathcal{D}$ be a nontrivial block design admitting a flag-transitive and point-primitive automorphism group G and let $H := G_\alpha$, where α is a point of $\mathcal{D}$. The theorem of O'Nan and Scott (see [14] for details) classifies primitive groups into five types: affine, almost simple, product, simple diagonal and twisted wreath product. In this talk, however, we are interested in nontrivial block design $\mathcal{D}$ admitting a flag-transitive and point-primitive automorphism group G of almost simple type. In this direction, we recently studied in [15, 16] the case where the socle X of G is a projective special linear groups of dimension at least 3 or an orthogonal simple groups of odd dimension and our main results are Theorems 1.1 and 1.1 below:

Theorem 1.1. *Let $\mathcal{D}$ be a nontrivial block design admitting an almost simple automorphism group G whose socle X is isomorphic to $PSL_n(q)$ with $n \geqslant 3$ and $q = p^a$ and let $H = G_\alpha$ with $\alpha \in \mathcal{P}$ and $f(q) = \gcd(v-1, d, |H|)$, for all nontrivial subdegrees d of G. If G is flag-transitive and point-primitive, then $\mathcal{D}$ is as in one of the lines in* Table 1*, or one of the following holds:*

(a) $H \in \mathcal{C}_1$,

(b) H *is a* $\mathcal{C}_2$*-subgroup of type* $GL_{n/2}(q) \wr S_2$ *if* $a \cdot f(q) > 3q$,

(c) H *is a* $\mathcal{C}_3$*-subgroup of type* $GL_{n/2}(q^2)$ *if* $a \cdot f(q) > q$,

(d) H *is a* $\mathcal{C}_5$*-subgroup of type* $GL_n(q_0)$ *with* $q = q_0^2$.

(e) H *is a* $\mathcal{C}_8$*-subgroup of type* $Sp_n(q)$ *or* $PSU_n(q_0)$ *with* $q = q_0^2$.

Theorem 1.2. *Let $\mathcal{D}$ be a nontrivial block design admitting an almost simple automorphism group G whose socle X is isomorphic to $P\Omega_n(q)$ with $n \geqslant 7$ and $q = p^a$ odd and let $H = G_\alpha$ with $\alpha \in \mathcal{P}$ and $f(q) = \gcd(v-1, d, |H|)$, for all nontrivial subdegrees d of G. If G is flag-transitive and point-primitive, then one of the following holds:*

(a) $H \in \mathcal{C}_1$*-subgroup of type* P_i,

(b) $H \in \mathcal{C}_1$*-subgroup of type* N_i^ϵ *with* $2n \geqslant 4i + (1 + \sqrt{8i+8})$,

(c) $H \in \mathcal{C}_1$*-subgroup of type* N_i^ϵ *with* $2n < 4i + (1 + \sqrt{8i+8})$ *if* $8a \cdot f(q) > q^{[n-(n-2i)^2]/2}$,

(d) H *is a* $\mathcal{C}_5$*-subgroup of type* $GL_n(q_0)$ *with* $q = q_0^2$,

(e) H *is a* $\mathcal{S}$*-subgroup and* $(X, H_0) = (\Omega_7(3), G_2(3))$, *where* $H_0 = H \cap X$.

Acknowledgments

The results discussed in this talk were obtained during the course of my postdoctoral research at Alzahra University. I am deeply thankful to Nasrin Soltankhah for his guidance and assistance.

References

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[3] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013. With a foreword by Martin Liebeck.

[4] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[5] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[6] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022.

[7] H. Davies. Flag-transitivity and primitivity. *Discrete Math.*, 63(1):91–93, 1987.

[8] A. Delandtsheer and J. Doyen. Most block-transitive t-designs are point-primitive. *Geom. Dedicata*, 29(3):307–310, 1989.

[9] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl. Linear spaces with flag-transitive automorphism groups. *Geom. Dedicata*, 36(1):89–94, 1990.

[10] S. H. Alavi, M. Bayat, M. Biliotti, A. Daneshkhah, E. Francot, H. Guan, A. Montinaro, F. Mouseli, P. Rizzo, D. Tian, Y. Wang, X. Zhan, Y. Zhang, S. Zhou, and Y. Zhu. Block designs with $\gcd(r, \lambda) = 1$ admitting flag-transitive automorphism groups. *Results Math.*, 77(4):Paper No. 151, 17, 2022.

[11] X. Zhan and S. Zhou. Non-symmetric 2-designs admitting a two-dimensional projective linear group. *Designs, Codes and Cryptography*, 86(12):2765–2773, 2018.

[12] S. H. Alavi, M. Bayat, and A. Daneshkhah. Symmetric designs and projective special linear groups of dimension at most four. *Journal of Combinatorial Designs*, 28(9):688–709, 2020.

[13] Y. Zhang and S. Zhou. Flag-transitive non-symmetric 2-designs with $(r, \lambda) = 1$ and Exceptional Groups of Lie type. *The Electronic Journal of Combinatorics*, 27(2):P2.9, 2020.

[14] M. W. Liebeck, C. E. Praeger, and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A*, 44(3):389–396, 1988.

[15] M. bayat and N. Soltankhah. Block designs admitting flag-transitive and point-primitive automorphism groups associated to projective special linear groups. *Submitted*.

[16] M. bayat and N. Soltankhah. Flag-transitive and point-primitive Block designs and orthogonal groups of odd dimension. *Submitted*.

Email: mohsenbayat3989@gmail.com
Email: soltan@alzahra.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Stability Analysis of Fractional Differential Equation[1]

Safoura Tavousi
Mohammad Bagher Ghaemi
Reza Saadati
Hengameh Tamimi[2]
School of Mathematics and Computer Science, Iran University of Science and Technology
16846-13114
Tehran, Iran

Abstract

This research is dedicated to establishing the existence and uniqueness of solutions for a Caputo-Fabrizino fractional differential system. Additionally, it explores the Hyers-Ulam-Rassias and Hyers-Ulam-Mittag-Leffer stability of these solutions. This study utilizes the alternative fixed point theorem as a fundamental tool in its analysis. In recent papers, authors used the Schauder fixed point theorem and the Laplace transform to prove the stability of Caputo-Fabrizio equations, but we use the alternative fixed point theorem to prove the stability of these equations.

Keywords: Stability theory of functional-differential equations, Functional-differential equations, fractional derivatives, Fixed-point theorems, Mittag-Leffer functions, Control/observation systems.
AMS Mathematical Subject Classification [2010]: 34K20, 34K37, 47H10, 33E12, 93C23, 46B25.

1 Introduction

The Caputo-Fabrizio fractional derivative was introduced by Michele Caputo and Mauro Fabrizio in 2015 and represents a relatively recent development in the field of fractional calculus. One of the main advantages of the Caputo-Fabrizio derivative is that it is more suitable for certain applications in physics and engineering because it avoids the singularity at $t = s$ found in the traditional Caputo derivative. This derivative is defined using an exponential kernel, which provides a more flexible approach to modeling some processes.

This paper explores the stability of Caputo-Fabrizio differential equations, particularly focusing on Hyers-Ulam-Rassias and Hyers-Ulam-Mittag-Leffer stability of

$$\begin{cases} {}^{CF}\mathbb{I}^{\beta} P(\kappa) = \mu(\kappa, P(\kappa)) \;\; \kappa \in [0, b], \\ P(0) = 0, \end{cases} \tag{1}$$

in which ${}^{CF}\mathbb{I}^{\beta}$ is the Caputo-Fabrizio integral of order β. By analyzing these types of stability, the study seeks to understand how solutions react to small perturbations. This understanding is essential for applications that require precise and stable solutions, such as in engineering and scientific modeling. The research offers valuable insights into the behavior of fractional differential equations, thereby enhancing both their practical utility and theoretical understanding.

[2]speaker

2 Preliminaries

Theorem 2.1 (Alternative fixed point). *[2] Consider generalized complete metric space (Φ, γ), and Lipschitz mapping $T\colon \Phi \longrightarrow \Phi$ with constant $\beta < 1$. Then, for some $i \in \Phi$ either,*

$$\gamma(T^m(i), T^{m+1}(i)) = +\infty \quad (m \geq 0),$$

or we can find a natural number m_0 such that:

$$\gamma(T^m(i), T^{m+1}(i)) < +\infty \quad (\forall m \geq m_0),$$

then the followings are true:

1. *The fixed point α of T is the convergence point of the sequence $\{T^n(i)\}$;*
2. *In the set $M = \{\alpha^* \in \Phi\colon \gamma(T^m(i), \alpha^*) < +\infty\}$, α is the unique fixed point of T;*
3. *For all $\alpha^* \in M$, $\gamma(\alpha^*, \alpha) \leq \frac{1}{\beta - 1}\gamma(\alpha^*, T(\alpha^*))$.*

Definition 2.2. [1] The function $P : [\alpha, \infty) \to \mathbb{R}$ is smooth, then the Caputo-Fabrizio integral of order β is defined as

$${}^{CF}\mathbb{I}^{\beta} P(\kappa) = (1 - \beta)[P(\kappa) - P_0] + \beta \int_0^{\kappa} P(\nu)\, \mathrm{d}\nu \tag{2}$$

with $P_0 = \int_{\alpha}^{0} e^{-\frac{\beta}{1-\beta}\nu} P'_{\nu}\, \mathrm{d}\nu$. Of course, if $\alpha = 0$, then $P_0 = 0$, and

$${}^{CF}\mathbb{I}^{\beta} P(\kappa) = (1 - \beta)P(\kappa) + \beta \int_0^{\kappa} P(\nu)\, \mathrm{d}\nu. \tag{3}$$

Definition 2.3. Let $\varphi \in \mathcal{C}([0, b], \mathbb{R})$, and $\Upsilon = \mathcal{C}([0, b], \mathbb{R})$ if for each $P \in \Upsilon$ the following condition is verified:

$$\left|(1 - \beta)\mu(\kappa, P(\kappa)) + \beta \int_0^{\kappa} \mu(\nu, P(\nu))\, \mathrm{d}\nu - P(\kappa)\right| \leq \varphi(\kappa) \tag{4}$$

then the system (1) is Hyers-Ulam-Rassias stable and there exists solution $Q \in \Upsilon$ of system (1) such that:

$$|Q(\kappa) - P(\kappa)| \leq \sigma\varphi(\kappa), \qquad \kappa \in [0, b] \tag{5}$$

where positive constant σ does not depend on P.

Definition 2.4. [3] Assume the gamma function Γ. A generalization of the exponential function is the Mittag Leffler function given by

$$E_i(\Delta) := \sum_{\kappa=0}^{\infty} \frac{\Delta^{\kappa}}{\Gamma(\kappa i + 1)}, \qquad i \in \mathbf{C},\ \mathbf{Re}(i) > 0. \tag{6}$$

Definition 2.5. The system (1) is Hyers-Ulam-Mittag-Leffer stable according to $E_i(-|(\Delta(\kappa) - \Delta(0))^i|)$ if for each $P \in \Upsilon$, the following condition is verified:

$$\left|(1 - \beta)\mu(\kappa, P(\kappa)) + \beta \int_0^{\kappa} \mu(\nu, P(\nu))\, \mathrm{d}\nu - P(\kappa)\right| \leq E_i(-|(\Delta(\kappa) - \Delta(0))^i|), \tag{7}$$

then there exist positive constant σ and solutions $Q \in \Upsilon$ of (1) such that

$$|Q(\kappa) - P(\kappa)| \leq \sigma E_i(-|(\Delta(\kappa) - \Delta(0))^i|), \qquad \kappa \in (0, b). \tag{8}$$

3 Main results

This section shows that (1) has a unique solution. Then, the stability of Hyers-Ulam-Rassias, and Hyers-Ulam-Mittag-Leffer for (1) according to the alternative fixed point theorem is investigated.

Lemma 3.1. *Let $\varphi \in \Upsilon$, and $P, Q \in \Upsilon$ for $\kappa \in [0, b]$, if we define a mapping $d : \Upsilon \times \Upsilon \to [0, +\infty]$, by*

$$d(P(\kappa), Q(\kappa)) := \inf \left\{ c \geq 0 : |P(\kappa) - Q(\kappa)| \leq c\varphi(\kappa) \right\}. \tag{9}$$

Then we demonstrate that (Υ, d) constitutes a generalized metric space.

Proof. For every $\kappa \in [0, b]$ we show that $d(P(\kappa), Q(\kappa)) = 0$ if and only if $P(\kappa) = Q(\kappa)$. Assume $d(P(\kappa), Q(\kappa)) = 0$, then for all $P(\kappa), Q(\kappa) \in \Upsilon$ and $\kappa \in [0, b]$, we have:

$$\inf \left\{ c \geq 0 : |P(\kappa) - Q(\kappa)| \leq c\varphi(\kappa) \right\} = 0,$$

so for every $\kappa \in [0, b]$ we have $P(\kappa) = Q(\kappa)$, and conversely. This can be easily demonstrated $d(P(\kappa), Q(\kappa)) = d(Q(\kappa), P(\kappa))$ for every $P, Q \in \Upsilon$. Now, consider for $j = 1, 2$; there exist constants f_j such that $d(P(\kappa), \eta(\kappa)) = f_1$ and $d(Q(\kappa), \eta(\kappa)) = f_2$. Then, we have

$$\begin{cases} |P(\kappa) - \eta(\kappa)| \leq f_1\varphi(\kappa), \\ |Q(\kappa) - \eta(\kappa)| \leq f_2\varphi(\kappa), \end{cases} \tag{10}$$

according to the triangular property in absolute magnitudes, we can define $k_1 = f_1 + f_2$ such that:

$$|P(\kappa) - Q(\kappa)| \leq |P(\kappa) - \eta(\kappa)| + |Q(\kappa) - \eta(\kappa)| \leq k_1\varphi(\kappa), \tag{11}$$

If we take the infimum from the above relationship, we obtain:

$$\begin{aligned} d\left(P(\kappa), Q(\kappa)\right) &\leq \inf\left\{f_1 \geq 0 : |P(\kappa) - \eta(\kappa)| \leq f_1\varphi(\kappa)\right\} + \inf\left\{f_2 \geq 0 : |Q(\kappa) - \eta(\kappa)| \leq f_2\varphi(\kappa)\right\} \\ &= d(P(\kappa), \eta(\kappa)) + d(Q(\kappa), \eta(\kappa)). \end{aligned}$$

Now, we demonstrate the completeness of (Υ, d). Consider a Cauchy sequence $\{P_n(\kappa)\}_n$. This means that for any positive number i, there exists a natural $\mathbb{N}_i$ such that for all $n, m \geqslant \mathbb{N}_i$, we have:

$$d(P_n(\kappa), P_m(\kappa)) < i.$$

With definition (9), for all $\kappa \in [0, b]$ we can express:

$$|P_n(\kappa) - P_m(\kappa)| \leqslant i\varphi(\kappa). \tag{12}$$

Let $\kappa \in [0, b]$ is fixed, so the sequence $\{P_n(\kappa)\}_n$ is a Cauchy sequence in $\mathbb{R}$ and, due to the completeness of $\mathbb{R}$, converges for each $\kappa \in [0, b]$. Consequently, we can define a function $P(\kappa)\colon [0, b] \to \mathbb{R}$ by

$$P(\kappa) = \lim_{n\to\infty} P_n(\kappa).$$

Given that $\varphi(\kappa)$ is continuous and bounded over the compact interval $[0, b]$. Thus, (12) implies that $\{P_n(\kappa)\}_n$ converges uniformly to $P(\kappa)$ in the usual topology of $\mathbb{R}$. Hence, $P \in \Upsilon$. If we suppose m approaches to infinity, for $i > 0$ a natural $\mathbb{N}_i$ exists such that for $n \geqslant \mathbb{N}_i$ it follows from (12) that

$$|P_n(\kappa) - P(\kappa)| \leqslant i\varphi(\kappa), \tag{13}$$

for all posetive i there exists natural $\mathbb{N}_i$ such that for all $n > \mathbb{N}_i$ considering equation (9), we obtain

$$d(P(\kappa), P_n(\kappa)) \leqslant i.$$

This indicates that the Cauchy sequence$\{P_n\}$ converges to P in (Υ, d), demonstrating the completeness of (Υ, d). □

Theorem 3.2 (UHR stability)**.** *Assume $P \in \Upsilon$ satisfies* (4)*, $\varphi \in \Upsilon$, and conditions* (R_1)*,* (R_2)*, and* (R_3) *hold:*

(R_1) *There exist constant $\theta > 0$ such that*

$$|\mu(\kappa, P(\kappa)) - \mu(\kappa, Q(\kappa))| \leq \theta |P(\kappa) - Q(\kappa)|, \tag{14}$$

(R_2) *There exist constant $\delta < 1$ such that*

$$\int_0^\kappa \varphi(\nu)\, \mathrm{d}\nu \leq \delta \varphi(\kappa), \tag{15}$$

(R_3) *There exist constant $\gamma < 1$ such that*

$$\gamma = \theta(|1 - \beta| + \beta). \tag{16}$$

Thus a unique solution of (1) *is $Q \in \Upsilon$ such that*

$$Q(\kappa) = (1 - \beta)\mu(\kappa, Q(\kappa)) + \beta \int_0^\kappa \mu(\nu, Q(\nu))\, \mathrm{d}\nu, \tag{17}$$

in which

$$|Q(\kappa) - P(\kappa)| \leq \frac{c_1}{1 - \gamma}\varphi(\kappa), \qquad \kappa \in [0, b]. \tag{18}$$

Proof. Assume that $P, Q \in \Upsilon$ and $\kappa \in [0, b]$ define a mapping $d : \Upsilon \times \Upsilon \to [0, +\infty]$ by

$$d\Big(P(\kappa), Q(\kappa)\Big) = \inf\{c > 0, |P(\kappa) - Q(\kappa)| < c\varphi(\kappa)\}. \tag{19}$$

According to Lemma 3.1 (Υ, d) is a generalized metric space.

Step 1. We define the operator $F : \Upsilon \to \Upsilon$ and then we prove that it is contractive.

$$F(P(\kappa)) = (1 - \beta)\mu(\kappa, P(\kappa)) + \beta \int_0^\kappa \mu(\nu, P(\nu))\, \mathrm{d}\nu. \tag{20}$$

First, we need to prove that $F(P(\kappa))$ belongs to the space Υ. Based on the fundamental theorem of calculus, we can conclude that $F(P(\kappa))$ is continuously differentiable on the interval $[0, b]$, since $P(\kappa)$ is a continuous function, which implies that $F(P(\kappa)) \in \Upsilon$. We claim that F is contractive on Υ. Let $P(\kappa), Q(\kappa) \in \Upsilon$, and $d(P(\kappa), Q(\kappa)) = h$ so that $h \in [0, \infty]$ be a constant. Furthermore, we can express:

$$\Big|P(\kappa) - Q(\kappa)\Big| \leq h\varphi(\kappa). \tag{21}$$

It can be written using relations (19), (R_1), and (R_2)

$$\begin{aligned}
&\Big|(1-\beta)\mu(\kappa,P(\kappa))+\beta\int_0^{\kappa}\mu(\nu,P(\nu))\,\mathrm{d}\nu-\Big((1-\beta)\mu(\kappa,Q(\kappa))+\beta\int_0^{\kappa}\mu(\nu,Q(\nu))\,\mathrm{d}\nu\Big)\Big| \qquad (22)\\
&\le\Big|(1-\beta)\mu(\kappa,P(\kappa))-(1-\beta)\mu(\kappa,Q(\kappa))+\Big(\beta\int_0^{\kappa}\mu(\nu,P(\nu))\,\mathrm{d}\nu-\beta\int_0^{\kappa}\mu(\nu,Q(\nu))\,\mathrm{d}\nu\Big)\Big|\\
&\le\Big|(1-\beta)\Big(\mu(\kappa,P(\kappa))-\mu(\kappa,Q(\kappa))\Big)\Big|+\Big|\beta\Big(\int_0^{\kappa}\mu(\nu,P(\nu))\,\mathrm{d}\nu-\int_0^{\kappa}\mu(\nu,Q(\nu))\,\mathrm{d}\nu\Big)\Big|\\
&\le|1-\beta|\Big|\mu(\kappa,P(\kappa))-\mu(\kappa,Q(\kappa))\Big|+\beta\int_0^{\kappa}\Big|\mu(\nu,P(\nu))-\mu(\nu,Q(\nu))\Big|\,\mathrm{d}\nu\\
&\le\theta|1-\beta|\Big|P(\kappa)-Q(\kappa)\Big|+\beta\int_0^{\kappa}\theta\Big|P(\nu)-Q(\nu)\Big|\,\mathrm{d}\nu\\
&\le\theta|1-\beta|h\varphi(\kappa)+\theta\beta\int_0^{\kappa}h\varphi(\nu)\,\mathrm{d}\nu\\
&\le h\theta|1-\beta|\varphi(\kappa)+\theta\beta\delta h\varphi(\kappa)\\
&\le\theta(|1-\beta|+\delta\beta)h\varphi(\kappa).
\end{aligned}$$

If we take the infimum from the above relationship, we have:

$$d\Big(F(P(\kappa)),F(Q(\kappa))\Big)\le\theta(|1-\beta|+\delta\beta)d(P(\kappa),Q(\kappa)). \qquad (23)$$

According to (R_3), F is a contraction .

Step 2. Suppose $P\in\Upsilon$, then we show that $d\Big(P(\kappa),F(P(\kappa))\Big)<\infty$ for $\kappa\in[0,b]$. According to (4),(19), and (20), we have

$$\begin{aligned}
d\Big(P(\kappa),F(P(\kappa))\Big)&=\inf\left\{c>0,\left|P(\kappa)-\left((1-\beta)\mu(\kappa,P(\kappa))+\beta\int_0^{\kappa}\mu(\nu,P(\nu))\,\mathrm{d}\nu\right)\right|\le\varphi(\kappa)\right\} \qquad (24)\\
&\le c\le 1<\infty.
\end{aligned}$$

Now, according to the Theorem 2.1, we can find the element $Q\in\Upsilon$ that satisfies the following conditions:

1. The fixed point Q of F is the convergence point of the sequence $\{F^m(P(\kappa))\}$;
2. In the set $\Upsilon^*=\Big\{P^*\in\Upsilon:d\Big(F((P(\kappa)),P^*(\kappa)\Big)<\infty,\kappa\in[0,b]\Big\}$, Q is a unique fixed point of F, such that,
$$F(Q(\kappa))=(1-\beta)\mu(\kappa,Q(\kappa))+\beta\int_0^{\kappa}\mu(\nu,Q(\nu))\,\mathrm{d}\nu.$$
3. If $P^*\in\Upsilon^*$, and $\gamma=\theta(|1-\beta|+\beta)$, then we have
$$d\left(P^*(\kappa),Q(\kappa)\right)\le\frac{1}{1-\gamma}d\left(F\left(P^*(\kappa)\right),P^*(\kappa)\right).$$

From (24), because $P\in\Upsilon^*$ we get

$$d\Big(P(\kappa),Q(\kappa)\Big)\le\frac{c}{1-\gamma}.$$

Then,

$$|P(\kappa)-Q(\kappa)|\le\frac{c}{1-\gamma}\varphi(\kappa),\qquad\qquad\kappa\in[0,b]. \qquad (25)$$

□

Corollary 3.3 (UHML stability). *Assume $P \in \Upsilon$ satisfies 4, and conditions (R_1), (R_2), hold:*

(R_1) *There exist constants $\theta > 0$ such that*

$$|\mu(\kappa, P(\kappa)) - \mu(\kappa, Q(\kappa))| \leq \theta |P(\kappa) - Q(\kappa)|. \tag{26}$$

(R_2) *There exist constant $\delta < 1$ such that*

$$\int_0^\kappa E_\iota(-|(\Delta(\nu) - \Delta(0))^i|)\, \mathrm{d}\nu \leq \delta E_\iota(-|(\Delta(\kappa) - \Delta(0))^i|). \tag{27}$$

(R_3) *There exist constant $\gamma < 1$ such that*

$$\lambda = \theta(|1 - \beta| + \beta). \tag{28}$$

Thus, a unique solution of (1) *is $Q \in \Upsilon$ such that*

$$Q(\kappa) = (1 - \beta)\mu(\kappa, Q(\kappa)) + \beta \int_0^\kappa \mu(\nu, Q(\nu))\, \mathrm{d}\nu, \tag{29}$$

in which

$$|P(\kappa) - Q(\kappa)| \leq \left(\frac{c}{1 - \gamma}\right) E_i(-|(\Delta(\kappa) - \Delta(0))^i|), \qquad \kappa \in [0, b]. \tag{30}$$

Proof. Similarly to Theorem 3.2, we can prove this corollary. □

References

[1] Losada, J., and Nieto, J. J. Fractional integral associated to fractional derivatives with nonsingular kernels. *Progress in Fractional Differentiation and Applications*, 7(3), (2021) 137-143.

[2] Diaz, J. B., and Margolis, B. A fixed point theorem of the alternative, for contractions on a generalized complete metric space. *Bulletin of the American Mathematical Society*, 74(2), (1968), 305-309.

[3] Kilbas, A. A. *Theory and applications of fractional differential equations.*(2006) Elsevier.

e-mail: safouratavousi77@gmail.com
e-mail: mghaemi@iust.ac.ir
e-mail: rsaadati@eml.cc
e-mail: hengamehtamimi@gmail.com

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Disseminating Information Across a Network: an Evolutionary Study

Abbas Rahimi[1]
Department of Pure Mathematics, Faculty of Mathematical Science, University of Kashan, Kashan, Iran

Abolfazl Aghdaee
Department of Computer Science, Faculty of Mathematical Science, University of Kashan, Kashan, Iran

Mahsa Soheil Shamaee
Department of Computer Science, Faculty of Mathematical Science, University of Kashan, Kashan, Iran

Gholam Hossein Fath-tabar
Department of Pure Mathematics, Faculty of Mathematical Science, University of Kashan, Kashan, Iran

Abstract

The graph-burning problem is a significant issue in graph theory, and it has important applications in network science, particularly regarding weighted graphs. In this context, networks are modeled as graphs where nodes represent entities and edges denote connections with specific bandwidths, reflected in the weights that indicate message transmission times. The challenge involves efficiently disseminating a message from a central authority to all nodes, either directly or through neighboring nodes while minimizing time. This paper aims to determine an optimal sequence that utilizes the fewest vertices for effective message spreading in weighted graphs. Given its NP-hard nature, this study generalizes two evolutionary algorithms to find optimal solutions and compare their effectiveness.

Keywords: burning graph, weighted graph, evolutionary algorithms
Mathematics Subject Classification [2010]: 13D45, 39B42

1 Introduction

The graph burning problem is a fundamental issue in graph theory, and it has numerous applications in network science. This paper will focus on the graph-burning problem in the context of weighted graphs. Imagine a network of entities interconnected by channels that have specific bandwidths. This network can be represented as a graph, where each entity is depicted as a node and the connections between them are shown as edges. The graph is weighted because the weight assigned to each edge reflects the time required for a message to travel from one vertex to another. Essentially, the weight of each edge corresponds directly to the bandwidth of the channel linking the two adjacent vertices. We treat time as divided into discrete slots, each lasting one unit. The weight associated with each edge indicates the number of time slots needed to send a message from one vertex to another connected by that edge.

Imagine a central authority tasked with spreading an important message across a network, ensuring that all nodes receive it as quickly as possible. There are two main approaches: the central authority can either send the message directly to a node or allow one of its neighboring nodes to pass the message along via an edge. However, the cost of sending messages from the central authority to the other nodes is often high, primarily due to the significant geographical distances involved. Consequently, delivering the message

[1]speaker

from the central authority to each node usually requires a considerable amount of time. In contrast, it is generally more effective for the system to function in a largely decentralized manner instead of relying on a central authority. If that central authority were to fail, the entire process of message transmission would break down, leaving no nodes with the message.

The goal of tackling the graph burning problem on weighted graphs is to determine a sequence that uses the fewest vertices, thereby minimizing the time needed to disseminate the message. In this sequence, at each time interval, the vertices gather information from a central authority and pass it on to their adjacent vertices. To our knowledge, this paper is the first to study the graph burning problem on weighted graphs.

At first glance, the burning problem on a weighted graph seems similar to the task of finding a minimum-spanning tree. This analogy is valid when the central entity transmits the message only to the initial node, enabling the other nodes to independently pass the information to their neighbors. However, in the context explored in this article, the central authority must send the message to one specific node at each time step, to ensure that all nodes receive the information in the shortest amount of time possible. In fact, this problem essentially merges the task of locating a minimum spanning tree in a weighted graph with the concept of graph burning in an unweighted graph.

Given that the burning problem on an unweighted graph is NP-hard, it follows that the burning problem on a weighted graph is also NP-hard. Therefore, in this study, we adopted two population-based evolutionary algorithms with a single objective: genetic algorithm (GA) and particle swarm optimization (PSO) to identify near-optimal solutions and subsequently compare their performance.

This paper is organized in the following manner: The upcoming section offers a review of relevant studies concerning the burning problem in unweighted graphs. Section 3 discusses the adaptation of single-objective evolutionary algorithms to tackle the burning problem in weighted graphs. The next section details the experimental studies carried out. Lastly, Section 5 concludes the paper and highlights possible avenues for future research.

2 Related Works

Numerous studies have explored the graph burning problem in unweighted graphs from various viewpoints. This problem was mathematically modeled by Bonato et al. in 2014. [3] in an innovative manner. The Model combining ideas from mathematics, computer science, and social networks, became one of the most popular interdisciplinary problems that attracted researchers' attention. However, in a Graph Burning model, one specific node that receives the information immediately notifies the others neighboring the same node. This process continues until all the nodes in the network "burn" or learn. The Burning Number has been explained as a significant metric in this model meant to determine the extent to which information is spread. This number has been utilized to determine the most effective sequence of information flow. In that same year, this number had in the later years been proven to be asymptotically one in many instances [20].

In [3] the Burning Number parameter was first introduced as a measure of the speed with which information disseminates, and also out of the blue in many recent works has been asymptotically proven [20] a ceiling for that number. Papers [17] ,[18] dealt with the parametric complexity of this problem. Theoretical research on the various classes of graphs that pertain to the problem, including but not limited to algorithms, bounds, and graph burning.

A recent survey on Graph Burning [9],[4] should be consulted for additional information. The approximation methods to solve this problem have been investigated in papers [9],[10],[11], [16]. In this context, approximation algorithms of the 3-approximation ratio were suggested in [9],[10]. It was also established in [10] a 2-approximation algorithm for trees. Outside approximation, algorithms, heuristic techniques have been abundantly and examined and discovered in papers [14],[15], [22], [26]. The heuristic methods to solve this problem are addressed by Shimon et al. [22] as follows:

1. Maximum Eigenvector Centrality Heuristic (MECH): In this approach, a node with the greatest eigenvector centrality is first selected and placed into the burn sequence. The rule is that this action starts with an empty burn sequence and ends when the valid sequence is, finally, formed.

2. Corner Cutting Heuristic (CCH): In this approach, a set of nodes termed corners are selected using an algorithm. This set of corners and the eigenvector centrality are used to identify the candidate (central) nodes. The candidate nodes go through the WASPAS algorithm for the selection of the next fire source.

3. Greedy Forward Search Heuristic (GFSSH): Besides WASPAS output, this approach also looks for less promising nodes and incorporates them in the fire source selection process. Forward search techniques such as A* select a fire source among these nodes at each iteration (step). This scenario enables better comprehensive coverage of the solution space and often guarantees better solution quality.

In their subsequent research, Shimon et al. [23] used other than eigenvector centrality to implement the MECH method with 30 other centrality measures, which is a novel approach. In this study, centrality measures were applied as well as tested against other datasets. The findings indicated that betweenness and closeness centralities were the most prevalent for general networks while for geometric networks (such as mobile networks), the most effective centrality measure became betweenness centrality. Gatoum et al. [15] discussed three heuristics based on the eigenvector centrality for their recent investigations:

1. Spine-Based Greedy Method (BBGH)

2. Modified Corner Cutting Heuristic (ICCH)

3. Component-Based Recursive Heuristic (CBRH)

They utilized these algorithms together with other heuristic methods on the SNAP and Network Data Repository datasets [19], [21]. Their results showed that their suggested algorithms produced similar results to other previous methods (for example, the three methods proposed by Shimon et al. in [22]), but this time at a much faster rate.

The Genetic Algorithm is a population-based optimization method based on the natural selection principles [24]. Thus, a multitude of optimization problems that range from, to name a few, engineering, logistics, management, and economics, have been addressed by these algorithms [8].

In a recent publication[25], a Centered genetic Algorithm (CBAG) was proposed to tackle the graph burning problem. This algorithm starts the initial stage of chromosome population generation based on centrality measures. Then the chromosomes are constructed through some cross-over and mutation operations. To test the effectiveness of this algorithm, CBAG was tried out on 15 standard graphs of different sizes. The results were that, in general, CBAG is superior to other heuristic and approximation algorithms.

3 The proposed methods

In the following, we proposed two approaches based on single-objective evolutionary algorithms-Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) to tackle the burning problem in weighted graphs.

3.1 BurningPSO

In our PSO-based approach to solving the burning problem in a weighted graph, we first initialize a population of particles, where each particle represents a unique solution. Each solution, or particle, is structured as a sequence of nodes in the graph, specifying the order in which nodes will be selected to ignite the burning process. Each particle is initially assigned a zero velocity, implying no movement or change to its structure in the first iteration. In addition to this, the initial sequence of each particle is recorded as its best personal solution. At the same time, the best solution among all particles is identified as the global best. This initialization ensures that we start with diverse potential solutions, which the algorithm will iteratively improve.

The fitness of the sequence of each particle is then evaluated using the *burning-graph-fitness* function. In this function, the algorithm simulates the burning process starting from each node in the sequence and

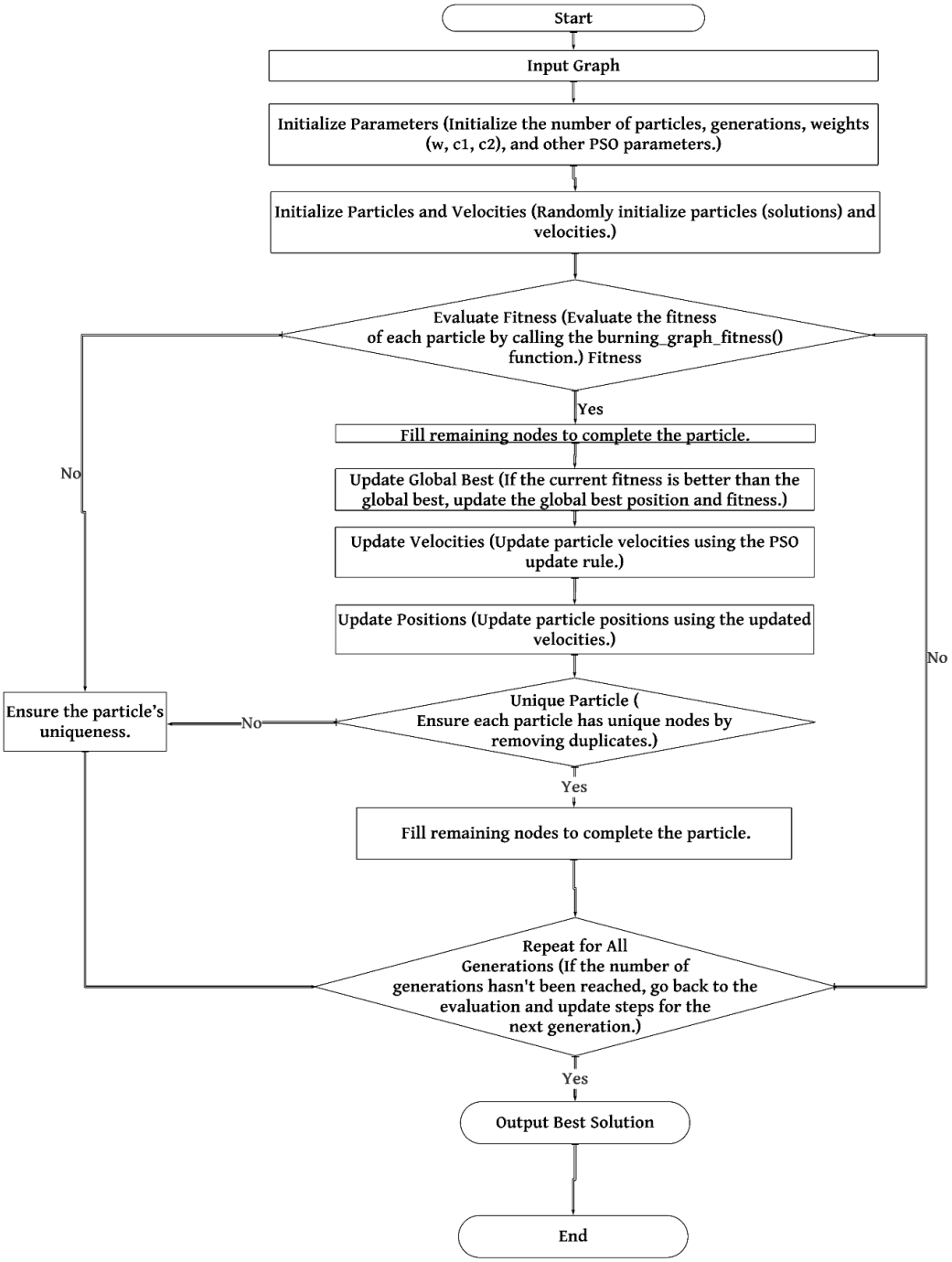


Figure 1: The flowchart of the proposed BurningPSO

spreading across its neighbors based on a given adjacency structure. The function tracks nodes as they ignite and records the time taken to burn each one, aiming to minimize the burn time across all nodes. Specifically, the fitness function computes the number of nodes in the sequence, the exact sequence of node selections, and the burn time, which is taken as the fitness score in this research. The lower this burn time, the better the fitness.

The proposed method updates each particle's velocity and position to explore new potential solutions. In PSO, velocity is a critical factor that combines aspects of a particle's previous movement, the gap between

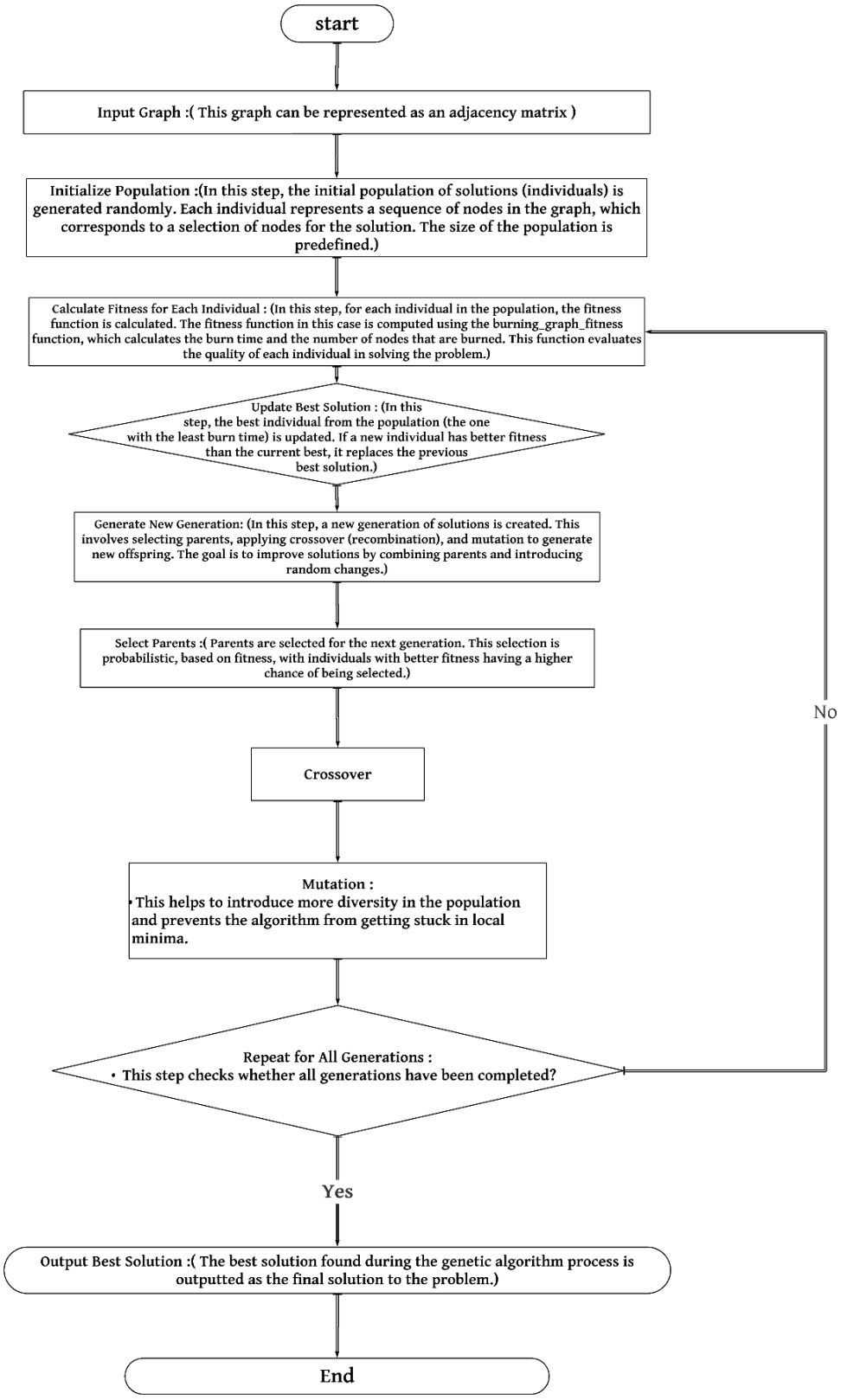


Figure 2: The flowchart of the proposed BurningGA

its personal best and current position, and the gap between the global best and current position. Each of these components is weighted: the particle's momentum, or inertia, is represented by w; the attraction to its personal best is influenced by c_1 and a random coefficient r_1; and the pull towards the global best is controlled by c_2 and a random coefficient r_2. These weights and coefficients introduce a degree of randomness and flexibility in particle movement, allowing particles to explore a wide range of solutions and avoid becoming trapped in suboptimal local solutions. In BurningPSO, the position and velocity of each particle are updated iteratively to find the optimal solution. The velocity is updated as follows:

$$v_i(t+1) = w \times v_i(t) + c_1 \times r_1 \times (pbest_i - x_i(t)) + c_2 \times r_2 \times (gbest - x_i(t))$$

where w (inertia weight) takes a value of 0.5, controlling the influence of the previous velocity, $v_i(t+1)$ denotes velocity of particle i at iteration $t+1$, c_1 is the cognitive coefficient (self-attraction), encouraging movement towards the particle's personal best position ($pbest_i$), c_2 represents social coefficient (group attraction), encouraging movement towards the global best position ($gbest$). r_1 and r_2 are random numbers in $[0, 1]$, introducing stochastic behavior. Moreover, $x_i(t)$ denotes the current position of particle i at iteration t. Once a new velocity is calculated for each particle, it is applied to update the particle's position by adjusting node indices in its sequence. The position of the particle i at iteration $t+1$ is updated as follows:

$$x_i(t+1) = x_i(t) + v_i(t+1)$$

where $x_i(t+1)$ is the position of particle i at iteration $t+1$. Since the sequence represents a unique order of nodes, the proposed method must handle any constraints introduced by this structure. Specifically, particles can sometimes produce duplicate nodes when their positions are updated, so the proposed method includes a step to enforce uniqueness in each particle's sequence. It removes duplicates and appends any missing nodes in order to create a complete and valid sequence. This step maintains the integrity of each solution, ensuring each particle remains a viable candidate for the burning graph problem.

After iterating through the generations, BurningPSO returns the global best solution identified across all generations. This final solution includes the optimal sequence of nodes to achieve the minimum burn time, providing an efficient way to solve the burning graph problem with Particle Swarm Optimization. The sequence and its corresponding burn time represent the best solution found, effectively balancing exploration and exploitation to yield a robust result. The flowchart of the proposed PSO is shown in Figure 1.

3.2 BurningGA

Similar to particles in BurningPSO, each solution is modeled as a chromosome in BurningGA. The fitness in BurningGA is the same as the fitness function in BurningPSO which is described in the previous section. The cross-over is the single point and the mutation is the random swapping of two genes in an offspring.

Once the parents are selected, offspring are generated using a single-point crossover technique. A random crossover point is chosen, and the child inherits the first part of its sequence from one parent and the remaining part from the other parent. Care is taken to ensure that the child does not contain duplicate nodes by appending only those nodes from the second parent that are not present in the first portion of the sequence. This process generates two offspring from each parent pair, ensuring genetic diversity in the next generation while preserving good traits from both parents.

The algorithm begins by randomly generating an initial population of candidate solutions. Each solution is a sequence of nodes, randomly sampled from the total number of nodes in the graph. These sequences represent different strategies for selecting nodes in the burning process. To generate the next generation of solutions, parent solutions are selected using a fitness-proportionate selection mechanism (roulette wheel selection). Parents with lower fitness scores are more likely to be selected to produce offspring. Once parents are selected, offspring are generated through a single-point crossover operation. To introduce variability into the population and avoid premature convergence, a mutation operator is applied to the offspring. The mutation consists of randomly swapping two nodes in the sequence with a predefined mutation probability. This allows the algorithm to explore new regions of the solution space that may not have been accessible through crossover alone.

The newly generated offspring replace the old population, and the process repeats for a predefined number of generations. After each generation, the algorithm continues to refine the population toward better node sequences. after termination, the algorithm returns the best solution found, including the sequence of selected nodes and the corresponding burn time. The flowchart of the proposed BurningGA is shown in Figure 2.

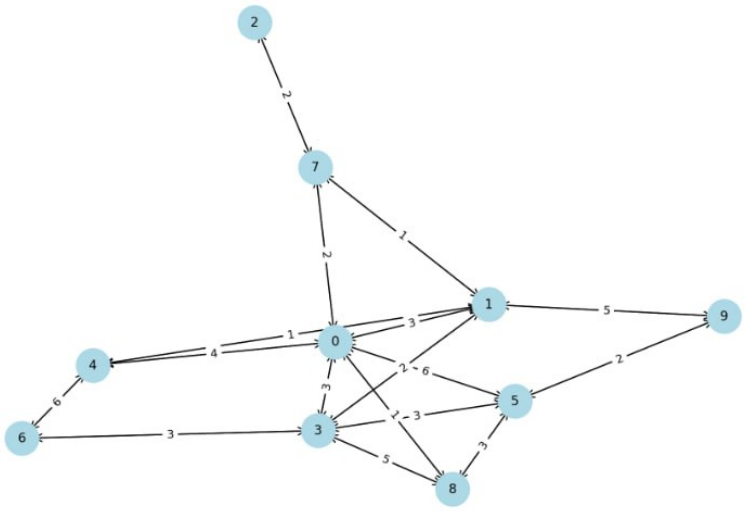


Figure 3: A sample weighted graph in which our proposed BurningPSO finds the optimal solution ($[5, 7, 4, 6]$) whereas BurningGA finds the near-optimal one ($[3, 5, 1, 0, 2]$).

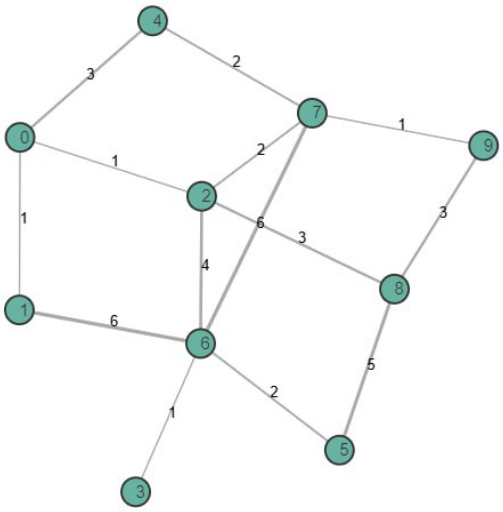


Figure 4: A sample weighted graph in which our proposed BurningGA finds the optimal solution ($[6, 7, 1, 8]$) whereas BurningPSO finds the near-optimal one ($[2, 7, 1, 6, 5]$).

4 Experimental Studies

In this paper, we conducted numerous experiments to evaluate the proposed methods. We constructed a dataset consisting of 100 random graphs, with the number of vertices varying from 4 to 11 and the number of edges ranging from 3 to 48. Additionally, the weights of the edges are randomly chosen integer values in the range of $[1, 6]$. The dataset is available upon request from the interested reader. Furthermore, the

number of particles is 30, the number of generations is 100, the mutation probability is 0.1, and the values of the parameters w, c_1, and c_2 are 0.5, 1.5, and 1.5, respectively.

Figure 3 illustrates a sample weighted graph in which our proposed BurningPSO effectively identifies the optimal solution, achieving a total burning time of 4 time slots. In contrast, BurningGA arrives at a near-optimal solution with a total burning time of 5 time slots. This figure demonstrates the superiority of BurningPSO over BurningGA in this instance. Figure 4 presents another sample weighted graph where BurningGA successfully identifies the optimal solution, while BurningPSO finds a near-optimal solution.

To evaluate the effectiveness of the proposed method, we implemented a Brute Force algorithm to determine the optimal solution precisely. Table 1 presents a comparison of BurningPSO, BurningGA, and Brute Force based on their accuracy and running time on the dataset graphs. Accuracy is measured by the percentage of graphs for which each method successfully identifies the optimal solution, while running time is reported in seconds for the total graph dataset. As shown, BurningGA outperforms BurningPSO in terms of accuracy. Conversely, BurningPSO demonstrates superior performance over both BurningGA and Brute Force in terms of running time.

Table 1: The accuracy and running time of the proposed methods, BurningPSO, BurningGA, and Brute force on 100 random graphs in dataset

	BurningPSO	BurningGA	Brute Force
accuracy	%95	%98	%100
time	27.67	42.75	20445.8852

Figure 5 presents two chart demonstrating the model's performance based on variations in the number of particles and repetitions:

1. Top chart: This graph illustrates the effect of the number of particles on the model's accuracy. The horizontal axis represents the number of particles, while the vertical axis indicates accuracy. It is observed that accuracy fluctuates as the number of particles changes, reaching a maximum of 99 at certain points (e.g., 40, 90, and 110) while decreasing at others (e.g., 20 and 100).

2. Bottom chart: This graph examines the impact of the number of repetitions on the model's accuracy. The horizontal axis shows the number of repetitions, and the vertical axis represents accuracy. The overall trend indicates an improvement in accuracy with an increase in repetitions, achieving 100 at 500 and 700 repetitions. However, temporary drops in accuracy are observed at points like 300 and 600.

This analysis highlights the importance of optimizing parameters such as the number of particles and repetitions to enhance the model's performance.

Figure 6 includes two chart that illustrate the impact of different parameters on the accuracy of an algorithm.

1. Top chart: This chart shows the relationship between Population Size and Accuracy. As the population size increases from 100 to 200, the accuracy improves from 99 to 100. However, beyond a population size of 200, the accuracy remains constant at 100. This indicates that increasing the population size up to a certain point can enhance accuracy, but further increases have no significant effect.

2. Bottom chart: This chart examines the effect of Mutation Probability on Accuracy. At low mutation probabilities (0.1 and 0.2), the accuracy is 98. However, when the mutation probability reaches 0.3, the accuracy increases to 100 and remains constant at higher values (up to 0.9). This shows that low mutation probabilities can reduce accuracy, but once a threshold is reached, the accuracy reaches its maximum value.

Conclusion: Both parameters (population size and mutation probability) have a direct impact on accuracy, but this effect is limited to a certain threshold, beyond which further changes do not influence the accuracy.

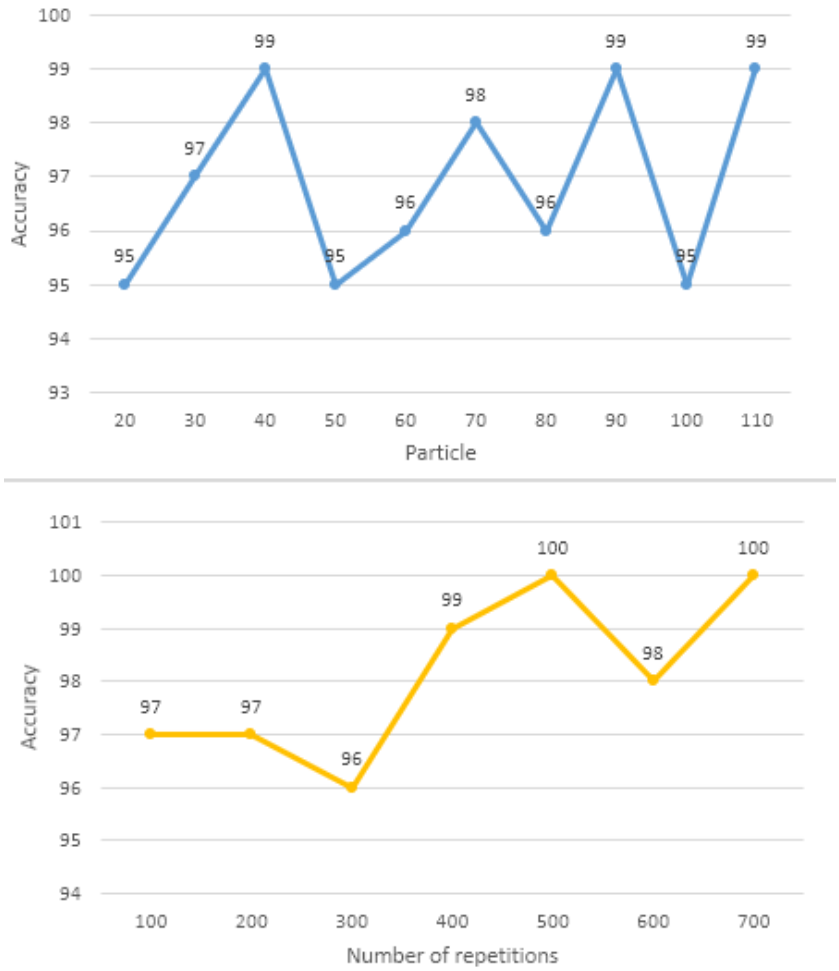


Figure 5: The model's performance based on variations in the number of particles and iterations for the PSO algorithm.

5 Conclusion

The graph-burning problem is a crucial topic within graph theory, with significant relevance in network science, especially in the context of weighted graphs. In this framework, networks are represented as graphs where the nodes symbolize entities and the edges signify connections with specific bandwidths, represented by weights that indicate the time it takes to transmit messages. The primary challenge lies in efficiently spreading a message from a central source to all nodes, either directly or through adjacent nodes, while minimizing the time required. This paper seeks to identify an optimal sequence that uses the least number of vertices for effective message dissemination in weighted graphs. Due to its NP-hard classification, this research adapts two evolutionary algorithms to discover optimal solutions and assess their relative effectiveness.

One potential direction for future work is to explore adaptations of the graph-burning problem for dynamic graphs, where nodes and edges may change over time. This approach could yield more robust solutions that better account for real-world scenarios in network communication. Additionally, extending the problem to consider multiple objectives—such as minimizing both the time taken and the number of nodes through which the central authority disseminates the message—could lead to more comprehensive solutions that align more closely with real-world constraints.

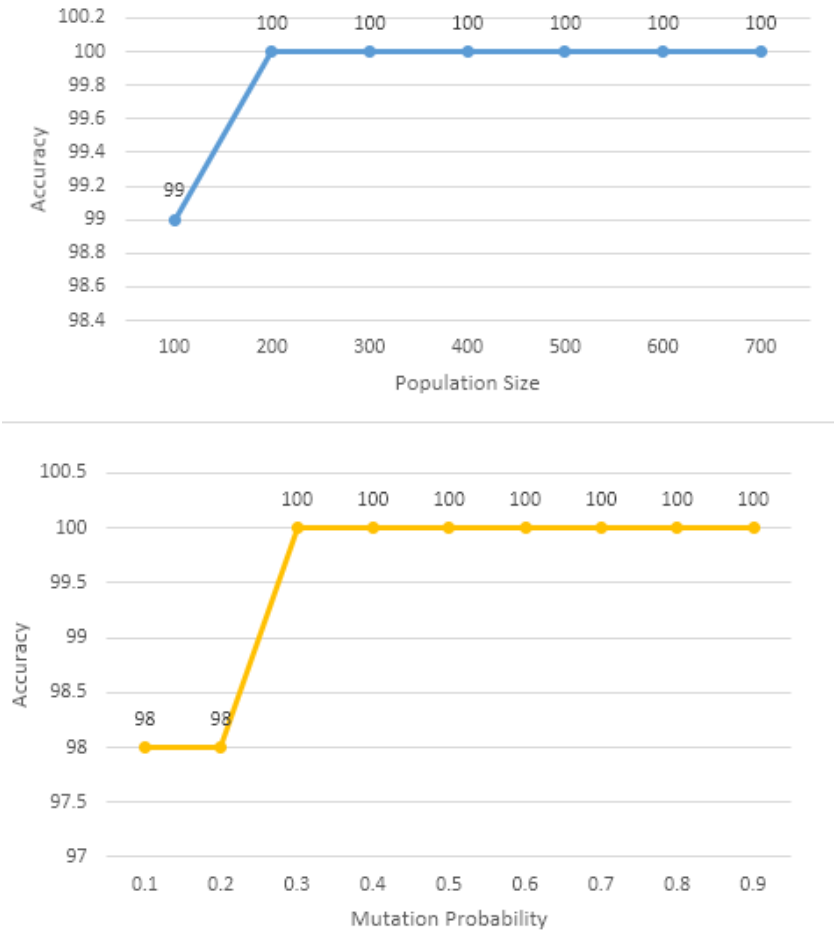


Figure 6: The impact of different parameters on the accuracy of the genetic algorithm.

References

[1] N. Alon, *Transmitting in the n-dimensional cube*, Discrete Applied Mathematics, 37-38(1992), pp.9—11, doi:10.1016/0166-218X(92)90121-P.

[2] A. Bonato, J. Janssen, and E. Roshanbin, *How to Burn a Graph*, Internet Mathematics, 12(2016), pp.85—100, doi:10.1080/15427951.2015.1103339.

[3] A. Bonato, J. Janssen, and E. Roshanbin, Burning a graph as a model of social contagion, In *International Workshop on Algorithms and Models for the Web-Graph*, Springer (2014), 13–22

[4] E. Roshanbin, *Burning a graph as a model for the spread of social contagion*, PhD thesis, Dalhousie University, Apr. 2016. URL: http://hdl.handle.net/10222/71417.

[5] A. Bonato, *A survey of graph burning*, Contributions to Discrete Mathematics 16, 1 (2021), pp.185—197.

[6] M. Nadjafikhah, M. Jafari, *Computation of partially invariant solutions for the einstein Walker manifolds' identifying equations*, Commun Nonlinear Sci Numer Simulat 18 (2013) 3317-3324.

[7] F. Topsze, *Topology and Measure*, Lecture Notes in Mathematics, Vol. 133, Springer, Berlin, 1970.

[8] Tanweer Alam, Shamimul Qamar, Amit Dixit, and Mohamed Benaida. *Genetic algorithm: Reviews, implementations, and applications*, arXiv preprint arXiv:2007.12673 (2020).

[9] Stéphane Bessy, Anthony Bonato, Jeannette Janssen, Dieter Rautenbach, and Elham Roshanbin. *Burning a graph is hard.*, Discrete Applied Mathematics 232 (2017), 73–87.

[10] Anthony Bonato and Shahin Kamali. 2019. *Approximation algorithms for graph burning.* In International Conference on Theory and Applications of Models of Computation. Springer, 74–92.

[11] Anthony Bonato and Thomas Lidbetter. 2019. *Bounds on the burning numbers of spiders and path-forests.* Theoretical Computer Science 794 (2019), 12–19.

[12] Ulrik Brandes. 2001. *A faster algorithm for betweenness centrality.* Journal of mathematical sociology 25, 2 (2001), 163–177.

[13] Ulrik Brandes and Christian Pich. 2007. *Centrality estimation in large networks.* International Journal of Bifurcation and Chaos 17, 07 (2007), 2303–2318.

[14] Zahra Rezai Farokh, Maryam Tahmasbi, Zahra Haj Rajab Ali Tehrani, and Yousof Buali. 2020. *New heuristics for burning graphs.* arXiv preprint arXiv:2003.09314 (2020).

[15] Rahul Kumar Gautam, Anjeneya Swami Kare, et al. 2022. *Faster heuristics for graph burning.* Applied Intelligence 52, 2 (2022), 1351–1361.

[16] Shahin Kamali, Avery Miller, and Kenny Zhang. 2020. *Burning two worlds.* In International Conference on Current Trends in Theory and Practice of Informatics. Springer, 113–124.

[17] Anjeneya Swami Kare and I Vinod Reddy. 2019. *Parameterized algorithms for graph burning problem.* In International Workshop on Combinatorial Algorithms. Springer, 304–314.

[18] Yasuaki Kobayashi and Yota Otachi. 2022. *Parameterized complexity of graph burning.* Algorithmica (2022), 1–15.

[19] Jure Leskovec and Andrej Krevl. 2014. SNAP Datasets: Stanford large network dataset collection.

[20] Sergey Norin and Jérémie Turcotte. 2022. *The Burning Number Conjecture Holds Asymptotically.* arXiv preprint arXiv:2207.04035 (2022).

[21] Ryan Rossi and Nesreen Ahmed. 2015. *The network data repository with interactive graph analytics and visualization.* In Twenty-ninth AAAI conference on artificial intelligence.

[22] Marek Šimon, Ladislav Huraj, Iveta Dirgová Luptáková, and Jiří Pospíchal. 2019. *Heuristics for spreading alarm throughout a network.* Applied Sciences 9, 16 (2019), 3269.

[23] Marek Šimon, Ladislav Huraj, Iveta Dirgová Luptáková, and Jiri Pospichal. 2019. *How to burn a network or spread alarm.* In MENDEL, Vol. 25. 11–18.

[24] SN Sivanandam and SN Deepa. 2008. *Genetic algorithms. In Introduction to genetic algorithms.* Springer, 15–37.

[25] Mahdi Nazeri, Ali Mollahosseini, Iman Izadi *CBAG: An Efficient Genetic Algorithm for the Graph Burning Problem* arXiv preprint arXiv:2208.01008v2 (2022)

Email: soheilshamaee@kashanu.ac.ir
Email: abbas.rahimi@grad.kashanu.ac.ir
Email: aghdaee80@std.kashanu.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

The weight spectrum of some classes of generalized Reed-Muller codes

Somayyeh Golalizadeh[1]
Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University, Tehran, Iran

Nasrin Soltankhah
Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University, Tehran, Iran

Abstract

In this paper, we determine the weight spectra of the generalized Reed-Muller codes $RM_q((m-2)(q-1)+b,m)$ for the cases $b=3,4$, $q=5,7$ and $m\geq 2$.

Keywords: Generalized Reed-Muller codes, Hamming weight, Weight spectrum

Mathematics Subject Classification [2010]: 13D45, 39B42

1 Introduction

Let p be a prime number, $n\geq 1$ an integer, $q=p^n$, F_q be the finite field with q elements and $m\geq 1$ an integer. We denote by B_m^q the F_q-algebra of the functions from F_q^m to F_q and by $F_q[x_1,\cdots,x_m]$ the F_q-algebra of polynomials in m variables with coefficients in F_q. Let r be an integer such that $1\leq r<m(q-1)$. The generalized Reed-Muller code of order r is the following subspace of the space $F_q^{q^m}$

$$RM_q(r,m)=\Big\{(f(x))_{x\in F_q^m}|f\in F_q[X_1,\cdots,X_m],\ deg(f)\leq r,\ \text{and}\ deg_{X_i}(f)<q\ \text{for}\ i=1,\cdots,m\Big\}$$

Here, $deg(f)$ denotes the total degree of f and $deg_{X_i}(f)$ is the X_i-degree of f.

Determining the Hamming weights of Reed-Muler codes has always been one of the most interesting research topic for many years. The weights of the Reed-Muller codes of length 2^m and orders $0,1,2,m-2,m-1,m$ are known. These weights equal $0,2^m$ for order 0, with additionally 2^{m-1} for the order 1, $2^{m-1}\pm 2^i$ where $\frac{m}{2}\leq i\leq m$ for the order 2, [4]. The weights in $RM_2(m,m)$ are all integers between 0 and 2^m since $RM_2(m,m)$ includes all vectors in $F_2^{2^m}$. The weights in $RM_2(m-1,m)$ are all even integers between 0 and 2^m and the weights in $RM_2(m-2,m)$ are all even integers between 0 and 2^m excluding 2 and 2^m-2. Recently, the authors in [1], determined the weights in $RM_2(m-3,m)$ for $m\geq 6$ and $RM_2(m-4,m)$ for $m\geq 8$. Unfortunately, there is not much information available on the weights of Reed-Muller codes for $q\geq 3$.

[1] speaker

2 Preliminaries and useful lemmas

The Hamming weight of an element $a = (a_1, a_2, \cdots, a_m) \in F_q^m$ is defined as the number of positions in which it is nonzero:

$$|(a_1, a_2, \cdots, a_m)| = ||i \in \{1, 2, \cdots, m\}|a_i \neq 0\}||$$

and it is denoted by $w_H(a)$. The set of all distinct Hamming weights (including the zero weight) is called the weight spectrum, i.e, if A_i is the number of codewords in a given code which have weight i, the weight spectrum of the code is just the set $\{i : A_i > 0\}$. In the throughout of paper, the symbol $wt(C)$ denotes the set of weights of the code C, i.e.

$$wt(C) = \{i \in N \cup \{0\}|\exists c \in C \;\; s.t. \;\; w_H(c) = i\}$$

We will use the following lemma to prove the results of this paper.

Lemma 2.1. *[5] Let r, m be integers such that $0 \leq r \leq m(q-1)$. Then*

$$wt(RM_q(m(q-1) - r - 1, m) \supseteq \bigoplus_{i=1}^{q} wt(RM_q((m-1)(q-1) - r - 1, m-1)).$$

3 Weight spectrum of $RM_q((m-2)(q-1)+3, m)$ when $q = 5, 7$

In this section, we provide some results on the weight spectrum of some families of Reed-Muler codes over the fields $\mathbb{F}_5$ and $\mathbb{F}_7$. In [1, 5], the authors determined the weight spectrum of some families of Reed-Muller codes over the field $\mathbb{F}_q$ for some q. We summarize a part of those results in the following theorems.

Theorem 3.1. *Let m be a positive integer, then*

1) *If $m \geq 6$, then $wt(RM_2(m-3, m)) = \{0, 2, 4, \cdots, 2^m\} \setminus \{2, 4, 6, 10, 2^m - 10, 2^m - 6, 2^m - 4, 2^m - 2\}$.*
2) *If $m \geq 8$, then $wt(RM_2(m-4, m)) = \{0, 16, 24, 28 + 2i, 2^m - 24, 2^m - 16, 2^m\}$ where i ranges over the set of consecutive integers from 0 to $2^{m-1} - 28$.*

Theorem 3.2. *Let m be a positive integer, then*

1) *If $m \geq 1$, then $wt(RM_3(2m-2, m)) = \{0, 3, 4, 5, \cdots, 3^m\}$.*
2) *If $m \geq 3$, then $wt(RM_3(2m-3, m)) \supseteq \{0, 6, 8, 9, \cdots, 3^m\}$.*
3) *If $m \geq 1$, then $wt(RM_5(4m-3, m)) = \{0, 4, 5, 6, \cdots, 5^m\}$.*

In the following theorem, we will determine all possible weights of a special class of Reed-Muller codes over the field $\mathbb{F}_5$.

Theorem 3.3. *For $m \geq 2$,*

$$wt(RM_5(4m-5, m)) = \{0, 10, 12, 13, 14, 15, \cdots, 5^m\}.$$

Proof. We proceed by induction on m. For $m = 2$ we get $RM_5(3, 2)$ whose weights belong to the set $\{0, 10, 12, 13, 14, 15, \cdots, 25\}$ and have been obtained with the aid of a python program.

Suppose now it is true for $m \geq 2$ and we want to prove the statement for $m + 1$. By Lemma 2.1 and induction hypothesis we have

$$\begin{aligned} wt(RM_5(4m-1, m+1) &\supseteq \bigoplus_{i=1}^{5} wt(RM_5(4m-5, m)) \\ &= \bigoplus_{i=1}^{5} \{0, 10, 12, 13, 14, \cdots, 5^m\}. \end{aligned}$$

Let $w \in \{0, 10, 12, 13, 14, \cdots, 5^{m+1}\}$, we need to prove that we can write w to the form $w = w_0 + w_1 + w_2 + w_3 + w_4$ in which $w_i \in \{0, 10, 12, 13, 14, \cdots, 5^m\}$ for $0 \leq i < 5$. By Euclidean division, w can be written to the form $w = k(5^m) + r$ with $0 \leq k \leq 5$ and $0 \leq r < 5^m$. The following three cases are distinguished.
Case 1: If $w \in \{0, 10, 12, 13, 14, \cdots, 5^m\}$, then we set $w_0 = w$ and $w_1 = \cdots = w_4 = 0$.
Case 2: If $w = k(5^m) + r$ with $1 \leq k \leq 5$ and $0 \leq r < 12$, we set the value of $k-1$ of w_i equal to 5^m, one of them $5^m - 12$, one equal to $r + 12$ and the rest of them equal to zero.
Case 3: If $w = k(5^m) + r$ with $1 \leq k \leq 4$ and $r \geq 12$, we set the value of k of w_i equal to 5^m, one equal to r and the rest of them equal to zero.
Finally, since the first, second and third minimum weight of $RM_5(4m-5, m)$ are equal to $10, 12, 13$, respectively, the proof is completed. □

In the following theorem, we try to recognize all possible weights of Reed-Muller code $RM_7(6m-9, m)$ and this purpose will be achieved except probably in a few special weights.

Theorem 3.4. *For $m \geq 2$,*

$$wt(RM_7(6m-9, m)) \supseteq \{0, 28, 30, 31, 34, 35, \cdots, 7^m\} \setminus \{50, 51, 52, 53, 54, 55, 57\}.$$

Proof. We prove the statement by induction on m. In the case $m = 2$ we get $RM_7(3, 2)$ whose weights belong to the set $\{0, 28, 30, 31, 34, 35, \cdots, 49\}$ and have been obtained with the aid of a python program.

Now, suppose that the claim is true for $m \geq 2$ and we want to prove the statement for $m+1$. By Lemma 2.1 and induction hypothesis we have

$$\begin{aligned} wt(RM_7(6m-3, m+1) &\supseteq \bigoplus_{i=1}^{7} wt(RM_7(6m-9, m)) \\ &\supseteq \bigoplus_{i=1}^{5} \{0, 28, 30, 31, 34, 35, \cdots, 7^m\} \setminus \{50, 51, 52, 53, 54, 55, 57\}. \end{aligned}$$

Let $w \in \{0, 28, 30, 31, 34, 35, \cdots, 7^{m+1}\} \setminus \{50, 51, 52, 53, 54, 55, 57\}$, we need to prove that we can write w to the form $w = w_0 + w_1 + \cdots + w_6$ in which $w_i \in \{0, 28, 30, 31, 34, 35, \cdots, 7^m\} \setminus \{50, 51, 52, 53, 54, 55, 57\}$ for $0 \leq i < 7$. By Euclidean division, w can be written to the form $w = k(7^m) + r$ with $0 \leq k \leq 7$ and $0 \leq r < 7^m$. The following two cases are distinguished.
Case 1: If $r \in \{0, 28, 30, 31, 34, 35, \cdots, 7^m\} \setminus \{50, 51, 52, 53, 54, 55, 57\}$, then we set the value of k of w_i equal to 7^m, one of them equal to r and the rest of them equal to zero.
Case 2: If $r \in \{1, 2, \cdots, 27, 29, 32, 33, \cdots, 50, 51, 52, 53, 54, 55, 57\}$, then we set the value of k of w_i equal to $7^m - x$, one of them equal to $kx + r$ in which $\lceil \frac{58-r}{k} \rceil \leq x \leq 7^m - 58$ and the rest of them equal to zero. □

4 Weight spectrum of $RM_q((m-2)(q-1)+4, m)$ when $q = 5, 7$

Theorem 4.1. *For $m \geq 2$,*

$$wt(RM_5(4m-4, m)) = \{0, 5, 8, 9, 10, 11, \cdots, 5^m\}.$$

Proof. We proceed by induction on m. For $m = 2$ we get $RM_5(4, 2)$ whose weights belong to the set $\{0, 5, 8, 9, 10, 11, \cdots, 25\}$ and have been obtained with the aid of a python program.

Suppose now it is true for $m \geq 2$ and we want to prove the statement for $m+1$. By Lemma 2.1 and induction hypothesis we have

$$\begin{aligned} wt(RM_5(4m, m+1) &\supseteq \bigoplus_{i=1}^{5} wt(RM_5(4m-4, m)) \\ &= \bigoplus_{i=1}^{5} \{0, 5, 8, 9, 10, 11, \cdots, 5^m\}. \end{aligned}$$

Let $w \in \{0, 5, 8, 9, 10, 11, \cdots, 5^{m+1}\}$, we need to prove that we can write w to the form $w = w_0 + w_1 + w_2 + w_3 + w_4$ in which $w_i \in \{0, 5, 8, 9, 10, 11, \cdots, 5^m\}$ for $0 \leq i < 5$. By Euclidean division, w can be written to the form $w = k(5^m) + r$ with $0 \leq k \leq 5$ and $0 \leq r < 5^m$. The following three cases are distinguished.
Case 1: If $w \in \{0, 5, 8, 9, 10, 11 \cdots, 5^m\}$, then we set $w_0 = w$ and $w_1 = \cdots = w_4 = 0$.
Case 2: If $w = k(5^m) + r$ with $1 \leq k \leq 5$ and $0 \leq r < 8$, we set the value of $k - 1$ of w_i's equal to 5^m, one of them $5^m - 8$, one equal to $r + 8$ and the rest of them equal to zero.
Case 3: If $w = k(5^m) + r$ with $1 \leq k \leq 4$ and $r \geq 8$, we set the value of k of w_i's equal to 5^m, one equal to r and the rest of them equal to zero.
Finally, since the first, second and third minimum weight of $RM_5(4m-5, m)$ are equal to $5, 8, 9$, respectively, the proof is completed. □

Theorem 4.2. *For $m \geq 2$,*

$$wt(RM_7(6m - 8, m)) = \{0, 21, 24, 25, 26, 27, \cdots, 7^m\}.$$

Proof. We proceed by induction on m. For $m = 2$ we get $RM_7(4, 2)$ whose weights belong to the set $\{0, 21, 24, 25, 26, 27, , \cdots, 49\}$ and have been obtained with the aid of a python program.

Suppose now it is true for $m \geq 2$ and we want to prove the statement for $m + 1$. By Lemma 2.1 and induction hypothesis we have

$$\begin{aligned} wt(RM_7(6m - 2, m + 1) &\supseteq \bigoplus_{i=1}^{7} wt(RM_7(6m - 8, m)) \\ &= \bigoplus_{i=1}^{7} \{0, 21, 24, 25, 26, 27, \cdots, 7^m\}. \end{aligned}$$

Let $w \in \{0, 21, 24, 25, 26, 27, \cdots, 7^{m+1}\}$, we need to prove that we can write w to the form $w = w_0 + w_1 + w_2 + w_3 + w_4 + w_5 + w_6$ in which $w_i \in \{0, 21, 24, 25, 26, 27, \cdots, 7^m\}$ for $0 \leq i < 7$. By Euclidean division, w can be written to the form $w = k(7^m) + r$ with $0 \leq k \leq 7$ and $0 \leq r < 7^m$. The following four cases are distinguished.
Case 1: If $w \in \{0, 21, 24, 25, 26, 27, \cdots, 7^m\}$, then we set $w_0 = w$ and $w_1 = \cdots = w_6 = 0$.
Case 2. If $w = k(7^m)$ with $1 \leq k \leq 7$, we set the value of k of w_i's equal to 7^m and the rest of them equal to zero.
Case 3: If $w = k(7^m) + r$ with $1 \leq k \leq 6$ and $1 \leq r < 24$, we set the value of $k - 1$ of w_i's equal to 7^m, one of them $7^m - 24$, one equal to $r + 24$ and the rest of them equal to zero.
Case 4: If $w = k(7^m) + r$ with $1 \leq k \leq 6$ and $r \geq 24$, we set the value of k of w_i's equal to 7^m, one equal to r and the rest of them equal to zero.
Finally, since the first, second and third minimum weight of $RM_7(6m - 8, m)$ are equal to $21, 24, 25$, respectively, the proof is completed. □

References

[1] C. Carlet, P. Solé, *The weight spectrum of two families of Reed-Muller codes*, Discrete Mathematics, (2023). hal-04127551

[2] D. Erickson, M. California *Institute of Technology. Division of Physics, Astronomy, Counting Zeros of Polynomials Over Finite Fields* (CIT thesis), California Institute of Technology, 1974.

[3] S. Golalizadeh, N. Soltankhah, *On the fourth weight of generalized Reed-Muller codes*, Des. Codes Cryptogr, **91**(2023), 3857-3879.

[4] F. J. MacWilliams, N. J. Sloane, *The theory of error-correcting codes*, North Holland, 1977.

[5] M. Shi, X. Li, A. Neri, P. Solé *How many weights can a cyclic code have?*, IEEE Transactions on Information Theory, **66(3)**(2019), 1449-1459.

Email: s.golalizadeh@gmail.com
Email: soltan@alzahra.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Calculation and comparison of topological indices of benzenoid systems

Zohreh Rajabinejad[1]
Department of Mathematics, Faculty of Mathematics, Statistics and Computer Science, Semnan University, Semnan, Iran

Saeed Mohammadian Semnani
Department of Mathematics, Faculty of Mathematics, Statistics and Computer Science, Semnan University, Semnan, Iran

Abstract

In this article, benzenoid systems are considered. The M-polynomial for the structures is obtained and using that polynomial, closed formulas for some degree-based indices are computed. These formulas are presented in terms of the number of hexagons in the base of the graph. Hence indices can be calculated without having to count the degrees of the vertices and partition the edges. Some topological indices of benzenoid graphs, such as triangular, rhombic, and hourglass benzenoids, are computed and compared. The results are displayed numerically and graphically.

Keywords: Molecular graph, Benzenoid systems, M-polynomial, Topological index.

AMS Mathematical Subject Classification [2010]: 05C09, 05C31, 05C90, 05C92

1 Introduction

Benzenoid systems are important structures in theoretical chemistry. A benzenoid system is an infinite hexagonal system or honeycomb network that has a finite and connected planar subgraph without cut vertices, and each interior face is a regular hexagon [2, 3]. These compounds, known as hydrocarbons, are composed primarily of carbon and hydrogen atoms and contain one or more benzene rings. Some of them are monocyclic, for example benzene (C_6H_6), which is the simplest member of the class, and some are polycyclic aromatic hydrocarbons (PAHs). These contain two or more fused benzene rings, for example, Pyrene ($C_{19}H_{12}$) with four fused benzene rings. In addition to the food industry, they can also be used as industrial solvents or as raw materials for the synthesis of various chemicals, including plastics, dyes, and pharmaceuticals. They are also of interest to many chemical and mathematical researchers due to their carcinogenicity and environmental hazards [2, 3].

Topological indices (Tl) are known for specifying the properties of chemical compounds [2]. Some Tls are used to predict the physical, chemical, and biological properties of benzenoid hydrocarbons. These indices,

[1]speaker

such as the Wiener index, Randic index, and Zagreb index can give insight into properties like boiling point, stability, and reactivity.

Tls are known as tools for predicting the chemical and biological properties of chemical structures and assessing the topological similarity between chemical structures [2, 4]. they are particularly helpful for isomer discrimination, structure–property relationships, structure–activity relationships, and drug design in chemistry, biochemistry, and nanotechnology [2]. Wiener first used Tls in 1947, which he named the Wiener index, and established that this index was closely correlated with alkane boiling points. In 1975, Randić introduced a graph parameter, now called the Randić index [5]. Gutman and Trinajstic introduced the first and second Zagreb index which provides quantitative measures of molecular branching [6, 7, 8]. Although hundreds of Tls have been built since 1947, the Wiener index, Randic index, Zagreb indices, and its versions are the most often used in chemical and mathematical literature. Among the oldest and most thoroughly studied structure-based topological descriptors with a variety of applications are the Zagreb and Randic indices [6, 7, 8, 2]. Some of the degree-based TIs are in Table 1 [9, 10, 11, 12, 13, 14, 15, 16, 17].

In mathematical chemistry, algebraic polynomials play an essential role in calculating Tls [18]. To simplify the calculation of indices, in 2015, Deutsch and Klavžar introduced a polynomial called the M-polynomial, which is written as [19, 20]:

$$M(G;x,y)=\sum_{\delta\leq i\leq j\Delta} m_{ij}(G)x^i y^j,$$

where $\delta = min\{d_v|v\in V(G)\}$, $\Delta = max\{d_v|v\in V(G)\}$, and $m_{ij}(G)$ is the number of edges $uv\in E(G)$ such that $\{d_u,d_v\}=\{i,j\}$, and d_u,d_v are the degree of vertices $u,v\in V(G)$. This polynomial is the most general algebraic polynomial for obtain a large number of degree-based Tls for a particular family of structures or networks [21].

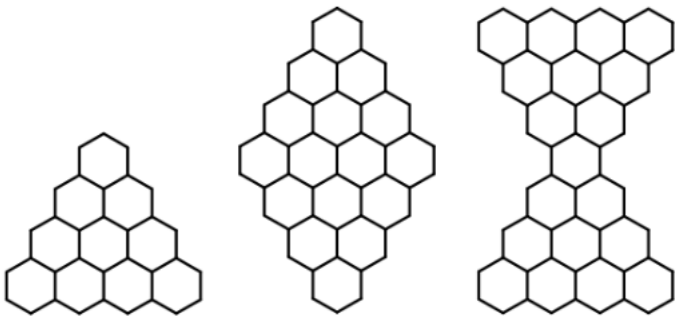


Figure 1: The banzenoid graphs T_r, R_r, and H_r from left to right.

In the next section, triangular, rhombic and hourglass benzenoids are investigated. The M-polynomials have been calculated for the structures. New formulas for First Zagreb, Second Zagreb, Hyper Zagreb, Modified Zagreb, Harmonic, Symmetric Division Deg, Inverse sum, Forgotten, Sigma, First Gourava, and Second Gourava indices are obtained. These formulas are in terms of the number of hexagons at the base of the graph. As a result, there is no need to count the degrees of the vertices and partitioning the edges to calculate these indices. Also, the relationship between the new formulas for the indices is found. The values of the indices for the benzenoid systems are calculated for 1 to ten. The results are displayed numerically and graphically.

2 Main results

In this article, T_r, R_r, and H_r are used to denote the r-dimensional triangular benzenoid, rhombic benzenoid, and hourglass benzenoid graphs, respectively. Figure 1 shows benzenoid graphs. The triangular benzenoids T_r are generalization of the benzene molecule C_6H_6 in which the hexagons are arranged in rows in a triangular benzenoid, and one hexagon growing in each row. In T_r, r is the number of hexagons in the base of graph. See Figure 1 [1]. T_r, has $|V(T_r)| = r^2 + 4r + 1$ vertices and $|E(T_r)| = \frac{3}{2}r(r+3)$ edges.

A benzenoid hourglass H_r is obtained from two copies of T_r by overlapping their extremal hexagons in the way shown in Figure 1. The number of vertices and edges of H_r is given by $|V(H_r)| = 2(r^2 + 4r - 2)$ and $|E(H_r)| = 3r^2 + 9r - 4$.

A benzenoid rhombus R_n is obtained from two copies of T_r by identifying hexagons in one of their base rows which is shown in Figure 1. Consequently, $|V(R_r)| = 2r(r+2)$ and $|E(R_r)| = 3r^2 + 4r - 1$ [3].

Edge partitioning of the T_r, H_r, and R_r graphs is given in Tables 1, 2, and 3. Table 4 shows the mathematical formula for the degree-based TIs used in this article and Table 5 includes some degree-based Tls computed via M-polynomial, where operators used are defined as:

$\mathrm{D}_x M(x,y) = x\frac{\partial M}{\partial x}$,
$D_y M(x,y) = y\frac{\partial M}{\partial y}$,
$S_x M(x,y) = \int_0^x \frac{M(t,y)}{t} d_t$,
$S_y M(x,y) = \int_0^y \frac{M(x,t)}{t} d_t$,
$JM(x,y) = M(x,x)$.

Table 1: Edge partition of T_r, when $r \geq 1$.

(d_u, d_v)	$(2,2)$	$(2,3)$	$(3,3)$	Total edges
Number of Edges	6	$6(r-1)$	$\frac{3}{2}r(r-1)$	$\frac{3}{2}r(r+3)$

Table 2: Edge partition of H_r, when $r \geq 2$.

(d_u, d_v)	$(2,2)$	$(2,3)$	$(3,3)$	Total edges
Number of Edges	8	$2(6r-8)$	$2 + 3r(r-1)$	$3(r^2+3r-2)$

Table 3: Edge partition of R_r, when $r \geq 1$.

(d_u, d_v)	$(2,2)$	$(2,3)$	$(3,3)$	Total edges
Number of Edges	6	$8(r-1)$	$3r^2 - 4r + 1$	$3r^2 + 4r - 1$

Table 4: Some degree-based topological indices.

Topological index	Mathematical formula
First Zagreb	$FZ(G) = \Sigma_{uv\in E(G)}\ (d_u + d_v)$
Second Zagreb	$SZ(G) = \Sigma_{uv\in E(G)}\ (d_u d_v)$
Hyper Zagreb	$HZ(G) = \Sigma_{uv\in E(G)}\ (d_u + d_v)^2$
Modified Zagreb	$MZ(G) = \Sigma_{uv\in E(G)}\ \frac{1}{d_u d_v}$
Harmonic	$H(G) = \Sigma_{uv\in E(G)}\ \frac{2}{d_u+d_v}$
Symmetric Division Deg	$SDD(G) = \Sigma_{uv\in E(G)}\ \frac{d_u^2+d_v^2}{d_u d_v}$
Inverse sum	$I(G) = \Sigma_{uv\in E(G)}\ \frac{d_u d_v}{d_u+d_v}$
Forgotten	$F(G) = \Sigma_{uv\in E(G)}\ d_u^2 + d_v^2$
Sigma	$\sigma(G) = \Sigma_{uv\in E(G)}\ (d_u - d_v)^2$
First Gourava	$Go_1(G) = \Sigma_{uv\in E(G)}\ (d_u + d_v + d_u d_v)$
Second Gourava	$Go_2(G) = \Sigma_{uv\in E(G)}\ (d_u^2 d_v + d_v^2 d_u)$

Table 5: Derivation of degree-based topological indices via M-polynomial.

Topological index	Derivative from $M(G;x,y)$
First Zagreb	$(D_x + D_y)M(T_r;x,y)\|_{x=y=1}$
Second Zagreb	$D_x D_y M(T_r;x,y)\|_{x=y=1}$
Hyper Zagreb	$D_x^2 JM(T_r;x,y)\|_{x=1}$
Modified Zagreb	$S_x S_y M(T_r;x,y)\|_{x=y=1}$
Harmonic	$2S_x JM(T_r;x,y)\|_{x=y=1}$
Symmetric Division Deg	$(D_x S_y + D_y S_x)M(T_r;x,y)\|_{x=y=1}$
Inverse sum	$S_x J D_x D_y M(T_r;x,y)\|_{x=1}$
Forgotten	$(D_x^2 + D_y^2)M(T_r;x,y)\|_{x=y=1}$
Sigma	$(D_x^2 + D_y^2 - 2D_x D_y)M(T_r;x,y)\|_{x=y=1}$
First Gourava	$(D_x + D_y + D_x D_x)M(T_r;x,y)\|_{x=y=1}$
Second Gourava	$(D_x^2 D_y + D_y^2 D_x)M(T_r;x,y)\|_{x=y=1}$

Theorem 2.1. *Consider T_r with $\frac{r(r+1)}{2}$ number of hexagons. Then its M-polynomial is as follows:*

$$M(T_r;x,y) = 6x^2y^2 + 6(r-1)x^2y^3 + \frac{3}{2}r(r-1)x^3y^3.$$

Proof. We can calculate the M-polynomial of T_r using Figure 1 and Table 1 as follows:

$$\begin{aligned} M(G;x,y) &= \sum_{\delta\le i\le j\le\Delta} m_{ij}(G)x^i y^j \\ &= m_{22}(G)x^2y^2 + m_{23}(G)x^2y^3 + m_{33}(G)x^3y^3 \\ &= 6x^2y^2 + 6(r-1)x^2y^3 + \frac{3}{2}r(r-1)x^3y^3. \end{aligned}$$

□

Theorem 2.2. *Let T_r, where $r \ge 1$. Then the following hold:*

(i) $FZ(T_r) = 9r^2 + 21r - 6$,

(ii) $SZ(T_r) = \frac{27}{2}r^2 + \frac{45}{2}r - 12$,

(iii) $SDD(T_r) = 3r^2 + 10r - 1$,

(iv) $MZ(T_r) = \frac{1}{2}r^2 + \frac{5}{6}r + \frac{1}{2}$,

(v) $H(T_r) = \frac{1}{2}r^2 + \frac{19}{10}r + \frac{3}{5}$,

(vi) $I(T_r) = \frac{9}{4}r^2 + \frac{99}{20}r - \frac{6}{5}$,

(vii) $\sigma(T_r) = 6(r-1)$,

(viii) $F(T_r) = 27r^2 + 51r - 30$,

(ix) $HZ(T_r) = 54r^2 + 96r - 54$,

(x) $GO_1(T_r) = \frac{45}{2}r^2 + \frac{87}{2}r - 18$,

(xi) $GO_2(T_r) = 81r^2 + 99r - 84$.

Proof. Let $M(T_r; x, y) = 6x^2y^2 + 6(r-1)x^2y^3 + \frac{3}{2}r(r-1)x^3y^3$. The following results are obtained by applying the operators on the M-polynomial.

$$
\begin{aligned}
D_xM(T_r; x, y) &= 12x^2y^2 + 12(r-1)x^2y^3 + \frac{9}{2}r(r-1)x^3y^3,\\
D_yM(T_r; x, y) &= 12x^2y^2 + 18(r-1)x^2y^3 + \frac{9}{2}r(r-1)x^3y^3,\\
S_xM(T_r; x, y) &= 3x^2y^2 + 3(r-1)x^2y^3 + \frac{1}{2}r(r-1)x^3y^3,\\
S_yM(T_r; x, y) &= 3x^2y^2 + 2(r-1)x^2y^3 + \frac{1}{2}r(r-1)x^3y^3,\\
S_xS_yM(T_r; x, y) &= \frac{3}{2}x^2y^2 + (r-1)x^2y^3 + \frac{1}{6}r(r-1)x^3y^3,\\
JM(T_r; x, y) &= 6x^4 + 6(r-1)x^5 + \frac{3}{2}r(r-1)x^6,\\
S_xJM(T_r; x, y) &= 3x^2y^2 + 3(r-1)x^2y^3 + \frac{1}{2}r(r-1)x^3y^3,\\
D_xD_yM(T_r; x, y) &= 24x^2y^2 + 36(r-1)x^2y^3 + \frac{27}{2}r(r-1)x^3y^3,\\
D_x^2D_yM((T_r; x, y) &= 48x^2y^2 + 72(r-1)x^2y^3 + \frac{81}{2}r(r-1)x^3y^3,\\
D_y^2D_xM(T_r; x, y) &= 48x^2y^2 + 108(r-1)x^2y^3 + \frac{81}{2}r(r-1)x^3y^3.
\end{aligned}
$$

Then due to Table 5, we conclude that

(*i*) $FZ(T_r) = (D_x + D_y)M(T_r; x, y)|_{x=y=1} = 9r^2 + 21r - 6$,
(*ii*) $SZ(T_r) = D_xD_yM(T_r; x, y)|_{x=y=1} = \frac{27}{2}r^2 + \frac{45}{2}r - 12$,
(*iii*) $SDD(T_r) = (D_xS_y + D_yS_x)M(T_r; x, y)|_{x=y=1} = 3r^2 + 10r - 1$,
(*iv*) $MZ(T_r) = S_xS_yM(T_r; x, y)|_{x=y=1} = \frac{1}{2}r^2 + \frac{5}{6}r + \frac{1}{2}$,
(*v*) $H(T_r) = 2S_xJM(T_r; x, y)|_{x=y=1} = \frac{1}{2}r^2 + \frac{19}{10}r + \frac{3}{5}$,
(*vi*) $I(T_r) = S_xJD_xD_yM(T_r; x, y)|_{x=1} = \frac{9}{4}r^2 + \frac{99}{20}r - \frac{6}{5}$,
(*vii*) $\sigma(T_r) = (D_x^2 + D_y^2 - 2D_xD_y)M(T_r; x, y)|_{x=y=1} = 6(r-1)$,
(*viii*) $F(T_r) = (D_x^2 + D_y^2)M(T_r; x, y)|_{x=y=1} = 27r^2 + 51r - 30$,
(*ix*) $HZ(T_r) = D_X^2JM(T_r; x, y)|_{x=1} = 54r^2 + 96r - 54$,

(x) $GO_1(T_r) = (D_x + D_y + D_xD_y)M(T_r; x, y)|_{x=y=1} = \frac{45}{2}r^2 + \frac{87}{2}r - 18$,
(xi) $GO_2(T_r) = (D_x^2D_y + D_y^2D_x)M(T_r; x, y)|_{x=y=1} = 81r^2 + 99r - 84$.

□

Theorem 2.3. *Consider H_r with $r(r+1)-1$ number of hexagons. Then its M-polynomial is as follows:*

$$M(H_r; x, y) = 8x^2y^2 + 2(6r-8)x^2y^3 + \big(2 + 3r(r-1)\big)x^3y^3.$$

Proof. We can calculate the M-polynomial of H_r using Figure 1 and Table 2 as follows:

$$\begin{aligned} M(G; x, y) &= \sum_{\delta \le i \le j \le \Delta} m_{ij}(G)x^iy^j = m_{22}(G)x^2y^2 + m_{23}(G)x^2y^3 + m_{33}(G)x^3y^3 \\ &= 8x^2y^2 + 2(6r-8)x^2y^3 + \big(2 + 3r(r-1)\big)x^3y^3. \end{aligned}$$

□

Theorem 2.4. *Let H_r, where $r \ge 2$. Then the following hold:*

(i) $FZ(H_r) = 18r^2 + 42r - 36$,

(ii) $SZ(H_r) = 27r^2 + 45r - 46$,

(iii) $SDD(H_r) = 6r^2 + 20r - \frac{44}{3}$,

(iv) $MZ(H_r) = \frac{1}{3}r^2 + \frac{5}{3}r - \frac{4}{9}$,

(v) $H(H_r) = r^2 + \frac{19}{5}r - \frac{26}{15}$,

(vi) $I(H_r) = \frac{9}{2}r^2 + \frac{99}{10}r - \frac{41}{5}$,

(vii) $\sigma(H_r) = 4(3r-4)$,

(viii) $F(H_r) = 54r^2 + 102r - 108$,

(ix) $HZ(H_r) = 108r^2 + 192r - 200$,

(x) $GO_1(H_r) = 45r^2 + 87r - 82$,

(xi) $GO_2(H_r) = 162r^2 + 198r - 244$.

Proof. Let $M(H_r; x, y) = 8x^2y^2 + 2(6r-8)x^2y^3 + \big(2 + 3r(r-1)\big)x^3y^3$. The following results are obtained

by applying the operators on the M-polynomial.

$$\begin{aligned}
&D_xM(H_r;x,y) = 16x^2y^2 + 4(6r-8)x^2y^3 + 3\big(2+3r(r-1)\big)x^3y^3,\\
&D_yM(H_r;x,y) = 16x^2y^2 + 6(6r-8)x^2y^3 + 3\big(2+3r(r-1)\big)x^3y^3,\\
&S_xM(H_r;x,y) = 4x^2y^2 + (6r-8)x^2y^3 + \frac{1}{3}\big(2+3r(r-1)\big)x^3y^3,\\
&S_yM(H_r;x,y) = 4x^2y^2 + \frac{2}{3}(6r-8)x^2y^3 + \frac{1}{3}\big(2+3r(r-1)\big)x^3y^3,\\
&S_xS_yM(H_r;x,y) = 2x^2y^2 + \frac{1}{3}(6r-8)x^2y^3 + \frac{1}{9}\big(2+3r(r-1)\big)x^3y^3,\\
&JM(H_r;x,y) = 8x^4 + 2(6r-8)x^5 + \big(2+3r(r-1)\big)x^6,\\
&S_xJM(H_r;x,y) = 2x^4 + \frac{2}{5}(6r-8)x^5 + \frac{1}{6}\big(2+3r(r-1)\big)x^6,\\
&D_xD_yM(H_r;x,y) = 32x^2y^2 + 12(6r-8)x^2y^3 + 9\big(2+3r(r-1)\big)x^3y^3,\\
&D_x^2D_yM((H_r;x,y) = 64x^2y^2 + 24(6r-8)x^2y^3 + 27\big(2+3r(r-1)\big)x^3y^3,\\
&D_y^2D_xM(H_r;x,y) = 64x^2y^2 + 36(6r-8)x^2y^3 + 27\big(2+3r(r-1)\big)x^3y^3.
\end{aligned}$$

Then due to Table 5, we conclude that

(*i*) $FZ(H_r) = (D_x+D_y)M(H_r;x,y)|_{x=y=1} = 18r^2+24r-36$,
(*ii*) $SZ(H_r) = D_xD_yM(H_r;x,y)|_{x=y=1} = 27r^2+45r-46$,
(*iii*) $SDD(H_r) = (D_xS_y+D_yS_x)M(H_r;x,y)|_{x=y=1} = 6r^2+20r-\frac{44}{3}$,
(*iv*) $MZ(H_r) = S_xS_yM(H_r;x,y)|_{x=y=1} = \frac{1}{3}r^2+\frac{5}{3}r-\frac{4}{9}$,
(*v*) $H(H_r) = 2S_xJM(H_r;x,y)|_{x=y=1} = r^2+\frac{19}{5}r-\frac{26}{15}$,
(*vi*) $I(H_r) = S_xJD_xD_yM(H_r;x,y)|_{x=1} = \frac{9}{2}r^2+\frac{99}{10}r-\frac{41}{5}$,
(*vii*) $\sigma(H_r) = (D_x^2+D_y^2-2D_xD_y)M(H_r;x,y)|_{x=y=1} = 4(3r-4)$,
(*viii*) $F(H_r) = (D_x^2+D_y^2)M(H_r;x,y)|_{x=y=1} = 54r^2+102r-108$,
(*ix*) $HZ(H_r) = D_X^2JM(H_r;x,y)|_{x=1} = 108r^2+192r-200$,
(*x*) $GO_1(H_r) = (D_x+D_y+D_xD_y)M(H_r;x,y)|_{x=y=1} = 45r^2+87r-82$,
(*xi*) $GO_2(H_r) = (D_x^2D_y+D_y^2D_x)M(H_r;x,y)|_{x=y=1} = 162r^2+198r-244$.

□

Theorem 2.5. *Consider R_r with r^2 number of hexagons. Then its M-polynomial is as follows:*

$$M(R_r;x,y) = 6x^2y^2 + 8(r-1)x^2y^3 + (3r^2-4r+1)x^3y^3.$$

Proof. We can calculate the M-polynomial of R_r using Figure 1 and Table 3 as follows:

$$\begin{aligned}
M(G;x,y) &= \sum_{\delta\le i\le j\le\Delta} m_{ij}(G)x^iy^j = m_{22}(G)x^2y^2 + m_{23}(G)x^2y^3 + m_{33}(G)x^3y^3\\
&= 6x^2y^2 + 8(r-1)x^2y^3 + (3r^2-4r+1)x^3y^3.
\end{aligned}$$

□

Theorem 2.6. *Let R_r, where $r \ge 1$. Then the following hold:*

(i) $FZ(R_r) = 18r^2 + 16r - 10$,

(ii) $SZ(R_r) = 27r^2 + 12r - 15$,

(iii) $SDD(R_r) = 6r^2 + \frac{28}{3}r - \frac{10}{3}$,

(iv) $MZ(R_r) = \frac{1}{3}r^2 + \frac{8}{9}r + \frac{5}{18}$,

(v) $H(R_r) = \frac{6}{5}r^2 + \frac{8}{5}r + \frac{1}{5}$,

(vi) $I(R_r) = \frac{9}{2}r^2 + \frac{18}{5}r - \frac{21}{10}$,

(vii) $\sigma(R_r) = 81r^2 - 100r + 19$,

(viii) $F(R_r) = 108r^2 - 40r - 20$,

(ix) $HZ(R_r) = 75r^2 + 100r - 79$,

(x) $GO_1(R_r) = 45r^2 + 28r - 25$,

(xi) $GO_2(R_r) = 162r^2 + 24r - 90$.

Proof. Let $M(R_r; x, y) = 6x^2y^2 + 8(r-1)x^2y^3 + (3r^2 - 4r + 1)x^3y^3$. The following results are obtained by applying the operators on the M-polynomial.

$$
\begin{aligned}
&D_xM(R_r; x, y) = 12x^2y^2 + 16(r-1)x^2y^3 + 3(3r^2 - 4r + 1)x^3y^3,\\
&D_yM(R_r; x, y) = 12x^2y^2 + 24(r-1)x^2y^3 + 3(3r^2 - 4r + 1)x^3y^3,\\
&S_xM(R_r; x, y) = 3x^2y^2 + 4(r-1)x^2y^3 + \frac{(3r^2 - 4r + 1)}{3}x^3y^3,\\
&S_yM(R_r; x, y) = 3x^2y^2 + \frac{8}{3}(r-1)x^2y^3 + \frac{(3r^2 - 4r + 1)}{3}x^3y^3,\\
&S_xS_yM(R_r; x, y) = \frac{3}{2}x^2y^2 + \frac{4}{3}(r-1)x^2y^3 + \frac{(3r^2 - 4r + 1)}{9}x^3y^3,\\
&JM(R_r; x, y) = 6x^4 + 8(r-1)x^5 + (3r^2 - 4r + 1)x^6,\\
&S_xJM(R_r; x, y) = \frac{3}{2}x^4 + \frac{8}{5}(r-1)x^5 + \frac{(3r^2 - 4r + 1)}{6}x^6,\\
&D_xD_yM(R_r; x, y) = 24x^2y^2 + 48(r-1)x^2y^3 + 9(3r^2 - 4r + 1)x^3y^3,\\
&D_x^2D_yM((R_r; x, y) = 48x^2y^2 + 96(r-1)x^2y^3 + 27(3r^2 - 4r + 1)x^3y^3,\\
&D_y^2D_xM(R_r; x, y) = 48x^2y^2 + 144(r-1)x^2y^3 + 27(3r^2 - 4r + 1)x^3y^3.
\end{aligned}
$$

Then due to Table 5, we conclude that

(i) $FZ(R_r) = (D_x + D_y)M(R_r; x, y)|_{x=y=1} = 18r^2 + 16r - 10$,
(ii) $SZ(R_r) = D_xD_yM(R_r; x, y)|_{x=y=1} = 27r^2 + 12r - 15$,
(iii) $SDD(R_r) = (D_xS_y + D_yS_x)M(R_r; x, y)|_{x=y=1} = 6r^2 + \frac{28}{3}r - \frac{10}{3}$,
(iv) $MZ(R_r) = S_xS_yM(R_r; x, y)|_{x=y=1} = \frac{1}{3}r^2 + \frac{8}{9}r + \frac{5}{18}$,
(v) $H(R_r) = 2S_xJM(R_r; x, y)|_{x=y=1} = \frac{6}{5}r^2 + \frac{8}{5}r + \frac{1}{5}$,
(vi) $I(R_r) = S_xJD_xD_yM(R_r; x, y)|_{x=1} = \frac{9}{2}r^2 + \frac{18}{5}r - \frac{21}{10}$,

(*vii*) $\sigma(R_r) = (D_x^2 + D_y^2 - 2D_xD_y)M(R_r; x, y)|_{x=y=1} = 81r^2 - 100r + 19$,
(*viii*) $F(R_r) = (D_x^2 + D_y^2)M(R_r; x, y)|_{x=y=1} = 108r^2 - 40r - 20$,
(*ix*) $HZ(R_r) = D_X^2 JM(R_r; x, y)|_{x=1} = 75r^2 + 100r - 79$,
(*x*) $GO_1(R_r) = (D_x + D_y + D_xD_y)M(R_r; x, y)|_{x=y=1} = 45r^2 + 28r - 25$,
(*xi*) $GO_2(R_r) = (D_x^2D_y + D_y^2D_x)M(R_r; x, y)|_{x=y=1} = 162r^2 + 24r - 90$.

□

Table 6: Computation of TIs of T_r.

r	FZ	SZ	SDD	MZ	H	I	σ	F	HZ	GO_1	GO_2
2	72	87	31	4.16	6.4	17.7	6	180	354	159	438
3	138	177	56	7.5	10.8	33.9	12	366	720	315	942
4	222	294	87	11.83	16.2	54.6	18	606	1194	516	1608
5	324	438	124	17.1667	22.6	79.8	24	900	1776	762	2436
6	444	609	167	23.5	30	109.5	30	1248	2466	1053	3426
7	582	807	216	30.8333	38.4	143.7	36	1650	3264	1389	4578
8	738	1032	271	39.1667	47.8	182.4	42	2106	4170	1770	5892
9	912	1284	332	48.5	58.2	225.6	48	2616	5184	2196	7368
10	1104	1563	399	58.8333	69.6	273.3	54	3180	6306	2667	9006

Table 7: Computation of TIs of H_r.

r	FZ	SZ	SDD	MZ	H	I	σ	F	HZ	GO_1	GO_2
2	120	152	49.3334	4.2233	9.8666	29.6	8	312	616	272	800
3	252	332	99.3334	7.5566	18.6666	62	20	684	1348	584	1808
4	420	566	161.3334	11.5566	29.4666	103.4	32	1164	2296	986	3140
5	624	854	235.3334	16.2233	42.2666	153.8	44	1752	3460	1478	4796
6	864	1196	321.3333	21.5556	57.0667	213.2	56	2448	4840	2060	6776
7	1140	1592	419.3333	27.5556	73.8667	281.6	68	3252	6436	2732	9080
8	1452	2042	529.3333	34.2222	92.6667	359	80	4164	8248	3494	11708
9	1800	2546	651.3333	41.5556	113.4667	445.4	92	5184	10276	4346	14660
10	2184	3104	785.3333	49.5556	136.2667	540.8	104	6312	12520	5288	17936

Table 8: Computation of TIs of R_r.

r	FZ	SZ	SDD	MZ	H	I	σ	F	HZ	GO_1	GO_2
2	94	117	39.33	3.39	8.2	23.1	143	332	421	211	606
3	200	264	78.66	5.94	15.8	49.2	448	832	896	464	1440
4	342	465	103.0003	9.1666	25.8	84.3	915	1548	1521	807	2598
5	520	720	193.3333	13.0556	38.2	128.4	1544	2480	2296	1240	4080
6	734	1029	268.6667	17.6111	53	181.5	2335	3628	3221	1763	5886
7	984	1392	356	22.8333	70.2	243.6	3288	4992	4296	2376	8016
8	1270	1809	455.3333	28.7222	89.8	314.7	4403	6572	5521	3079	10470
9	1592	2280	566.6667	35.2778	111.8	394.8	5680	8368	6896	3872	13248
10	1950	2805	690	42.5	136.2	483.9	7119	10380	8421	4755	16350

Corollary 2.7. *The relationships between TIs based on the degree of the benzenoid systems are as follows:*

Table 9: The relationships between topological indices of benzenoid systems:

$$\mathrm{FZ}(\mathrm{H}_r) = 2FZ(T_r) - 38r - 24 = FZ(R_r) - 12r - 26$$
$$\mathrm{SZ}(\mathrm{H}_r) = 2SZ(T_r) - 22 = SZ(R_r) + 33r - 31$$
$$\mathrm{SDD}(\mathrm{H}_r) = 2SDD(T_r) - \tfrac{38}{3} = SDD(R_r) + \tfrac{32}{3}r - \tfrac{42}{3}$$
$$\mathrm{MZ}(\mathrm{H}_r) = MZ(R_r) + \tfrac{7}{9}r - \tfrac{13}{18}$$
$$\mathrm{H}(\mathrm{H}_r) = 2H(T_r) - \tfrac{44}{15}$$
$$\mathrm{I}(\mathrm{H}_r) = I(R_r) + \tfrac{63}{10}r - \tfrac{42}{5} = 2I(T_r) - \tfrac{29}{5}$$
$$\sigma(H_r) = 2\sigma(T_r) - 4$$
$$\mathrm{F}(\mathrm{H}_r) = 2F(T_r) - 48 = \tfrac{F(R_r)}{2} + 122r - 98$$
$$\mathrm{HZ}(\mathrm{H}_r) = 2HZ(T_r) - 92$$
$$\mathrm{GO}_1(H_r) = 2GO_1(T_r) - 46 = GO_1(R_r) + 59r - 57$$
$$\mathrm{GO}_2(H_r) = 2GO_2(T_r) - 76 = GO_2(R_r) + 174r - 154$$

Proof. The relations in Table 9 are obtained by comparing the formulas obtained from theorems 2.2, 2.4, and 2.6. □

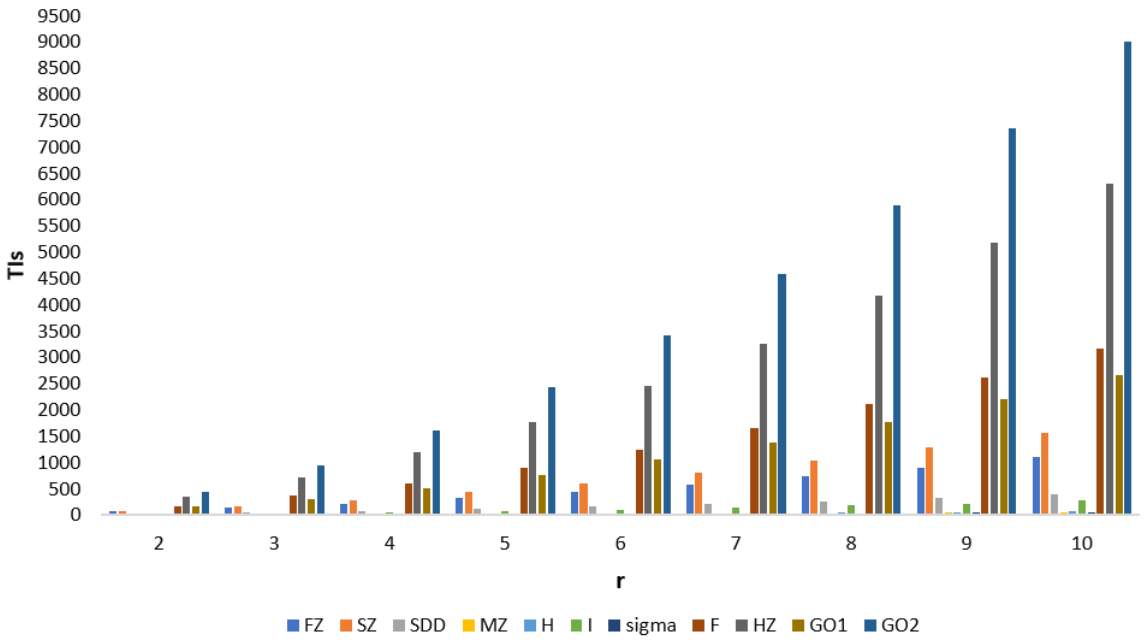


Figure 2: Comparison of topological indices for T_r.

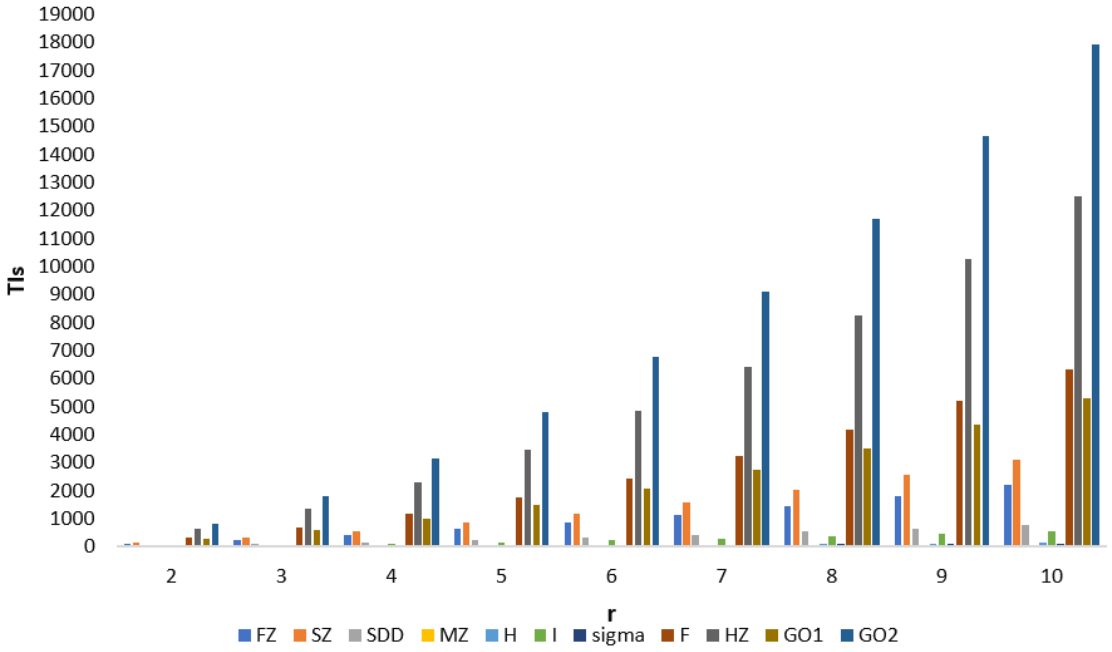


Figure 3: Comparison of topological indices for H_r.

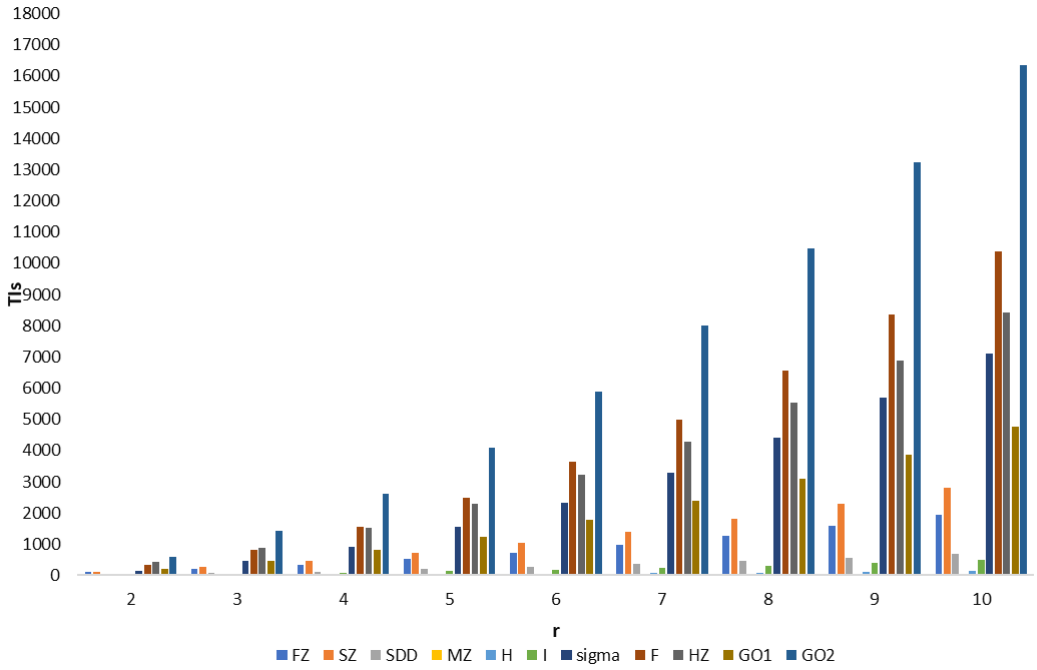


Figure 4: Comparison of topological indices for R_r.

3 Conclusion

The closed formulas for some degree-based indices for the benzenoid systems were obtained. They are presented based on the number of hexagons at the base of the graph so that the indices can be calculated without the need to count the degrees of the vertices and partition the edges. The numerical values of these TIs for triangular benzenoid, rhombic benzenoid, and hourglass benzenoid with the values of the variable

r ranging from 2 to 10 are shown in Tables 6, 7, and 8. As the value of r increases, it can be seen from Figures 2, 3, and 4 that all indices are increasing. Among the investigated indices for benzenoid systems, the MZ has the lowest value, and the GO_2 has the highest value. The relationships between the topological indices of benzenoid systems are shown in Table 9. The FZ, SZ, SDD, H, I, HZ, GO_1, and GO_2 indices have the highest value for the hourglass benzenoid and the lowest value for the triangular benzenoid. The σ and F indices have the highest and lowest values for the rhombic benzenoid and triangular benzenoid, respectively, and the MZ index has the highest value for the triangular benzenoid and the lowest value for the rhombic benzenoid.

References

[1] R. N. Raj, R. S. Rajan, H. Byeon, C. T. Nagaraj, and G. Kokila, On the metric dimension for the line graphs of hammer and triangular benzene structures, Math. Stat. 11 (2023) 953–959.

[2] K. Sharma, V. K. Bhat, J. B. Liu, Second leap hyper-Zagreb coindex of certain benzenoid structures and their polynomials, Computational and Theoretical Chemistry 1223 (2023) 114088.

[3] L. Amir, M. Saheli, Computing two types of geometric-arithmetic indices of some benzenoid graphs, J. Discrete Math Its App 8. 3 (2023) 171–175.

[4] E. Deutsch, S. Klavzar, M-polynomial and degree-based topological indices, arXiv preprint arXiv: 1407.1592 (2014).

[5] Y. Liang, B. Wu, General Randić indices of a graph and its line graph, Open Mathematics. 21(1), (2023) 20220611. doi: 10.1515/math-2022-0611.

[6] I. Gutman, K. C. Das, The first Zagreb index 30 years after, MATCH Commun, Math. Comput. Chem. 50 (2004) 83–92.

[7] I. Gutman, N. Trinajstić, Graph theory and molecular orbitals. Total π-electron energy of alternant hydrocarbons, Chem. Phys. Lett. 17 (1972) 535–538.

[8] I. Gutman, N. Trinajstic, C. F. Wilcox, Graph theory and molecular orbitals. XII. Acyclic polyenes, J. Chem. Phys. 62 (1975) 3399–3405.

[9] C. K. Gupta, V. Lokesha, S. B. Shwetha, P. S. Ranjini, On the symmetric division deg index of graph, Southeast Asian Bulletin of Mathematics 40 (2016) 41–51.

[10] L. Zhong, The harmonic index for graphs, Appl. Math. Lett. 25 (2012) 561–566.

[11] B. Furtula, I. Gutman, A forgotten topological index, J. Math. Chem. 53 (2015) 1184–1190.

[12] I. Gutman, M. Togan, A. Yurttas, A. S. Cevik, I. N. Cangul, Inverse problem for sigma index, MATCH Commun. Math. Comput. Chem. 79 (2018) 491–508.

[13] S. Fajtlowicz, On conjectures of Graffiti, Discrete Math. 72 (1988) 113–118.

[14] G. H. Shirdel, H. Rezapour, A. M. Sayadi, The Hyper-Zagreb index of graph operations, Iranian J. Math. Chem. 4 (2013) 213–220.

[15] V. R. Kulli, The gourava indices and coindices of graphs, Ann. Pure Appl. Math. 14 (2017) 33–38.

[16] H. Rezapour, R. Nasiri, S. Mousav, The hyper-Zagreb index of trees and unicyclic graphs, Iranian J. Math. Sci. Inf. 18 (2023) 41–54.

[17] Z. Rajabinejad, S. Mohammadian-Semnani, Calculation of topological indices based on the distance of polyacenes without edge counting, Polycyclic Aromatic Compounds (2023) 1–12, doi:10.1080/10406638.2023.2276244.

[18] M. Nadeem, M. A. Alam, N. Ali, M. I. Elashiry, An Algebraic Approach of Topological Indices Connected with Finite Quasigroups, J. Function Spaces. 14 (2024) 1948465.

[19] E. Deutsch, S. Klavžar, M-polynomial and degree-based topological indices, Iranian J. Math. Chem. 6 (2015) 93–102.

[20] M. Ajmal, W. Nazeer, M. Munir, S. M. Kang, C. Y. Jung, The M-Polynomials and topological indices of generalized prism network, Int. J. Math. Anal. 11 (2017) 293–303.

[21] R.S. Haoer, Topological indices of metal-organic networks via neighborhood M-polynomial, J. Discrete Math. Sci. Cryptogr. 24 (2), 369–390 (2021), doi:10.1080/09720529.2021.1888433.

e-mail: zohreh_rajabinejad@semnan.ac.ir
e-mail: s_mohammadian@semnan.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Calculation of degree-based and neighborhood degree sum-based topological indices of Hammer and its line graph.

Zohreh Rajabinejad[1]
Department of Mathematics, Faculty of Mathematics, Statistics and Computer Science, Semnan University, Semnan, Iran.

Saeed Mohammadian Semnani
Department of Mathematics, Faculty of Mathematics, Statistics and Computer Science, Semnan University, Semnan, Iran.

Abstract

The hammer n-dimensional structure H_n is obtained by terminating the ends of a linear polyacene of length n with two pyrene fragments. In this paper, a new version of Zagreb indices by replacing s_u with d_u in First Zagreb, Second Zagreb, Modified Zagreb, and Hyper Zagreb are introduced. Then on the hammer graph and its line graph, the general formulas for degree-based and neighborhood sum-based versions of First Zagreb, Second Zagreb, Modified Zagreb, and Hyper Zagreb indices are determined via M-polynomial and S-polynomial. These formulas are based on the length of the linear polyacene connecting the two pyrene fragments present in the hammer structure and do not require edge counting. The relationships between these topological indices are examined. Finally, degree-based and neighborhood sum-based versions of topological indices of the hammer graph and its line graph are compared numerically and graphically.

Keywords: Graph theory, M-polynomial, Topological index, Hammer n-dimensional, Line graph

AMS Mathematical Subject Classification [2010]: 05C09, 05C31, 05C90, 05C92, 05C76

1 Introduction

Chemical graph theory is a branch of graph theory that deals with the mathematical modeling of chemical phenomena [1, 2]. Molecular descriptors or topological indices are used to represent chemical structure numerically. They predict the physical, biological, and chemical properties of new structures obtained from a molecule or molecular compound. The ability of the TIs to predict the properties of molecules measures their quality [1]. TIs depend on the degree of a vertex, the distance between two vertices, the eigenvalues of the graph, etc [4].

The Zagreb indices were first introduced in 1972 by Gutman and Trinajst´c [2]. They closely correlate with the total π-electron energy of alternant hydrocarbons [2, 4]. The first Zagreb index, $M_1(G)$, is the sum

[1]speaker

of the squares of the degrees of the vertices. The second Zagreb index is the sum of the products of the degrees of adjacent vertices, which are defined as:

$$M_1(G) = \Sigma_{i=1}^{n} d_i^2 = \Sigma_{i\sim j}(d_i + d_j),$$
$$M_2(G) = \Sigma_{i\sim j} d_i d_j.$$

The modified second Zagreb index is as follows [5]:

$$M_2^*(G) = \Sigma_{i\sim j} \frac{1}{d_i d_j}.$$

The hyper-Zagreb index HZ was put forward in 2013 by Shirdel et al. and is defined as [3]:

$$HZ = \Sigma_{ij\in E(G)}(d_i + d_j)^2.$$

Using topological polynomials instead of calculating TIs facilitates the presentation of information about molecular graphs. Some topological polynomials include M, NM, SMP polynomials, etc.

The M-polynomial generates TIs based on degree. This polynomial was introduced in 2015 by Deutsch and Klavžar as follows:

$$M(G; x, y) = \sum_{\delta\leq i\leq j\leq\Delta} m_{ij}(G) x^i y^j,$$

where $\delta = min\{d_v | v \in V(G)\}$, $\Delta = max\{d_v | v \in V(G)\}$, and $m_{ij}(G)$ is the number of edges $uv \in E(G)$ such that $\{d_u, d_v\} = \{i, j\}$, and d_u, d_v are the degree of vertices $u, v \in V(G)$ [9].

The NM-polynomial depends on the sum of the degrees of adjacent vertices [6]. The SMP-polynomial is used to easily calculate Szeged, Mostar, and PI indices of graphs using partial derivatives [7, 8]. Recently, formulas have been obtained for calculating the TIs of some hydrocarbons, which can be calculated using the apparent property of the structure of the desired hydrocarbon without polynomial calculation [8].

This paper focuses on the first, second, hyper, and modified Zagreb indices and their neighborhood sum-based versions and calculates them for the hammer graph and its line graph. The general formulas offered are based on the length of the linear polyacene connecting two pyrene fragments in the hammer structure so that TIs are obtained without the need to count the degrees of vertices and partition the edges.

2 Main result

The hammer n-dimensional structure H_n is obtained by terminating the ends of a linear polyacene of length n with two pyrene fragments, see the hammer graph and its line graph in Figure 1. The structure H_n consists of $4n + 30$ vertices, $5n + 37$ edges and $n + 8$ hexagons [10]. The line graph of hammer LH_n contains $37 + 5n$ vertices and $58 + 8n$ edges. Edge partitioning of the H_n graph and its line graph LH_n are given in Tables 1 and 2, respectively. Table 3 shows the mathematical formula for the degree-based TIs used in this article and Table 4 includes some degree-based topological indices (TI) computed via M-polynomial.

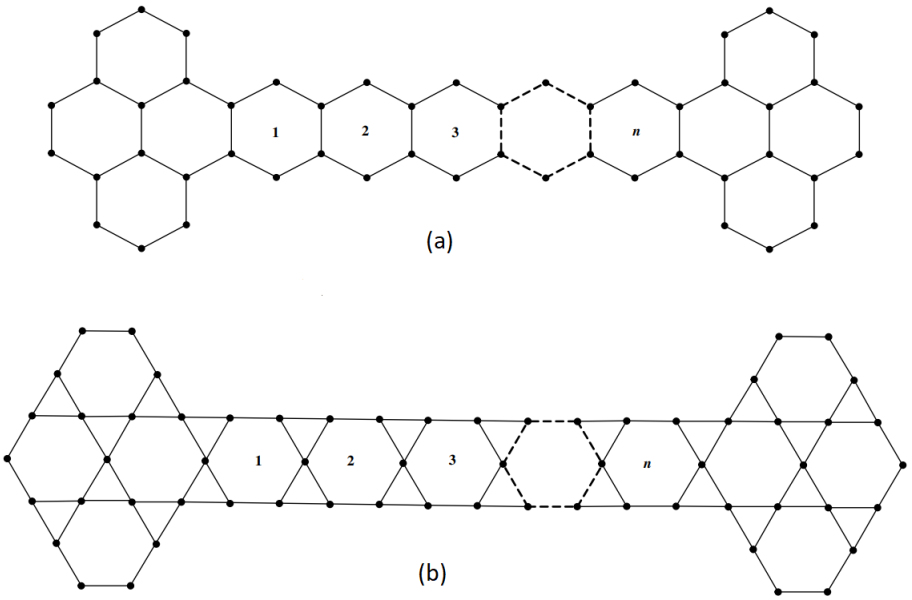


Figure 1: (a) Structure of hammer n-dimensional H_n, (b) Line graph of hammer n-dimensional LH_n.

Table 1: Partition of the edges of H_n.

Edges types	$\{2,2\}$	$\{2,3\}$	$\{3,3\}$
Number	10	$4n+12$	$n+15$

Table 2: Partition of the edges of LH_n.

Edges types	$\{2,2\}$	$\{2,3\}$	$\{3,3\}$	$\{3,4\}$	$\{4,4\}$
Number	4	12	$2+4n$	$20+4n$	20

Table 3: Degree-based topological indices.

Topological index	Mathematical formula
First Zagreb	FZ=$\Sigma_{uv\in E(G)} d_u + d_v$
Second Zagreb	SZ=$\Sigma_{uv\in E(G)} d_u d_v$
Hayper Zagreb	HZ=$\Sigma_{uv\in E(G)} (d_u + d_v)^2$
Modified Zagreb	MZ=$\Sigma_{uv\in E(G)} \frac{1}{d_u d_v}$

Table 4: Derivation of some TIs from M-polynomial.

Topological index	Derivative from $M(G;x,y)$
First Zagreb	$(D_x + D_y)M(G;x,y)\|_{x=y=1}$
Second Zagreb	$D_x D_y M(G;x,y)\|_{x=y=1}$
Hayper Zagreb	$D_x^2 JM(G;x,y)\|_{x=y=1}$
Modified Zagreb	$S_x S_y M(G;x,y)\|_{x=y=1}$

Definition 2.1. Let G be a chemical graph such that uv is the edge in edges set $E(G)$ then, the neighbor's degree sum of a vertex v denoted by s_v is the sum of all the degrees of the vertices adjacent to v, and it is

given as:

$$s_v = \Sigma_{uv \in E(G)} d_u,$$

where d_u is the degree of vertex u.

Definition 2.2. The S-polynomial is as follows:

$$S(G; x, y) = \sum_{\delta \leq i \leq j \Delta} S_{ij}(G) x^i y^j,$$

where $\delta = min\{s_v | v \in V(G)\}$, $\Delta = max\{s_v | v \in V(G)\}$, and $S_{ij}(G)$ is the number of edges $uv \in E(G)$ such that $\{s_u, s_v\} = \{i, j\}$.

The new Zagreb indices are calculated the neighborhood degree sum-based by substituting s_u for d_u in Fz, Sz, Mz, and Hz. These indices are given in Table 5.

Table 5: Neighborhood degree sum-based topological indices.

Topological index	Mathematical formula
Neighborhood degree sum-based First Zagreb	SFZ=$\Sigma_{uv \in E(G)} s_u + s_v$
Neighborhood degree sum-based Second Zagreb	SSZ=$\Sigma_{uv \in E(G)} s_u s_v$
Neighborhood degree sum-based Hyper Zagreb	SHZ=$\Sigma_{uv \in E(G)} (s_u + s_v)^2$
Neighborhood degree sum-based Modified Zagreb	SMZ=$\Sigma_{uv \in E(G)} \frac{1}{s_u s_v}$

Partitions of edges of H_n and LH_n based on the neighborhood sum degree of their end vertices are in Tables 6 and 7.

Table 6: Edges partition of H_n based on the neighborhood sum degree.

Edges types	$\{4,5\}$	$\{5,5\}$	$\{5,7\}$	$\{5,8\}$	$\{6,7\}$	$\{6,8\}$	$\{7,7\}$	$\{7,9\}$	$\{8,8\}$	$\{8,9\}$	$\{9,9\}$
Number	8	2	8	4	$4(n-1)$	4	$(n-1)$	4	6	4	2

Table 7: Edges partition of LH_n based on the neighborhood sum degree.

Edges types	$\{5,5\}$	$\{5,9\}$	$\{5,10\}$	$\{6,9\}$	$\{9,9\}$	$\{9,14\}$	$\{10,10\}$	$\{10,11\}$
Number	4	4	4	4	4	8	$4n-6$	4
Edges types	$\{10,12\}$	$\{10,14\}$	$\{10,15\}$	$\{11,14\}$	$\{14,14\}$	$\{14,15\}$	$\{14,16\}$	$\{15,16\}$
Number	$4(n-1)$	4	4	8	4	8	4	4

Theorem 2.3. *Let G be the base graph of H_n, where $n \geq 1$. Then the M-polynomial of G is as follows:*

$$M(G; x, y) = 10x^2y^2 + (4n+12)x^2y^3 + (n+15)x^3y^3.$$

Proof. Using Figure 1$-(a)$ and Table 1, the M-polynomial of G is calculated as follows:

$$\begin{aligned} M(G; x, y) &= \sum_{\delta \leq i \leq j \Delta} m_{ij}(G) x^i y^j = \sum_{2 \leq i \leq j \leq 3} m_{ij}(G) x^i y^j \\ &= m_{22}(G) x^2 y^2 + m_{23}(G) x^2 y^3 + m_{33}(G) x^3 y^3 \\ &= 10x^2y^2 + (4n+12)x^2y^3 + (n+15)x^3y^3. \end{aligned}$$

□

Proposition 2.4. *Let G be the graph of H_n, where $n \geq 1$. Then TIs of G are obtained as follows:*

- $FZ(G) = 26n + 190$,
- $SZ(G) = 33n + 247$,
- $HZ(G) = 136n + 10^3$,
- $MZ(G) = 0.5555n + 5.5$.

Proof. Let $M(G; x, y) = 10x^2y^2 + (4n + 12)x^2y^3 + (n + 15)x^3y^3$. The following results are obtained by applying the operators on the M-polynomial:

$$\begin{aligned}
D_xM(G; x, y) &= 20x^2y^2 + 2(4n + 12)x^2y^3 + 3(n + 15)x^3y^3,\\
D_yM(G; x, y) &= 20x^2y^2 + 3(4n + 12)x^2y^3 + 3(n + 15)x^3y^3,\\
D_xD_yM(G; x, y) &= 40x^2y^2 + 6(4n + 12)x^2y^3 + 9(n + 15)x^3y^3,\\
S_yM(G; x, y) &= 5x^2y^2 + \frac{4n + 12}{3}x^2y^3 + \frac{n + 15}{3}x^3y^3,\\
S_xS_yM(G; x, y) &= \frac{5}{2}x^2y^2 + \frac{4n + 12}{9}x^3y^3 + \frac{n + 15}{9}x^3y^3,\\
JM(G; x, y) &= 10x^4 + (4n + 12)x^5 + (n + 15)x^6,\\
D_x^2JM(G; x, y) &= 160x^4 + 25(4n + 12)x^5 + 36(n + 15)x^6.
\end{aligned}$$

Then due to Table 4, we conclude that:

- $FZ(G) = (D_x + D_y)M(G; x, y)|_{x=y=1} = 26n + 190$,
- $SZ(G) = D_xD_yM(G; x, y)|_{x=y=1} = 33n + 247$,
- $MZ(G) = S_xS_yM(G; x, y)|_{x=y=1} = \frac{5}{9}n + \frac{11}{2}$,
- $HZ(G) = D_x^2JM(G; x, y)|_{x=1} = 136n + 10^3$.

□

Theorem 2.5. *Let G be the base graph of H_n, where $n \geq 1$. Then the S-polynomial of G is as follows:*

$$\begin{aligned}
S(G; x, y) =& 8x^4y^5 + 2x^5y^5 + 8x^5y^7 + 4x^5y^8 + 4(n - 1)x^6y^7 + 4x^6y^8 + (n - 1)x^7y^7\\
&+ 4x^7y^9 + 6x^8y^8 + 4x^8y^9 + 2x^9y^9.
\end{aligned}$$

Proof. Using Figure 1$-(a)$ and Table 6, the S-polynomial of G is calculated as follows:

$$\begin{aligned}
S(G; x, y) &= \sum_{\delta \leq i \leq j \Delta} s_{ij}(G)x^iy^j = \sum_{4 \leq i \leq j \leq 9} s_{ij}(G)x^iy^j\\
&= s_{4,5}x^4y^5 + s_{5,5}x^5y^5 + s_{5,7}x^5y^7 + s_{5,8}x^5y^8 + s_{6,7}x^6y^7 + s_{6,8}x^6y^8 + s_{7,7}x^7y^7\\
&+ s_{7,9}x^7y^9 + s_{8,8}x^8y^8 + s_{8,9}x^8y^9 + s_{9,9}x^9y^9\\
&= 8x^4y^5 + 2x^5y^5 + 8x^5y^7 + 4x^5y^8 + 4(n - 1)x^6y^7 + 4x^6y^8 + (n - 1)x^7y^7\\
&+ 4x^7y^9 + 6x^8y^8 + 4x^8y^9 + 2x^9y^9.
\end{aligned}$$

□

Proposition 2.6. *Let G be the graph of H_n, where $n \geq 1$. Then TIs of G are obtained as follows:*

- $SFZ(G) = 66n + 494$,
- $SSZ(G) = 217n + 1711$,
- $SMZ(G) = 0.1156n + 1.0131$.
- $SHZ(G) = 872n + 6972$,

Proof. Let $S(G;x,y) = 8x^4y^5 + 2x^5y^5 + 8x^5y^7 + 4x^5y^8 + 4(n-1)x^6y^7 + 4x^6y^8 + (n-1)x^7y^7 + 4x^7y^9 + 6x^8y^8 + 4x^8y^9 + 2x^9y^9$. The following results are obtained by applying the operators on the S-polynomial:

$$\begin{aligned}
D_xS(G;x,y) &= 32x^4y^5 + 10x^5y^5 + 45x^5y^7 + 20x^5y^8 + 24(n-1)x^6y^7 + 24x^6y^8 + 7(n-1)x^7y^7 \\
&\quad + 28x^7y^9 + 48x^8y^8 + 32x^8y^9 + 18x^9y^9, \\
D_yS(G;x,y) &= 40x^4y^5 + 10x^5y^5 + 56x^5y^7 + 32x^5y^8 + 28(n-1)x^6y^7 + 32x^6y^8 + 7(n-1)x^7y^7 \\
&\quad + 36x^7y^9 + 48x^8y^8 + 36x^8y^9 + 18x^9y^9, \\
D_xD_yS(G;x,y) &= 160x^4y^5 + 50x^5y^5 + 280x^5y^7 + 160x^5y^8 + 168(n-1)x^6y^7 + 192x^6y^8 + 49(n-1)x^7y^7 \\
&\quad + 252x^7y^9 + 384x^8y^8 + 288x^8y^9 + 162x^9y^9, \\
S_yS(G;x,y) &= \frac{8}{5}x^4y^5 + \frac{2}{5}x^5y^5 + \frac{8}{7}x^5y^7 + \frac{1}{2}x^5y^8 + \frac{4}{7}(n-1)x^6y^7 + \frac{1}{2}x^6y^8 + \frac{1}{7}(n-1)x^7y^7 + \frac{4}{9}x^7y^9 \\
&\quad + \frac{3}{4}x^8y^8 + \frac{4}{9}x^8y^9 + \frac{2}{9}x^9y^9, \\
S_xS_yS(G;x,y) &= \frac{2}{5}x^4y^5 + \frac{2}{25}x^5y^5 + \frac{8}{35}x^5y^7 + \frac{1}{10}x^5y^8 + \frac{2}{21}(n-1)x^6y^7 + \frac{1}{12}x^6y^8 + \frac{1}{49}(n-1)x^7y^7 \\
&\quad + \frac{4}{63}x^7y^9 + \frac{3}{32}x^8y^8 + \frac{1}{18}x^8y^9 + \frac{2}{81}x^9y^9, \\
JS(G;x,y) &= 8x^9 + 2x^{10} + 8x^{12} + 4x^{13} + 4(n-1)x^{13} + 4x^{14} + (n-1)x^{14} + 4x^{16} + 6x^{16} + 4x^{17} + 2x^{18}, \\
D_x^2JS(G;x,y) &= 648x^9 + 200x^{10} + 1152x^{12} + 676x^{13} + 676(n-1)x^{13} + 784x^{14} + 196(n-1)x^{14} + 1024x^{16} \\
&\quad + 1536x^{16} + 1156x^{17} + 648x^{18}.
\end{aligned}$$

Then due to Table 4, we conclude that:

- $SFZ(G) = (D_x + D_y)M(G;x,y)|_{x=y=1} = 66n + 494$,
- $SSZ(G) = D_xD_yM(G;x,y)|_{x=y=1} = 217n + 1711$,
- $SMZ(G) = S_xS_yM(G;x,y)|_{x=y=1} = 0.1156n + 1.0131$,
- $SHZ(G) = D_x^2JM(G;x,y)|_{x=1} = 872n + 6972$.

□

Theorem 2.7. *Let G be the base graph of LH_n, where $n \geq 1$. Then the M-polynomial of G is as follows:*

$$M(G;x,y) = 4x^2y^2 + 12x^2y^3 + (2+4n)x^3y^3 + (20+4n)x^3y^4 + 20x^4y^4.$$

Proof. Using Figure 1−(*b*) and Table 2, the M-polynomial of LH_n is calculated as follows:

$$\begin{aligned} M(G;x,y) &= \sum_{\delta\le i\le j\Delta} m_{ij}(G)x^iy^j = \sum_{2\le i\le j4} m_{ij}(G)x^iy^j \\ &= m_{22}(G)x^2y^2 + m_{23}(G)x^2y^3 + m_{33}(G)x^3y^3 \\ &+ m_{34}(G)x^3y^4 + m_{44}(G)x^4y^4 \\ &= 4x^2y^2 + 12x^2y^3 + (2+4n)x^3y^3 + (20+4n)x^3y^4 + 20x^4y^4. \end{aligned}$$

□

Proposition 2.8. *Let G be the graph of LH_n, where $n \ge 1$. Then TIs of G are obtained as follows:*

- $FZ(G) = 52n + 388$,
- $SZ(G) = 84n + 666$,
- $HZ(G) = 340n + 2696$,
- $MZ(G) = \frac{7}{9}n + \frac{113}{36}$.

Proof. Let $M(G;x,y) = 4x^2y^2 + 12x^2y^3 + (2+4n)x^3y^3 + (20+4n)x^3y^4 + 20x^4y^4$. The following results are obtained by applying the operators on the M-polynomial:

$$\begin{aligned} D_xM(G;x,y) &= 8x^2y^2 + 24x^2y^3 + 3(2+4n)x^3y^3 + 3(20+4n)x^3y^4 + 80x^4y^4, \\ D_yM(G;x,y) &= 8x^2y^2 + 36x^2y^3 + 3(2+4n)x^3y^3 + 4(20+4n)x^3y^4 + 80x^4y^4, \\ D_xD_yM(G;x,y) &= 16x^2y^2 + 72x^2y^3 + 9(2+4n)x^3y^3 + 12(20+4n)x^3y^4 + 320x^4y^4, \\ S_yM(G;x,y) &= 2x^2y^2 + 4x^2y^3 + \frac{1}{3}(2+4n)x^3y^3 + (5+n)x^3y^4 + 5x^4y^4, \\ S_xS_yM(G;x,y) &= x^2y^2 + 2x^2y^3 + \frac{1}{9}(2+4n)x^3y^3 + \frac{1}{3}(5+n)x^3y^4 + \frac{5}{4}x^4y^4, \\ JM(G;x,y) &= 4x^4 + 12x^5 + (2+4n)x^6 + (20+4n)x^7 + 20x^8, \\ D_x^2JM(G;x,y) &= 64x^4 + 300x^5 + 36(2+4n)x^6 + 49(20+4n)x^7 + 1280x^8. \end{aligned}$$

Then due to Table 4, we conclude that:

- $FZ(G) = (D_x + D_y)M(G;x,y)|_{x=y=1} = 52n + 388$,
- $SZ(G) = D_xD_yM(G;x,y)|_{x=y=1} = 84n + 666$,
- $MZ(G) = S_xS_yM(G;x,y)|_{x=y=1} = \frac{7}{9}n + \frac{113}{36}$,
- $HZ(G) = D_x^2JM(G;x,y)|_{x=1} = 340n + 2696$.

□

Theorem 2.9. *Let G be the base graph of LH_n, where $n \ge 2$. Then the S-polynomial of G is as follows:*

$$\begin{aligned} S(G;x,y) &= 4x^5y^5 + 4x^5y^9 + 4x^5y^{10} + 4x^6y^9 + 4x^9y^9 + 8x^9y^{14} + (4n-6)x^{10}y^{10} + 4x^{10}y^{11} \\ &+ 4(n-1)x^{10}y^{12} + 4x^{10}y^{14} + 4x^{10}y^{15} + 8x^{11}y^{14} + 4x^{14}y^{14} + 8x^{14}y^{15} + 4x^{14}y^{16} + 4x^{15}y^{16}. \end{aligned}$$

Proof. Using Figure 1−(*b*) and Table 7, the S-polynomial of G is calculated as follows:

$$\begin{aligned}S(G;x,y) &= \sum_{\delta\leq i\leq j\leq\Delta} s_{ij}(G)x^iy^j = \sum_{5\leq i\leq j16} s_{ij}(G)x^iy^j\\ &= s_{5,5}(G)x^5y^5 + s_{5,9}(G)x^5y^9 + s_{5,10}(G)x^5y^{10} + s_{6,9}(G)x^6y^9 + s_{9,9}(G)x^9y^9 + s_{9,14}(G)x^9y^{14}\\ &+ s_{10,10}(G)x^{10}y^{10} + s_{10,11}(G)x^{10}y^{11} + s_{10,12}(G)x^{10}y^{12} + s_{10,14}(G)x^{10}y^{14} + s_{10,15}(G)x^{10}y^{15}\\ &+ s_{11,14}(G)x^{11}y^{14} + s_{14,14}(G)x^{14}y^{14} + s_{14,15}(G)x^{14}y^{15} + s_{14,16}(G)x^{14}y^{16} + s_{15,16}(G)x^{15}y^{16}\\ &= 4x^5y^5 + 4x^5y^9 + 4x^5y^{10} + 4x^6y^9 + 4x^9y^9 + 8x^9y^{14} + (4n-6)x^{10}y^{10} + 4x^{10}y^{11}\\ &+ 4(n-1)x^{10}y^{12} + 4x^{10}y^{14} + 4x^{10}y^{15} + 8x^{11}y^{14} + 4x^{14}y^{14} + 8x^{14}y^{15} + 4x^{14}y^{16} + 4x^{15}y^{16}.\end{aligned}$$

□

Proposition 2.10. *Let G be the graph of LH_n, where $n \geq 2$. Then neighborhood degree sum-based TIs of G are obtained as follows:*

- $SFZ(G) = 1332 + 168n$,
- $SSZ(G) = 7360 + 880n$,
- $SHZ(G) = 0.6591 + 0.07333n$,
- $SMZ(G) = 33052 + 3536n$.

Proof. Let $S(G;x,y) = 4x^5y^5 + 4x^5y^9 + 4x^5y^{10} + 4x^6y^9 + 4x^9y^9 + 8x^9y^{14} + (4n-6)x^{10}y^{10} + 4x^{10}y^{11} + 4(n-1)x^{10}y^{12} + 4x^{10}y^{14} + 4x^{10}y^{15} + 8x^{11}y^{14} + 4x^{14}y^{14} + 8x^{14}y^{15} + 4x^{14}y^{16} + 4x^{15}y^{16}$. The following results

are obtained by applying the operators on the S-polynomial:

$$\begin{aligned}
D_xS(G;x,y) =&20x^5y^5+20x^5y^9+20x^5y^{10}+24x^6y^9+36x^9y^9+72x^9y^{14}+10(4n-6)x^{10}y^{10}\\
&+40x^{10}y^{11}+40(n-1)x^{10}y^{12}+40x^{10}y^{14}+40x^{10}y^{15}+88x^{11}y^{14}+56x^{14}y^{14}\\
&+112x^{14}y^{15}+56x^{14}y^{16}+60x^{15}y^{16},\\
D_yS(G;x,y) =&20x^5y^5+36x^5y^9+40x^5y^{10}+36x^6y^9+36x^9y^9+112x^9y^{14}+10(4n-6)x^{10}y^{10}\\
&+44x^{10}y^{11}+48(n-1)x^{10}y^{12}+56x^{10}y^{14}+60x^{10}y^{15}+112x^{11}y^{14}+56x^{14}y^{14}\\
&+120x^{14}y^{15}+64x^{14}y^{16}+64x^{15}y^{16},\\
D_xD_yS(G;x,y) =&100x^5y^5+180x^5y^9+200x^5y^{10}+216x^6y^9+324x^9y^9+1008x^9y^{14}+100(4n-6)x^{10}y^{10}\\
&+440x^{10}y^{11}+480(n-1)x^{10}y^{12}+560x^{10}y^{14}+600x^{10}y^{15}+1232x^{11}y^{14}+784x^{14}y^{14}\\
&+1680x^{14}y^{15}+896x^{14}y^{16}+960x^{15}y^{16},\\
S_yS(G;x,y) =&\frac{4}{5}x^5y^5+\frac{4}{9}x^5y^9+\frac{2}{5}x^5y^{10}+\frac{4}{9}x^6y^9+\frac{4}{9}x^9y^9+\frac{4}{7}x^9y^{14}+\frac{1}{10}(4n-6)x^{10}y^{10}+\frac{4}{11}x^{10}y^{11}\\
&+\frac{1}{3}(n-1)x^{10}y^{12}+\frac{2}{7}x^{10}y^{14}+\frac{4}{15}x^{10}y^{15}+\frac{4}{7}x^{11}y^{14}+\frac{2}{7}x^{14}y^{14}+\frac{8}{15}x^{14}y^{15}+\frac{1}{4}x^{14}y^{16}\\
&+\frac{1}{4}x^{15}y^{16},\\
S_xS_yS(G;x,y) =&\frac{4}{25}x^5y^5+\frac{4}{45}x^5y^9+\frac{2}{25}x^5y^{10}+\frac{2}{27}x^6y^9+\frac{4}{81}x^9y^9+\frac{4}{63}x^9y^{14}+\frac{1}{100}(4n-6)x^{10}y^{10}\\
&+\frac{2}{55}x^{10}y^{11}+\frac{1}{30}(n-1)x^{10}y^{12}+\frac{1}{35}x^{10}y^{14}+\frac{2}{75}x^{10}y^{15}+\frac{4}{77}x^{11}y^{14}+\frac{1}{49}x^{14}y^{14}\\
&+\frac{4}{105}x^{14}y^{15}+\frac{1}{56}x^{14}y^{16}+\frac{1}{60}x^{15}y^{16},\\
JS(G;x,y) =&4x^{10}+4x^{14}+8x^{15}+4x^{18}+8x^{23}+(4n-6)x^{20}+4x^{21}+4(n-1)x^{22}+4x^{24}+12x^{25}\\
&+4x^{28}+8x^{29}+4x^{30}+4x^{31},\\
D_x^2JS(G;x,y) =&400x^{10}+784x^{14}+1800x^{15}+1296x^{18}+4232x^{23}+400(4n-6)x^{20}+1764x^{21}\\
&+1936(n-1)x^{22}+2304x^{24}+7500x^{25}+3136x^{28}+6728x^{29}+3600x^{30}+3844x^{31}.
\end{aligned}$$

Then due to Table 4, we conclude that:

- $SFZ(G) = (D_x + D_y)S(G;x,y)|_{x=y=1} = 1332 + 168n$,
- $SSZ(G) = D_xD_yS(G;x,y)|_{x=y=1} = 7360 + 880n$,
- $SMZ(G) = S_xS_yS(G;x,y)|_{x=y=1} = 0.6591 + 0.07333n$,
- $SHZ(G) = D_x^2JS(G;x,y)|_{x=1} = 33052 + 3536n$.

□

Corollary 2.11. *Using Propositions 2.4 and 2.6, the following holds:*

$$SFZ(H_n) - FZ(H_n) = 304 + 40n$$
$$SSZ(H_n) - SZ(H_n) = 1464 + 184n$$
$$SHZ(H_n) - HZ(H_n) = 5972 + 736n$$
$$SMZ(H_n) - MZ(H_n) = -4.4869 - 0.4399n.$$

Corollary 2.12. *Using Propositions 2.8 and 2.10, the following holds:*

$$SFZ(LH_n) - FZ(LH_n) = 944 + 116n$$
$$SSZ(LH_n) - SZ(LH_n) = 6694 + 796n$$
$$SHZ(LH_n) - HZ(LH_n) = 30356 + 3196n$$
$$SMZ(LH_n) - MZ(LH_n) = -2.4798 - 0.7044n.$$

Table 8: Calculation of FZ, SZ, HZ, MZ, SFZ, SSZ, SHZ, and SMZ indices of H_n.

n	1	2	3	4	5	6	7	8	9	10
FZ	216	242	268	294	320	346	372	398	424	450
SZ	280	313	346	379	412	445	478	511	544	577
MZ	6.0556	6.6111	7.1667	7.7222	8.2778	8.8333	9.3889	9.9444	10.5000	11.0556
HZ	1136	1272	1408	1544	1680	1816	1952	2088	2224	2360
SFZ	560	626	692	758	824	890	956	1022	1088	1154
SSZ	1928	2145	2362	2579	2796	3013	3230	3447	3664	3881
SMZ	1.1287	1.2443	1.3599	1.4755	1.5911	1.7067	1.8223	1.9379	2.0535	2.1691
SHZ	7844	8716	9588	10460	11332	12204	13076	13948	14820	15692

Table 9: Calculation of FZ, SZ, HZ, MZ, SFZ, SSZ, SHZ, and SMZ indices of LH_n.

n	1	2	3	4	5	6	7	8	9	10
FZ	440	492	544	596	648	700	752	804	856	908
SZ	750	834	918	1002	1086	1170	1254	1338	1422	1506
MZ	3.9167	4.6944	5.4722	6.2500	7.0278	7.8056	8.5833	9.3611	10.1389	10.9167
HZ	3036	3376	3716	4056	4396	4736	5076	5416	5756	6096
SFZ	1500	1668	1836	2004	2172	2340	2508	2676	2844	3012
SSZ	8240	9120	10000	10880	11760	12640	13520	14400	15280	16160
SMZ	0.7324	0.8058	0.8791	0.9524	1.0257	1.0991	1.1724	1.2457	1.3191	1.3924
SHZ	36588	40124	43660	47196	50732	54268	57804	61340	64876	68412

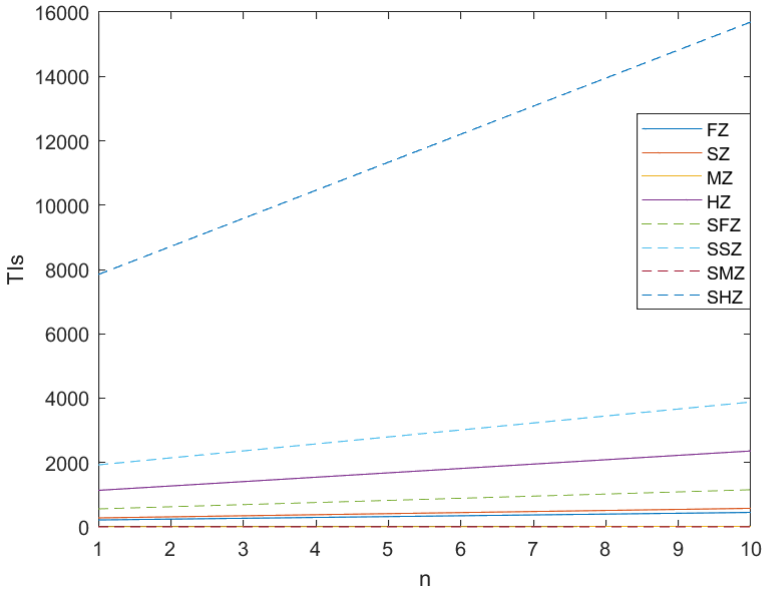


Figure 2: Comparison of FZ, SZ, HZ, MZ, SFZ, SSZ, SHZ, and SMZ indices of H_n.

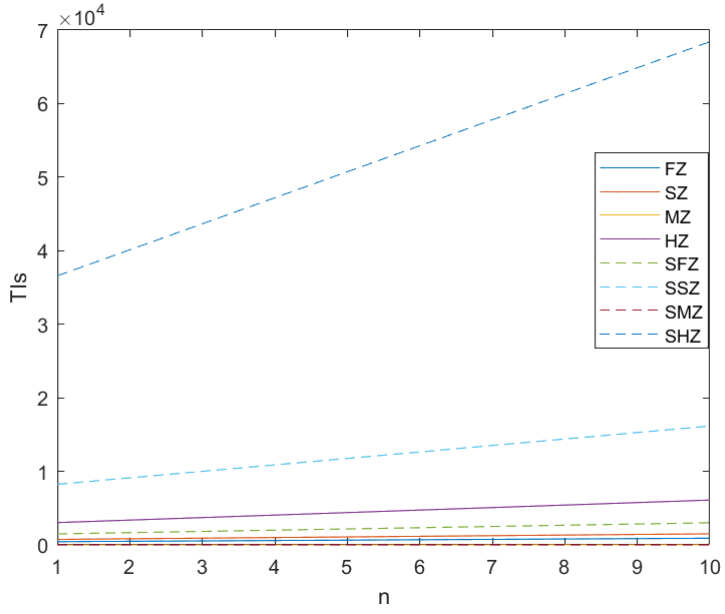


Figure 3: Comparison of FZ, SZ, HZ, MZ, SFZ, SSZ, SHZ, and SMZ indices of LH_n.

3 Conclusion

In this paper, new Zagreb indices were presented by replacing s_u with d_u in First Zagreb, Second Zagreb, Modified Zagreb, and Hyper Zagreb, in Table 5. Then, general formulas were obtained for FZ, SZ, MZ, HZ, and their new versions according to n, where n is the length of the linear polyacene connecting two pyrene fragments in the hammer structure. The relationship between these formulas was investigated. Also, the values of these indices were calculated to investigate the chemical properties and biological behavior of structures of H_n and LH_n for $n = 1, \ldots, 10$, see Tables 8 and 9.

Topological indices of the hammer graph and its line graph are compared numerically and graphically. According to Tables 8 and 9 and Figures 2 and 3, with the increase of n, the indices of both structures were increasing. For the hammer graph, the neighborhood degree sum-based topological indices have a higher value than the topological indices based on degree, except for the SMZ index. Its line graph also has similar conditions.

Among the investigated indices for the hammer graph and its line graph, SMZ and SHZ have the highest and lowest values, respectively. The SHZ and SMZ indices of the hammer line graph have the highest and lowest values in both the structure of the hammer and its line graph.

References

[1] Çolakoğlu, Özge, NM-polynomials and topological indices of some cycle-related graphs, Symmetry 14.8 (2022) 1706.

[2] W. Nazeer, M. Akmal, M. Imran, M. R. Farahani, H. Sector, On topological indices of line graph of subdivision of star and friendship graphs. International Journal of Pure and Applied Mathematics, 118(2) (2018) 413–417.

[3] S. Hayat, M. Adil Khan, Asad Khan, H. Jamil, M. Yasir, H. Malik, Extremal hyper-Zagreb index of trees of given segments with applications to regression modeling in QSPR studies, Alexandria Engineering Journal 80 (2023) 259–268.

[4] N. Akgunes, B. Aydin, Introducing new exponential Zagreb indices for graphs, Journal of Mathematics. 1 (2021), 6675321.

[5] A. Akbar, S. Stankov, E. Milovanović, M. Matejić, I. Milovanović, Bounds on the modified second Zagreb index, Discrete Applied Mathematics. 342 (2024) 385–390.

[6] Kumar, Santhosh, Bindhu K. Thomas, M-Polynomial and Degree based Topological Indices of Graphene, (2024).

[7] N, Tratnik, Žigert Pleteršek, P, Cut method for the multivariable Szeged-like polynomial with application to hyaluronic acid. International Journal of Quantum Chemistry, 124(1) (2024) e27252.

[8] Z. Rajabinejad, S. Mohammadian Semnani, Calculation of topological indices based on the distance of polyacenes without edge counting, Polycyclic Aromatic Compounds. 44, no. 9 (2024) 6302–6313.

[9] Z. Rajabinejad, S. Mohammadian Semnani, Calculation of topological indices based on M-polynomial for Polytrimethylene terephthalate, Journal of Discrete Mathematics and Its Applications. 9, no. 3 (2024) 181–190.

[10] Li, Yi-Xia, A. Rauf, M. Naeem, M. A. Binyamin, A. Aslam, Valency-Based Topological Properties of Linear Hexagonal Chain and Hammer-Like Benzenoid, Complexity 2021, no. 1 (2021) 9939469.

e-mail: zohreh_rajabinejad@semnan.ac.ir
e-mail: s_mohammadian@semnan.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A cryptosystem based on a hard graph problem[1]

Bahman Ahmadi[2]
Department of Mathematics, College of Science, Shiraz University, Shiraz, Fars, Iran
Majid Farhadi Sangdehi
Faculty of Mathematics and Computer Science, Damghan University, Damghan, Semnan, Iran

Abstract

Several public-key cryptosystems have been defined based on the hardness of some famous combinatorial problems. For a simple graph G, a *nowhere-zero k-flow* is an orientation of the edges of G along with an assignment of integer weights $\{\pm 1, \pm 2, \ldots, \pm(k-1)\}$ to the arcs in such a way that, at each vertex, the sum of the weights of the incoming arcs equals that of outgoing arcs. Finding the smallest such k has a similar nature to the problem of determining the chromatic number or the chromatic index of graphs. Therefore, it may be employed to serve as a graph theoretical hard problem in the heart of a cryptosystem. In this paper, we use the concept of nowhere-zero flows on graphs as the hard mathematical problem to construct a new cryptosystem.

Keywords: cryptography, graph, nowhere-zero flow
AMS Mathematical Subject Classification [2010]: 05C21,94A60,68P25

1 Introduction

The increasing demand for highly secure public-key cryptosystems has encouraged the cryptographers to develop new systems based on hard mathematical problems which would, most likely, resist against advanced cryptanalyses. However, very famous cryptosystems such as RSA and ElGamal whose securities rely on the difficulty of the problems of factoring large integers and finding discrete logarithms in finite groups, respectively, are seriously threatened by the development of quantum algorithms such as Shor's famous algorithm for factoring and Grover's quantum search algorithm. Therefore, one of the main objectives in the modern cryptography is to construct systems which would, hopefully, resist against quantum attacks.

One of the most interesting and well-known approaches to this problem is the so-called *lattice-based cryptography* which was first introduced by Ajtai in 1996 [2]. In this method, the security of the cryptosystem is based on the worst-case hardness of solving some *lattice problems*. After this invention, lattice-based cryptography attracted so much attention and many other lattice-based cryptosystems were introduced in order to improve the security and/or the practicality of the previous proposals. In contrast to the factoring problem, the attempts to devolve a quantum algorithm which can provide a significant speed up

[1] Will be presented in English
[2] speaker

in approximating the solutions of the lattice problems, have not yet been successful. This has led to the following conjecture.

Conjecture A. There is no polynomial time algorithm that approximates lattice problems to within polynomial factors.

This makes the lattice-based cryptography a very suitable candidate to resist against quantum attacks. The reader may refer to the survey [11] or the thesis [15] for detailed discussions about the subject. We also point out that there are some other candidates for the era of Post-Quantum Cryptography such as hash-based cryptography, code-based cryptography, multivariate-based cryptography and lattice-based cryptography; we refer the reader to the survey article [3] for a detailed review of the topic.

Another direction for introducing new public-key cryptosystems is to try to build the system based on hard combinatorial problems whose computational complexities have been thoroughly understood. Graph theory, in particular, is a rich source of such problems. It is well-known that the graph theoretical problems such as finding a proper vertex coloring, finding a maximum independent set and determining whether Hamiltonian paths/cycles exists in a simple graph, are NP-hard (the last one being even NP-complete). This would, therefore, entice cryptographers to introduce "graph-based" cryptosystems. The reader may see the references such as [6, 10, 12, 13] for some attempts on this subject.

For a simple graph G, a *nowhere-zero k-flow* is an orientation of the edges of G along with an assignment of integer weights $\{\pm 1, \pm 2, \ldots, \pm(k-1)\}$ to the arcs in such a way that, at each vertex, the sum of the weights of the incoming arcs equals that of outgoing arcs. This concept, which was first studied by Tutte in 1954, generalizes the theorems about face coloring of planar graphs to general graphs (see for instance Theorem 2.1). It has been the source of many interesting problems some of which still remain unsolved. Finding the smallest such k has been of great importance and has a similar nature to the problem of determining the chromatic number or the chromatic index of graphs. Therefore, it may be employed to serve as a graph theoretical hard problem in the heart of a cryptosystem.

In this paper, we introduce a new encryption scheme based on the problem of finding minimal nowhere-zero flows on graphs. We first present a brief background on the concept of nowhere-zero flows in Section 2. The structure of the proposed cryptosystem is, then, described in Section 3. Next, we present an example and some discussions about the practicality of the system in Section 4 and then describe a sample implementation of the system. We finally conclude the paper with some further remarks and open questions in Section 5. We assume the reader is familiar with the basic terminology of cryptography and graph theory. For detailed studies on these subjects, the reader may refer to the books [8] and [5], respectively.

2 Nowhere-Zero Flows

In this section we provide a brief overview of the concept of nowhere-zero flows (NZF). For more detailed discussions we refer the reader to [9], [1] and the references therein. Throughout the paper all the graphs are assumed to be simple (no loops or multiple edges are allowed), connected and undirected, unless otherwise declared.

Let $G = (V, E)$ be a graph and $k \geq 2$ be an integer. A nowhere-zero k-flow on G is a pair (D, f), where D is an orientation on the edges of G and $f : E \to \{\pm 1, \pm 2, \ldots, \pm(k-1)\}$ is a function which assigns the weights $\{\pm 1, \pm 2, \ldots, \pm(k-1)\}$ to the edges of G, in such a way that at any vertex $v \in V$, the sum of the

weights of the arcs leaving v is equal to the sum of the weights of the arc entering v. In other words, for any $v \in V$,

$$\sum_{e:\text{ leaving } v} f(e) = \sum_{e:\text{ entering } v} f(e).$$

Note that changing the direction of any arc e and at the same time negating its weight $f(e)$, will result in a new nowhere-zero k-flow. Therefore, if for an orientation D on the graph G, there is a nowhere-zero k-flow (D, f), then for any other orientation D' on G, there also exists a nowhere-zero k-flow. In other words, the nowhere-zero k-flows on a graph, do not really depend on the orientation and, hence, this concept essentially deals with the undirected graphs rather than digraphs.

It can, also, be shown that if there exist a nowhere-zero k-flow on a graph G, then G cannot have a cut edge; i.e. G must be 2-connected (recall the assumption of connectivity of the graphs). Hence, in the rest of the paper, the assumption is that the graphs are 2-edge connected. The smallest integer k for which a given graph G admits a nowhere-zero k-flow is called the *flow number* of G and is denoted by $\phi(G)$. If no such k exists, we write $\phi(G) = \infty$.

The following Theorem due to Tutte, shows the connection between the concept of nowhere-zero flows and the face coloring of the planar graphs.

Theorem 2.1. *Any planar graph G has a nowhere-zero k-flow if and only if G is k-face colorable.* □

It is well-known that the face coloring of a planar graph is equivalent to the vertex coloring of its *dual* graph. Hence Theorem 2.1 implies that finding minimal nowhere-zero k-flows in the relatively small family of planar graphs, is as hard as the problem of finding a minimal proper k-vertex coloring of the graphs in this family; see [7] for more details on the computational complexities of graph colorings. Therefore, the NZF problem (i.e. the problem of finding a minimal nowhere-zero k-flow on the given graph), in general, is as hard as the problem of determining the chromatic number of graphs. In other words, it is not hard to see the following.

Corollary 2.2. *For a given graph G, the problem of finding a nowhere-zero k-flow, where k is minimal, is NP-hard.* □

A very natural question that raises in the theory of nowhere-zero flows is whether for all graphs G, we have $\phi(G) < \infty$. This was Tutte's motivation for proposing his famous "5-flow conjecture" in 1954:

Tutte's Conjecture. For any graph G, we have $\phi(G) \leq 5$.

The conjecture is still open, but in 1981, Seymour [14] solved the problem with $k = 6$:

Theorem 2.3. *For any graph G, we have $\phi(G) \leq 6$.* □

In addition, one can make the bound even better by putting further conditions on the graphs. For example, it can be easily shown that if all the vertices of the graph have even degrees (i.e. if the graph is *even*), then the graph has a nowhere-zero 2-flow:

Lemma 2.4. *For any graph G, $\phi(G) = 2$ if and only if G is even.* □

Although there is no classification of the graphs whose flow number is ≥ 3, the following list of results can be useful in determination of the flow number of graphs.

Theorem 2.5. *Any 3-regular graph G has a nowhere-zero 3-flow if and only if G is bipartite.* □

Theorem 2.6. *Any graph G has a nowhere-zero 4-flow if and only if G is the union of two even graphs.* □

Theorem 2.7. *Any 3-regular graph G has a nowhere-zero 4-flow if and only if G is 3-edge colorable.* □

Theorem 2.8. *Any 4-edge connected graph has a nowhere-zero 4-flow.* □

There are, also, many other attempts that help to determine the flow number of the graphs which have some structures, some of which provide methods for constructing desired flows. As we will discuss in Section 5, however, these structured graphs are not suitable for our purpose in this paper. In other words, we will be looking for the graphs which are as unstructured as possible so that finding the minimal flows is "sufficiently hard".

3 The NZF-Based Cryptosystem

In this section we describe a public-key cryptosystem based on the nowhere-zero flows on graphs. As for the security parameters, we choose large enough integers n and R, and a large enough real number $\alpha > 0$.

Alice, first, constructs a 2-edge-connected graph $G = (V, E)$ with $V = \{v_1, \ldots, v_n\}$ and $E = \{e_1, \ldots, e_m\}$ such that the flow number $\phi(G) = k > 2$. Next she builds a nowhere-zero k-flow (D, f) on G (see Section 4 for some notes about finding an NZF). Note that according to Lemma 2.4, G cannot be an even graph and, therefore, building a k-flow will not be easy, which makes the system secure, as discussed later in this section. Note also that by switching the direction of an edge and negating its assigned weight, if necessary, we can always assume that all the weights are positive. Let M be the *incidence* matrix of G with respect to the orientation D; that is, let M be an $n \times m$ matrix whose rows and columns are indexed by the vertices and the edges of G, respectively, such that

$$M_{(i,j)} = \begin{cases} 1, & \text{if in } D, \text{the arc } e_j \text{ leaves } v_i, \\ -1, & \text{if in } D, \text{the arc } e_j \text{ enters } v_i, \\ 0, & \text{otherwise.} \end{cases}$$

We define a column vector $\mathbf{z} \in (\mathbb{Z}^+)^m$ as $\mathbf{z}^\top = [f(e_1), \ldots, f(e_m)]$ and call it the *flow vector* of (D, f). It follows from the definition of the nowhere-zero flows that $M\mathbf{z} = \mathbf{0}$. Also, if we let $N = M^\top M$, then $N\mathbf{z} = \mathbf{0}$. The $m \times m$ matrix N has all its diagonal entries equal to 2 and all the other entries are either 0, -1 or 1. Now, Alice publishes the matrix N as her public key and keeps the nowhere-zero k-flow (D, f), or equivalently, the vector $\mathbf{z}$ as her secret key.

In order to send a message $\mathbf{m} \in \{0, 1\}^m$ to Alice, Bob first chooses an $m \times m$ matrix L, whose entries are all selected uniformly at random from the $\{0, \pm 1, \ldots, \pm\alpha\}$, for some fixed integer α. He, also, picks up a random $m \times m$ permutation matrix P. Then, he computes the ciphertext as

$$C = LN + P + kD,$$

where $D = \text{diag}(\mathbf{m})$ is the $m \times m$ diagonal matrix whose diagonal is $\mathbf{m}$.

On the other hand, in order to decrypt Bob's cipher text C, Alice first calculates

$$\mathbf{m}' = \lfloor \frac{1}{k} C\mathbf{z} \rfloor,$$

where for a vector $\mathbf{x} = (x_1, \ldots, x_s)$, by $\lfloor \mathbf{x} \rfloor$ we mean the vector $(\lfloor x_1 \rfloor, \ldots, \lfloor x_s \rfloor)$. Alice, then, recovers $\mathbf{m}$ from $\mathbf{m}'$ by simply changing all nonzero elements of $\mathbf{m}'$ to 1. We summarize the NZF-based cryptosystem as follows:

NZF-Based Cryptosystem:

- **Key Generation:** Choose the security parameters n and α; build a 2-edge-connected graph $G = (V, E)$ with $V = \{v_1, \ldots, v_n\}$ and $E = \{e_1, \ldots, e_m\}$ such that the flow number $\phi(G) = k > 2$; build a nowhere-zero k-flow (D, f) on G with the flow vector $\mathbf{z}$; then calculate the matrix N as above. The public key is N while the private key is $\mathbf{z}$.

- **Encryption:** To encrypt the vector $\mathbf{m} \in \{0, 1\}^m$, choose a random (ephemeral) $m \times m$ matrix L, with integer entries $\ell_{i,j}$, where $|\ell_{i,j}| \leq \alpha$; generate a random $m \times m$ permutation matrix P; construct the $m \times m$ diagonal matrix D, with diagonal $\mathbf{m}$, and finally compute the ciphertext $C = LN + P + kD$.

- **Decryption:** To decrypt the received ciphertext C, calculate the vector $\mathbf{m}' = \lfloor \frac{1}{k} C\mathbf{z} \rfloor$, and retrieve $\mathbf{m}$ from $\mathbf{m}'$ by changing any nonzero component to 1.

To see why the system is valid, we first observe that, since $\mathbf{z}$ is in the null-space of N, we have

$$\mathbf{m}' = \lfloor \frac{1}{k} C\mathbf{z} \rfloor = \lfloor \frac{1}{k} LN\mathbf{z} + \frac{1}{k} P\mathbf{z} + D\mathbf{z} \rfloor = \lfloor \frac{1}{k} P\mathbf{z} \rfloor + D\mathbf{z} = D\mathbf{z}.$$

Note that the last equation follows if and only if $\mathbf{z}$ is the vector of a nowhere-zero k-flow on G (and that it may not hold if $\mathbf{z}$ is the vector of a nowhere-zero k'-flow, with $k' > k$). This, along with the fact that $\mathbf{z}$ has all nonzero entries, shows that the decrypted vector is the same as $\mathbf{m}$.

For an adversary, Eve, to recover the message from the cipher text C, there are two main obstacles. The randomly chosen security matrix L, which is different for each message, sufficiently masks the message vector $\mathbf{m}$, so that recovering the vector from C without knowing $\mathbf{z}$ is sufficiently computationally "hard". If, on the other hand, Eve decides to guess the structure of the secret flow vector $\mathbf{z}$, according to Corollary 2.2, it would amount to solving a combinatorial NP-hard.

4 Implementation and The Practical Point of View

In this section we illustrate the NZF-based cryptosystem by a small example and discuss about some practical aspects of the system. We further describe a real implementation of the system.

We first choose the security parameters as $n = 7$ and $\alpha = 10$. As for her public key, Alice chooses the graph G depicted in Figure 1.

This is a 2-connected graph which, according to Lemma 2.4 does not admit a nowhere-zero 2-flow. Hence $\phi(G) > 2$. She then builds a nowhere-zero 3-flow (D, f) on G as shown in Figure 2, indicating that $\phi(G) = k = 3$. Next she obtains the incidence matrix of the flow as

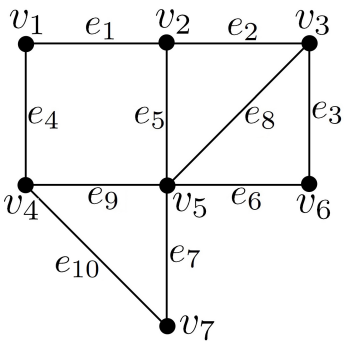


Figure 1: Alice's graph G

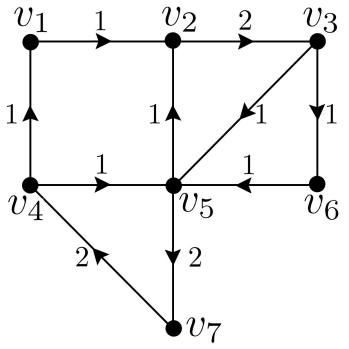


Figure 2: A nowhere-zero 3-flow on G

$$M = \begin{array}{c|cccccccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} \\ \hline v_1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ v_2 & -1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ v_3 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ v_4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & -1 \\ v_5 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 & -1 & 0 \\ v_6 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ v_7 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \end{array}.$$

It then follows that

$$N = M^\top M = \begin{bmatrix} 2 & -1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & -1 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 & 2 & -1 & 1 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 & -1 & 2 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 2 & -1 & -1 & -1 \\ 0 & -1 & 1 & 0 & -1 & 1 & -1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 1 & -1 & 1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & -1 & 2 \end{bmatrix}.$$

Alice publishes the matrix N as her public key and keeps the flow vector

$$\mathbf{z} = [1, 2, 1, 1, 1, 1, 2, 1, 1, 2]^\top$$

as her private key.

Now suppose Bob decides to send the message $\mathbf{m} = [0, 1, 0, 0, 1, 0, 1, 0, 1, 1]^\top$ to Alice. He first chooses his ephemeral matrix L as follows

$$L = \begin{bmatrix} -7 & 2 & -3 & -9 & 5 & -7 & 0 & 3 & -7 & -3 \\ 9 & -1 & 7 & 8 & -7 & 4 & -9 & -10 & 6 & -2 \\ 7 & 6 & 3 & 2 & 6 & 4 & 4 & -10 & -4 & -9 \\ -7 & 8 & -4 & -7 & 2 & -6 & -2 & -2 & 3 & 4 \\ 6 & 4 & 5 & -7 & 9 & 5 & -4 & 0 & -9 & -9 \\ 2 & -10 & -7 & -8 & -7 & 5 & 6 & -3 & -9 & -9 \\ 3 & -6 & 9 & 2 & 3 & -1 & -7 & 6 & 0 & -7 \\ 5 & -10 & -4 & -3 & -7 & 9 & -5 & 1 & -10 & 4 \\ 10 & 0 & 2 & 2 & 1 & -10 & -10 & 4 & -8 & -2 \\ 3 & 9 & 4 & -2 & 8 & -3 & 8 & -9 & 9 & 1 \end{bmatrix}.$$

He, then picks up the permutation matrix P as the matrix corresponding to the permutation $\sigma = (1,3,9,4,5)(2,8,10,6,7)$ and then computes the ciphertext as

$$\begin{aligned} C =& LN + P + kD \\ =& LN + P + 3\,\mathrm{diag}(0,1,0,0,1,0,1,0,1,1) \\ =& \begin{bmatrix} -2 & 6 & 3 & -15 & 12 & -20 & 19 & -18 & -29 & 10 \\ 4 & 2 & 1 & 15 & -13 & 13 & -23 & 15 & 32 & -9 \\ 12 & 6 & -14 & 2 & 27 & -19 & 33 & -33 & -12 & -20 \\ -13 & 27 & -12 & -8 & -7 & -7 & -1 & -19 & -13 & 14 \\ 25 & -12 & 1 & -20 & 23 & -9 & 14 & -8 & -16 & 2 \\ 15 & -5 & -12 & -18 & 11 & 6 & 22 & -6 & -14 & -7 \\ 13 & -32 & 31 & 8 & 3 & -1 & -6 & 30 & 18 & -9 \\ 16 & -15 & -6 & -25 & -4 & 25 & -21 & 19 & -5 & 27 \\ 19 & -17 & 18 & -11 & 16 & -17 & -3 & 1 & -6 & 12 \\ 7 & 12 & -7 & 1 & 21 & -25 & 26 & -33 & -13 & -10 \end{bmatrix}. \end{aligned}$$

Upon receiving Bob's ciphertext C, Alice simply calculates

$$\mathbf{m}' = \lfloor \frac{1}{k} C\mathbf{z} \rfloor = [0,2,0,0,1,0,2,0,1,2]^\top,$$

from which she recovers the original message $\mathbf{m}$.

This is, of course, a very simple example of the system and does not meet efficient security requirements. The graph G must include a "large" number of vertices and edges so that even strong algorithms of finding NZFs fail to generate suitable flows in a practical time. Choosing large and dense graphs as well as higher security parameters R and α will, certainly, affect the practicality of the system. In particular, they will increase both the encryption time and the memory space required for the operations. Similar to the other cryptosystem, though, one usually prefers to pay such costs in order to attain a sufficiently secure cryptosystem.

In what follows we describe a sample implementation of the system. First we note that if C is the cycle $x_1 - x_2 - \cdots - x_n - x_1$, then we can orient the edges as $x_1 \to x_2 \to \cdots \to x_n \to x_1$ and assign any fixed positive integer weight to all the arcs. This shows that we can build a nowhere zero k-flow on any graph which is a union of disjoint cycles (such as the complete graphs K_{2n+1}), for any $k \geq 2$. Also, it is easy to construct 4-flows on K_4. Furthermore, by a little trial and error we can see that the Petersen graph P admits a nowhere-zero 5-flow; see Figure 3. On the other hand, it is well-known that P is not 3-edge-colorable. This, along with Theorem 2.7 shows that P cannot have a smaller flow; i.e. $\phi(P) = 5$. Finally, we observe that if two graphs G and G' have nowhere-zero k-flows, then the graph obtained by identifying a vertex from G and a vertex from G' will, also, admit a nowhere-zero k-flow. This will help Alice to build arbitrarily large and unstructured graphs with the desired flow on them. For instance we have tried the graph G_{57} shown in Figure 4 which has $n = 57$ vertices and $m = 125$ edges. This graph has been constructed by consecutively identifying some vertices from graphs K_3, K_4, C_4, K_5 and P, and then making disjoint cycles using some of remaining vertices of those graph (the edges of which are pale in the figure). Using the facts mentioned

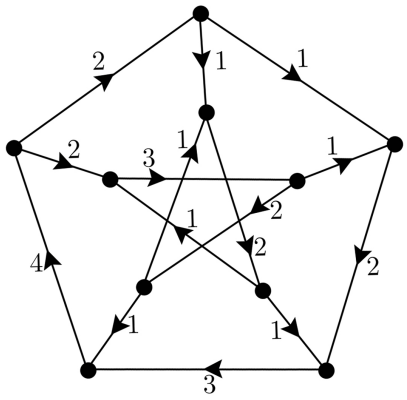


Figure 3: A 5-flow on the Petersen graph

above we could easily build a nowhere-zero 5-flow (with positive weights) on G_{57} showing that $\phi(G_{57}) = 5$. We also choose the security parameters as $R = 6$ and $\alpha = 10$. Having entered these data in the MAPLE software on our PC with a quad-core 3GHz processor, the encryption process for each binary message (of size 125) is performed in a split of a second.

5 Discussion

Based on the difficulty of finding a nowhere-zero k-flow on the 2-edge connected graphs (where $k > 2$), we constructed a public-key cryptosystem in which the public key consist of a large simple graph along with an orientation of its edges and where the private key is a nowhere-zero k-flow on the graph, where k is minimal. We, then, described a sample way for real life implementation. We conclude the article with some remarks and open questions.

First we note that, based on the results mentioned in Section 2, finding nowhere-zero k-flows on some graphs are relatively easier thanks to some graph theoretical structures on those graphs. This means that Alice should be careful not to choose the graph G from those families of graphs and should design a graph which is as random and unstructured as possible. For example, she should avoid the planar graphs. In a proof of Theorem 2.1 due to Younger, given a proper k-face coloring of the planar graph G, an easy way for constructing a nowhere-zero k-flow is presented (see for example [1] for the details of this proof). It is, on the other hand, well-known that every planar graph is 4-face colorable (the 4-color Theorem). Hence if G is a 2-edge connected planar graph, one can build a nowhere-zero k-flow on G (with $k \leq 4$) using a proper k-face coloring of G. The 3-flow in Figure 1 is obtained using the same method since G is planar; this is one of the reasons that the small example of Section 4 is not secure.

The next comment is about the security of the presented cryptosystem. As mentioned in Section 1, the advent of the quantum algorithm threatens the security of the "number -theoretic" cryptosystems such as RSA, and that the lattice-based cryptography is a decent candidate to resist against these threats. We point out that at the present time have been no quantum algorithms which can efficiently speed up the classic algorithms for solving the graph coloring problem. See for example the attempt in [4]. This motivates us to conjecture that the "graph-coloring-based" cryptosystems, such as our NZF-based scheme, are also good candidates for post-quantum cryptography.

We conclude with some open question. The practicality of the proposed system should be closely investigated. More specifically, some detailed analysis of the time and space required for encryption/decryption

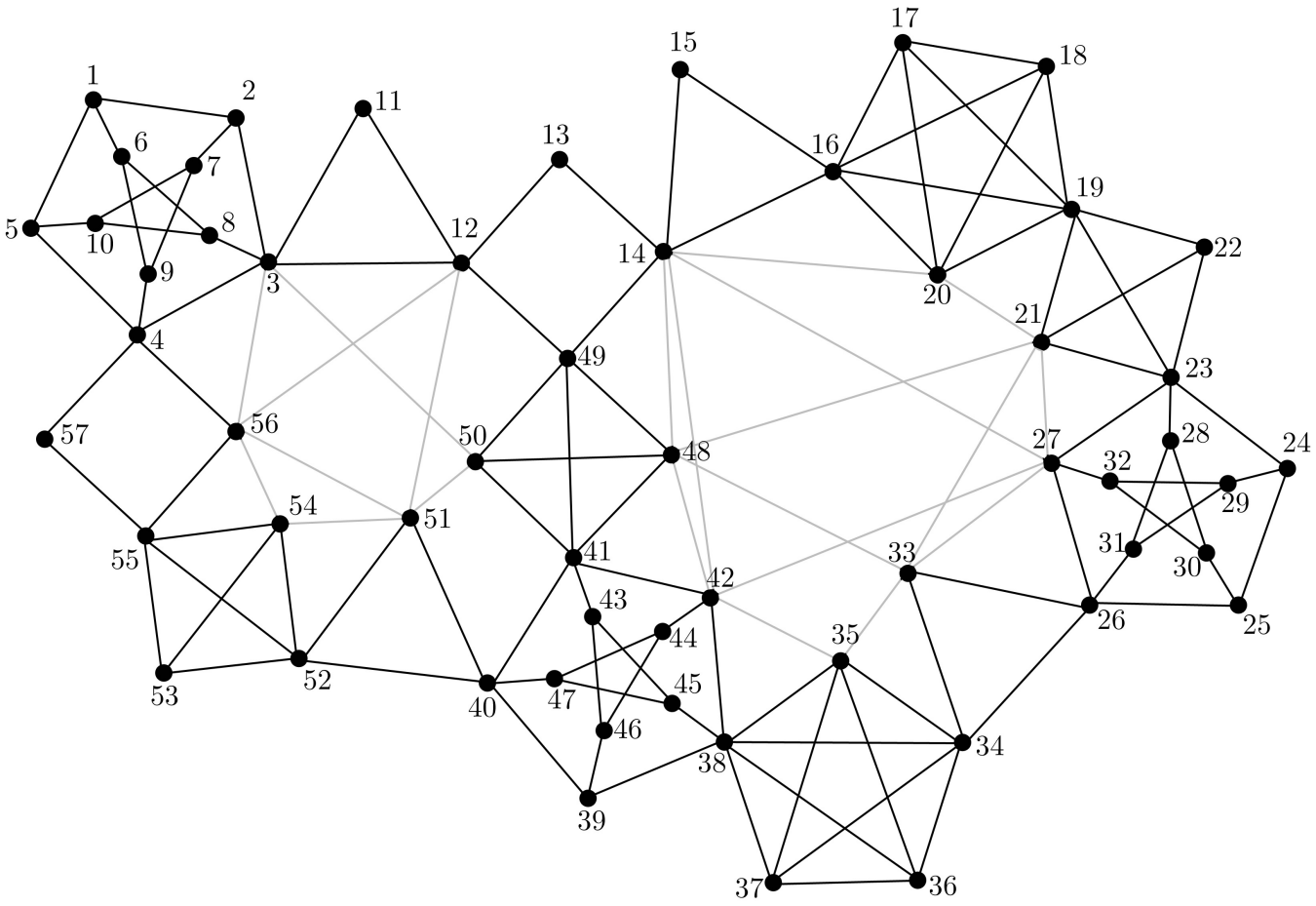


Figure 4: The graph G_{57} with $\phi(G_{57}) = 5$

processes can well describe the behavior of the system in practical applications. Hence, a natural question that we come up with here is: what security parameters one should choose in order to obtain an applied secure system?

References

[1] Bahman Ahmadi. k-Flows on Graphs. Sharif University of Technology, 2007. M.Sc. thesis (in Persian).

[2] M. Ajtai. Generating hard instances of lattice problems (extended abstract). *In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 99–108. ACM, 1996.

[3] Gorjan Alagic, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the first round of the nist post-quantum cryptography standardization process. 2019.

[4] Ellie DHondt. Quantum approaches to graph colouring. *Theoretical Computer Science*, 410(4):302 – 309, 2009.

[5] Reinhard Diestel. *Graph theory {graduate texts in mathematics; 173}*. Springer-Verlag Berlin and Heidelberg GmbH & amp, 2000.

[6] Michael Fellows and Neal Koblitz. Combinatorial cryptosystems galore! *Contemporary Mathematics*, 168:51–51, 1994.

[7] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness (Series of Books in the Mathematical Sciences)*. W. H. Freeman, first edition edition, 1979.

[8] Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, and Joseph H Silverman. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.

[9] François Jaeger. Nowhere-zero flow problems. *Selected topics in graph theory*, 3:71–95, 1988.

[10] N. Koblitz, A.J. Menezes, Y.H. Wu, and R.J. Zuccherato. *Algebraic Aspects of Cryptography*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2012.

[11] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post-quantum cryptography*, pages 147–191. Springer, 2009.

[12] Andrzej Paszkiewicz, Anna Górska, Karol Górski, Zbigniew Kotulski, Kamil Kulesza, and Janusz Szczepański. Proposals of graph based ciphers, theory and implementations. In *Proceedings of the Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO, RCMIS*, pages 4–6, 2001.

[13] PLK Priyadarsini. A survey on some applications of graph theory in cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, 18(3):209–217, 2015.

[14] Paul D Seymour. Nowhere-zero 6-flows. *Journal of Combinatorial Theory, Series B*, 30(2):130–135, 1981.

[15] Joop van de Pol. Lattice-based cryptography. *Master's thesis, Eindhoven University of Technology*, 2011.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

A new proof for the hardness of the graph burning problem

Elham Roshanbin[1]
Alzahra University, Tehran, Iran

Abstract

Burning number is a graph parameter that measures the speed of contagion in a graph process, called graph burning. Study of the computational complexity of the burning number of graphs from different perspectives has got researchers attention. In particular, the Graph Burning problem has been defined and studied in this regard. The Graph Burning problem considers whether or not the burning number of a graph exceeds a given integer k. It is known that Graph Burning problem is an **NP**-complete problem for $k \geq 4$. However, in proving all of the known **NP**-completeness results on the Graph Burning problem, only the reductions from the Distinct 3-Partition problem have been used. Here we provide a different proof for the **NP**-completeness of the Graph Burning problem by a reduction from a problem that is called Planar 3-SAT.

Keywords: Graph burning, Burning number, Computational complexity, NP-complete, Planar 3-SAT
Mathematics Subject Classification [2010]: 05C85, 05C90

1 Introduction

The study of the social contagion is an active topic in social network analysis [1, 8, 15, 16, 21, 22]. As a simplified, deterministic model for the spread of influence in social networks, the *graph burning* process was defined by Anthony Bonato et al in [4], in 2014. Graph burning is defined on a simple, undirected, and finite graph G in discrete time-steps, as follows.

Initially at time $t = 0$, all the nodes are unburned. At each round, every node is either *burned* or *unburned*; if a node is burned, then it remains in that state until the end of the process. At every round $t \geq 1$, we choose an unburned node to burn, if such a node is available. Once a node is burned in round t, each of its unburned neighbours becomes burned in round $t + 1$. The process ends when all the nodes are burned.

As a simplified measure for the speed of the spread of social contagion, the *burning number* of a graph G, written by $b(G)$, is the minimum number of rounds needed for the graph burning process to end. For example, it is easy to see that for the path $P_5 : v_1, v_2, v_3, v_4, v_5$ on 5 nodes, $b(P_5) = 3$, and this can be acheived for instance by burning the nodes v_3, v_4, and v_5 in order, as shown in Figure 1.

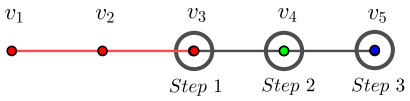


Figure 1: A burning process for P_5 that ends in 3 steps.

[1]speaker

Suppose that a burning process for a graph G ends in k steps, and for each i, $1 \leq i \leq k$, we denote the additional node that we burn in the i-th step by x_i. Such a node is called a *source of fire* and the sequence $(x_1, x_2, \ldots, x_k)$ is called a *burning sequence* for G. The burning number of G is then, the length of a shortest burning sequence for G. We call such a burning sequence, an *optimum* burning sequence. For example, the sequence (v_3, v_4, v_5), demonstrated in Figure 1, is an optimum burning sequence for P_5.

The only graph with burning number 1, is the graph with a single node. Graphs with burning number 2 have been characterized in [4, 5]. Graphs with burning number 3 also have been characterized recently in [19]. However, in general, it is known that finding the burning number of graphs is a hard problem [3, 23]. To be more clear, the *Graph Burning* problem is defined as follows.

Problem: Graph Burning
Instance: A finite simple graph G, and an integer $k \geq 4$.
Question: Is $b(G) \leq k$? In other words, does G contain a burning sequence $(x_1, x_2, \ldots, x_k)$?

It has been proved that the Graph Burning problem is **NP**-complete even for spider graphs, trees of maximum degree 3, path-forests (as a family of disconnected graphs), caterpillars, interval graphs, permutation graphs, and disk graphs [3, 9, 11, 13, 23]. In all of those proofs, a reduction from a numerical problem, called Distinct 3-Partition problem has been used. The Distinct 3-Partition problem is known to be strongly **NP**-complete [14] (which is needed and used in those proofs; see [10] for the concept of stongly **NP**-completeness). In this paper, we prove the **NP**-completeness of the Graph Burning problem using a reduction from a different known **NP**-complete problem, called Planar 3-SAT.

2 Main results

The main result of this section is Theorem 2.4. The strategy of the proof of Theorem 2.4 uses a reduction from the Planar 3-SAT problem. We apply some of the ideas that were used in the reductions for proving the **NP**-completeness of the domination problem in [12]. We first need some basic definitions from graph theory [24].

If v is a node of a graph G, then the *eccentricity* of v is defined as $\max\{d(v,u) : u \in V(G)\}$. The *radius* of G is the minimum eccentricity over the set of all nodes in G. The *center* of G consists of the nodes in G with minimum eccentricity. Every node in the center of G is called a *central* node of G. Given a positive integer k, the *k-th closed neighborhood* of v is defined to be the set $\{u \in V(G) : d(u,v) \leq k\}$ and is denoted by $N_k[v]$; we denote $N_1[v]$ simply by $N[v]$.

Let $s \geq 3$, and $\mathcal{P}$ be a collection of s distinct paths, each of them of order at least two, such that they only share at a single node c (i.e, c is the only node that those paths share). We call a graph that is obtained by pasting together the paths in $\mathcal{P}$ at the single node c, a *spider graph*. Each of the paths in $\mathcal{P}$ is called an *arm* of the spider, and the node c is called the *spider head*.

If all of the arms of a spider graph are of the same length r, then we denote such a graph by $SP(s,r)$. Note that in a $SP(s,r)$, the spider head c is the only central node. If we join the central nodes of two $SP(s,r)$ by adding an edge between them, then we call the obtained graph a *double spider graph*, and we denote it by $DSP(s,r)$. Note that in a double spider graph $DSP(s,r)$, there are exactly two central nodes that correspond to the central nodes of the spider graph $SP(s,r)$.

Here we also state some background on the burning number that is needed for proving our results. As proved in [4], a sequence of nodes $(x_1, x_2, \ldots, x_k)$ forms a burning sequence for a graph G if and only if, for each pair i and j, $d(x_i, x_j) \geq |j - i|$, and the following set equation holds:

$$N_{k-1}[x_1] \cup N_{k-2}[x_2] \cup \ldots \cup N_0[x_k] = V(G). \tag{1}$$

The following theorem from [4, 23] gives us a useful bound for the burning number of a graph.

Theorem 2.1. *For a connected graph G of radius r, $b(G) \leq r + 1$.*

A subgraph H of a graph G is called an *isometric* subgraph if, for every pair of nodes in H denoted by u, v, $d_H(u, v) = d_G(u, v)$. For example, since there is a unique path between any two nodes of a tree, every subtree of a tree is an isometric subgraph. The following theorem has been proved in [5, 23].

Theorem 2.2. *If H is an isometric subtree of a graph G, then $b(H) \leq b(G)$.*

We need the following lemma in proof of Theorem 2.4.

Lemma 2.3. *1. For a spider graph $SP(s, r)$, with $s \geq r$, we have that $b(SP(s, r)) = r + 1$. Moreover, for $s \geq r + 2$, every optimum burning sequence of $SP(s, r)$ must start by burning the central node.*

2. For a double spider graph $DSP(s, r)$ with $s \geq r + 1$, we have that $b(DSP(s, r)) = r + 2$. Moreover, for $s \geq r + 2$, if u and v are the central nodes of $DSP(s, r)$, and in an optimum burning sequence $(x_1, x_2, \ldots, x_{r+2})$ node x_1 is not a central node, then either x_1 is adjacent to u and $x_2 = v$, or x_1 is adjacent to v and $x_2 = u$.

Proof. Part (1) has been proved in [3], and to prove part (2), we use part (1) as follows.

Let u and v be the two central nodes of $DSP(s, r)$. Note that $DSP(s, r)$ is a graph of radius $r + 1$. Moreover, it contains two copies of the spider graph $SP(s + 1, r)$ as its isometric subtree, such that each of u and v is the central node of one of those spiders. Thus, if $s \geq r + 1$, then by part (1), Theorem 2.1, and Theorem 2.2, $r + 1 \leq b(DSP(s, r)) \leq r + 2$.

By cotradiction, suppose that $b(DSP(s, r)) = r + 1$. That is, there is a burning sequence $bs = (x_1, x_2, \ldots, x_{r+1})$ for $DSP(s, r)$. Hence, the fire started at the nodes in bs must also burn the two copies of the spider graph $SP(s + 1, r)$ with centers u and v. But since $s + 1 \geq r + 2$, by applying part (1) on each of those spiders, once we conclude that $x_1 = u$, and next, we clonclude that $x_1 = v$, which is a contradiction. Therefore, such a burning sequence bs does not exist, and thus, $b(DSP(s, r)) = r + 2$.

Now suppose that $s \geq r + 2$, and $bs = (x_1, x_2, \ldots, x_{r+2})$ is an optimum burning sequence for $DSP(s, r)$. If $x_1 \in \{u, v\}$, then clearly every node in $DSP(s, r)$ will be burned after $r + 2$ steps.

If $x_1 \neq u$ and $x_1 \neq v$, then without loss of generality, by symmetry assume that x_1 is closer to u than v (Otherwise, we will have a similar discussion). Thus, x_1 must be in one of the arms of $DSP(s, r)$ that is attached to u, and clearly x_1 is not adjacent to v. If x_1 is not adjacent to u, then we have two possibilities; either $x_2 = v$ or not.

If $x_2 = v$, then by pigeon-hole principle, there must be an arm attached to u that contains no fire source rather than possibly u (even in that case, $u = x_i$, for some $i \geq 3$). Let w be the leaf of such an arm. It can be easily checked that w cannot receive the fire from any fire source by the end of the $(r + 2)$-th step, which is a contradiction.

If $x_2 \neq v$, then by pigeon-hole principle, there must be at least one arm attached to v that contains no fire source rarther than possibly v (even in that case, $v = x_i$, for some $i \geq 3$). Let w be the leaf of such an arm. It can be easily checked that w cannot receive the fire from any fire source by the end of the $(r + 2)$-th step, which is again a contradiction. Therefore, we conclude that if x_1 is not a central node, then it has to be adjacent to a central node.

Now if x_1 is adjacent to u and $x_2 = v$, then clrealy every node in $DSP(s, r)$ will be burned after $r + 2$ steps. If x_1 is adjacent to u and $x_2 \neq v$, then again by pigeon-hole principle, there must be an arm attached to v that contains no fire source rather than possibly v (even in that case, $v = x_i$, for some $i \geq 3$). Let w be the leaf of such an arm. It can be easily checked that w cannot receive the fire from any fire source by the end of the $(r + 2)$-th step, which is a contradiction.

By the above discussion we have considered all the possiblities, and therefore, the proof follows. □

For the statment of the Planar 3-SAT problem which will be used in proof of Theorem 2.4, we need the following definitions.

A graph G is *planar* if there is a drawing of G in the plane such that no two edges of G cross each other except at the end-points. A *subdivision* of a graph G is a graph obtained from replacing some of the edges in G by longer paths. It is known that if a graph G is planar, then any subdivision of G is also planar [24].

Assume that $U = \{u_1, u_2, \ldots, u_k\}$ is a finite set of Boolean variables. By a *clause* over U, we mean a 3-element set $C = \{x_1, x_2, x_3\}$ in which each x_i is an element of U such as u_i or its negation (denoted by $\overline{u}_i$), and we do not have both u_i and $\overline{u}_i$ at the same time in C. Given the set U and a collection of 3-element clauses over U such as $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$, we construct a graph $G(\mathcal{C})$ as follows. For $1 \leq i \leq k$, let $E_i = \{u_i, \overline{u}_i\}$ be the set of two nodes corresponding to variable $u_i \in U$ and its negation. We take $\mathcal{C} \cup \left(\bigcup_{i=1}^{k} E_i\right)$ as the node set of graph $G(\mathcal{C})$. We then join each u_i to any C_j satisfying $u_i \in C_j$. Similarly, we join each $\overline{u}_i$ to any C_j that $\overline{u}_i \in C_j$. Finally, we connect every pair of nodes in each E_i by an edge, and the graph $G(\mathcal{C})$ is obtained.

Here is the statement of the Planar 3-SAT problem.

Problem: Planar 3-SAT
Instance: A finite set $U = \{u_1, u_2, \ldots, u_k\}$ of Boolean variables and a collection $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ of 3-element clauses over U, such that the graph $G(\mathcal{C})$ as described above is planar.
Question: Is there any satisfying truth assignment for $\mathcal{C}$; that is, a truth assignment for the variables in U such that every clause in $\mathcal{C}$ contains at least one True assigned variable?

It is known that Planar 3-SAT is **NP**-complete; see [20]. We are now ready to state and prove the main result.

Theorem 2.4. *The Graph Burning problem is **NP**-complete even when restricted to planar, connected or disconnected graphs.*

Proof. The burning problem is in **NP** since it takes polynomial time to find the $(k-i)$-th neighborhood of x_i, for $1 \leq i \leq k$, and therefore, to verify (1).

Now, let $U = \{u_1, u_2, \ldots, u_k\}$ be a set of Boolean varibales for some positive integer k, and let $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$ be a collection of 3-element clauses over U. We now construct a graph $G'(\mathcal{C})$ based on $\mathcal{C}$ as follows.

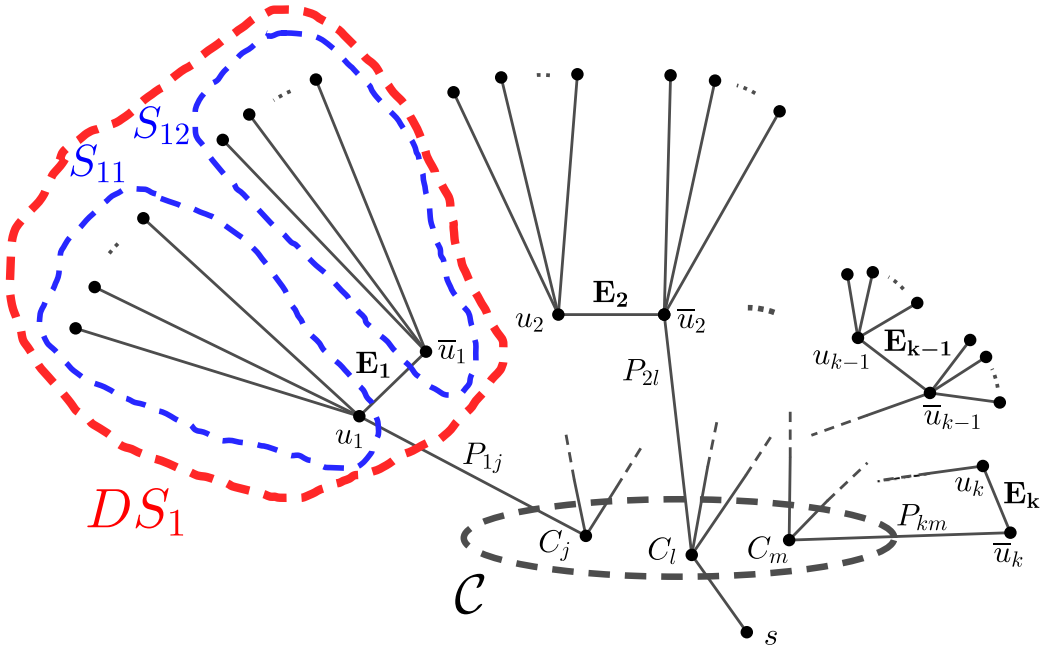


Figure 2: A depiction of the graph $G'(\mathcal{C})$.

First, we make the graph $G(\mathcal{C})$ as mentioned above with the node set $\mathcal{C} \cup \left(\bigcup_{i=1}^{k} E_i\right)$, where $E_i = \{u_i, \overline{u}_i\}$. We then replace each edge $\{u_i, C_j\}$ or $\{\overline{u}_i, C_j\}$ in $G(\mathcal{C})$ (by assumption, only one of them belongs to $G(\mathcal{C})$) with a path of length $k+1-i$, denoted by P_{ij}. We also add a single new node s. We then join s arbitrarily to one of the nodes in $\mathcal{C}$. Finally, we attach to each node u_i and $\overline{u}_i$ a spider graph $SP(k+2-i, k-i)$, denoted by S_{i1} and S_{i2}, respectively; where u_i and $\overline{u}_i$ are the centers of S_{i1} and S_{i2}. The resulting graph is $G'(\mathcal{C})$; see Figure 2.

It is evident that $|V(G'(\mathcal{C}))| = O(k^3 + mk + m)$. The graph $G'(\mathcal{C})$ is planar as we have attached some copies of the spider graphs (which are planar) to a subdivision of $G(\mathcal{C})$, which is a planar graph by assumption. Note that $\mathcal{C}$ forms an independent set for $G'(\mathcal{C})$. Moreover, for $1 \leq i \leq k$, every edge $u_i\overline{u}_i$ forms the center of a double spider graph $DSP(k-i+2, k-i)$, that we call it DS_i.

We want to show that $\mathcal{C}$ is satisfiable over U (of size k) if and only if $G'(\mathcal{C})$ has a burning sequence of size $k+1$.

First, suppose that there is a satisfying truth assignment for $\mathcal{C}$. Take $bs = (x_1, x_2, \ldots, x_k, s)$ in which $x_i = u_i$ if u_i is True; otherwise, $x_i = \overline{u}_i$. We claim that bs forms a burning sequence of size $k+1$ for $G'(\mathcal{C})$. To show this, we need to prove that by burning bs in the specified order, every node in $G'(\mathcal{C})$ will be burned after $k+1$ steps.

First, we can easily see that for $1 \leq i \leq k$, all the nodes in S_{i1} and S_{i2} are within distance $k-i+1$ from x_i, and x_i is the i-th fire source. Thus, they will be burned after $i + (k-i+1) = k+1$ steps from the beginning of the burning process. Since the x_i's satisfy $\mathcal{C}$, each $C_j \in \mathcal{C}$ contains at least one True assigned variable x_i, for some $1 \leq i \leq k$. Therefore, at the end of the $(k+1)$-th step, C_j will be burned, by the fire spread from x_i through the path P_{ij}. Finally, all the internal nodes on each P_{ij} are of distance at most $k-i+1$ from x_i, and hence, they will be burned after $i + (k-i+1) = k+1$ steps.

Conversely, suppose that $G'(\mathcal{C})$ has a burning sequence $(y_1, y_2, \ldots, y_{k+1})$ of size $k+1$. Note that by construction, we have a copy of $DSP(k+1, k-1) = DS_1$ with the center E_1, as an isometric subtree of $G'(\mathcal{C})$. Thus, by Theorem 2.2 and Lemma 2.3 (2), $b(G'(\mathcal{C})) \geq b(DS_1) = k+1$. Therefore, $b(G'(\mathcal{C})) = k+1$, and the sequence $(y_1, y_2, \ldots, y_{k+1})$ must be an optimum burning sequence. We now discuss on the possible choices for y_i's.

Note that, for $1 \leq i \leq k-1$, the nodes in each E_i form the center of $DS_i = DSP(k-i+2, k-i)$ as an isometric subtree of $G'(\mathcal{C})$. By Lemma 2.3 (2), for burning DS_i, we need at least $k-i+2$ steps. Moreover, the only connection between each DS_i and the rest of the graph is through the paths P_{ij}'s, and the paths P_{ij}'s only intersect possibly at their end points. Hence, by Lemma 2.3 (2), for $1 \leq i \leq k-1$, y_i must be a node x such that, either x is a central node of DS_i, or is adajacent to a central node in DS_i. But, if for some $1 \leq i \leq k-1$, y_i be a node that is adjacent to a central node of DS_i, then by Lemma 2.3 (2), $y_{i+1} \in E_i \subseteq DS_i$, which is a contradiction (since, y_{i+1} has to be either in E_{i+1} or in its neighbourhood). Thus, by Lemma 2.3 (2), y_i must be a central node of DS_i; that is, $y_i = x$, for some $x \in E_i$.

Knowing the nodes $y_1, y_2, \ldots, y_{k-1}$, we now consider y_k and y_{k+1} as follows. Note that for burning E_k we need two steps. On the other hand, by the end of the $(k-1)$-th step, all the nodes in the neighborhood of E_k are unburned, and there is no node among them that is adjacent to both nodes of E_k (it follows from the lenght of P_{ij}'s, for $1 \leq i \leq k-1$, and the definition of Planar 3-SAT, where we assume u_i and its negation do not appear in any given clause at the same time). Therefore, we must have $y_k \in E_k$. Finally, since s is of distance at least two from every burned node in the k-th step, then we must have $y_{k+1} = s$.

By the above discussion, all the nodes in DS_i's and P_{ij}'s, except for possibly the end points of some of P_{ij}'s which are in $\mathcal{C}$, will be burned after $k+1$ steps. Now, we have to consider $\mathcal{C}$. By assumption, $b(G'(\mathcal{C})) = k+1$, and we already proved that for $1 \leq i \leq k$, y_i must be selected from E_i. On the other hand, since $u_i\overline{u}_i$ is an edge, and considering the construction of $G'(\mathcal{C})$, if $y_i = x \in E_i$, and P_{ij}'s are the paths that connect x to the nodes in $\mathcal{C}$, then we can easily see that by the end of the $(k+1)$-th step, all the nodes in P_{ij}'s, including their end points in $\mathcal{C}$, are burned. But for any other P_{rl}, the end point of P_{rl} in $\mathcal{C}$ is not burned. Therefore, for having $\mathcal{C}$ burned by the end of the $(k+1)$-th step, there must be a selection

of $y_1, y_2, \ldots, y_k$ such that each $C_j \in \mathcal{C}$ will be burned by receiving the fire spread from y_i's in the $(k+1)$-th step. Hence, $\{y_i\}_{i=1}^{k}$ must be assigned True variables that satisfy $\mathcal{C}$.

Note that, since the set of Boolean variables must be of order at least three, then $k \geq 4$. The preceding discussion provides a reduction from Planar 3-SAT problem to the Graph Burning problem on a planar graph. There are other known **NP**-complete variations of the Planar 3-SAT, where its assumed that the constructed planar graph $G(\mathcal{C})$ is 3-connected with some more restrictions [17], or the set of nodes corresponding to the clauses, i.e., $\mathcal{C}$ are connected via a cycle; see [18]. Using those variations of the Planar 3-SAT, yet by the same proof as above, we could prove the **NP**-completeness of the Graph Burning for connected graphs. We could also modify $G'(\mathcal{C})$ such that the resulting graph is disconnected, just by taking s as an isolated node, and proof will be analogous. Hence, the Graph Burning problem is **NP**-complete even for disconnected graphs. □

References

[1] S. Banerjee, A. Das, A. Gopalan, S. Shakkottai, *Epidemic spreading with external agents*, In: Proceedings of IEEE Infocom, 2011.

[2] S. Bessy, A. Bonato, J. Janssen, D. Rautenbach, E. Roshanbin, *Bounds on the Burning Number*, Discrete Applied Mathematics 235 (2018) 16–22.

[3] S. Bessy, A. Bonato, J. Janssen, D. Rautenbach, E. Roshanbin, *Burning a Graph is Hard*, Discrete Applied Mathematics 232 (2017) 73–87.

[4] A. Bonato, J. Janssen, E. Roshanbin, *Burning a Graph as a Model of Social Contagion*, Lecture Notes in Computer Science 8882 (2014) 13–22.

[5] A. Bonato, J. Janssen, E. Roshanbin, *How to burn a graph*, Internet Mathematics 1-2 (2016) 85-100.

[6] A. Bonato, M.E. Messinger, P. Prałat, *Fighting constrained fires in graphs*, Theoretical Computer Science 434 (2012) 11–22.

[7] A. Bonato, R.J. Nowakowski, *The Game of Cops and Robbers on Graphs*, American Mathematical Society, Providence, Rhode Island, 2011.

[8] P. Domingos, M. Richardson, *Mining the network value of customers*, In: Proceedings of the 7th International Conference on Knowledge Discovery and Data Mining (KDD), 2001.

[9] Y. Gao, E. Roshanbin, *The graph burning problem for some families of graphs*, In: Proceedings of the 5th International Conference on Combinatorics, Cryptography, Computer Science and Computing, 2021.

[10] M.R. Garey, D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman & Co., 1990.

[11] A.T. Guptal, S.A. Lokhande, K. Mondal, *NP-Completeness Results for Graph Burning on Geometric Graphs*, CoRR: https://arxiv.org/abs/2003.07746, 2020.

[12] T.W. Haynes, S.T. Hedetniemi, P.J. Slater, *Fundamentals of Domination in Graphs* Marcel Dekker, New York, 1998.

[13] M. Hiller, A.M.C.A. Koster, E. Triesch, *On the Burning Number of p-Catrepillars*, Graphs and Combinatorial Optimization: from Theory to Applications, 2021, Volume 5, pp145–156.

[14] H. Hulett, T.G. Will, G.J. Woeginger, *Multigraph realizations of degree sequences: Maximization is easy, minimization is hard*, Operations Research Letters 36 (2008) 594–596.

[15] D. Kempe, J. Kleinberg, E. Tardos, *Maximizing the spread of influence through a social network*, In: Proceedings of the 9th International Conference on Knowledge scovery and Data Mining (KDD), 2003.

[16] D. Kempe, J. Kleinberg, E. Tardos, *Influential nodes in a diffusion model for social networks*, In: Proceedings 32nd International Colloquium on Automata, Languages and Programming(ICALP), 2005.

[17] J. Kratochvíl, *A special planar satisfiability problem and a consequence of its NP-completeness*, Discrete Applied Mathematics 52 (3) (1994) 233–252.

[18] J. Kratochvíl, A. Lubiw, and J. Nešetřil, *Noncrossing subgraphs in topological layouts*, SIAM J. Discrete Math 4(2) (1991) 223–244.

[19] Y. Li, G. Shi, X. Qin, *Graphs with burning number three*, Applied Mathematics and Computation, Volume 487, 2025, 129100, ISSN 0096-3003, https://doi.org/10.1016/j.amc.2024.129100.

[20] D. Lichtestein, *Planar formulae and their uses*, SIAM Journal of Computing 11 (1982) 329–343.

[21] E. Mossel, S. Roch, *On the submodularity of influence in social networks*, In: Proceedings of 39th Annual ACM Symposium on Theory of Computing(STOC), 2007.

[22] M. Richardson, P. Domingos, *Mining knowledge-sharing sites for viral marketing*, In: Proceedings of the 8th International Conference on Knowledge scovery and Data Mining (KDD), 2002.

[23] E. Roshanbin, *Burning a graph as a model of social contagion*, Ph.D. Thesis, Department of Mathematics and Statistics, Dalhousie University, 2016.

[24] D.B. West, *Introduction to Graph Theory, 2nd edition*, Prentice Hall, 2001.

Email: e.roshanbin@alzahra.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Graph-based analysis of pandemic interventions effectiveness

Marzieh Vahid Dastjerdi[1]
Research Center for Developing Advanced Technologies, Tehran, Iran

Behnaz Omoomi
Isfahan University of Technology, Isfahan, Iran

Abstract

Many mathematical modeling and simulations have been proposed for transmission of different infectious diseases based on information from social network structure. The mathematical approach is necessary to adopt appropriate interventions at the right time to slow the spread of the virus and reduce economic costs. The closure of schools and universities, the banning of mass rallies, and other policies of social distancing in countries are effective in terms of the social network parameters and the number of affected people per day. Although implementing social distancing as an effective strategy seems necessary, its implementation will incur socio-economic costs in the long term.

In this study, we designed a dynamic graph model for predicting the number of infected cases under different interventions, such as school or mosque closure and limited workplace activity and shopping malls. We apply this model for coronavirus transmission in a region of Isfahan in Iran. The results indicated that interventions like school closure led to moderate change in network parameters and had a desirable effect on the number of infected individuals. Moreover, for each proposed model, the accuracy assessment is performed based on the root mean square error between the real and estimated number of infected individuals, and the best fitting models are introduced to show that simulated interventions are in accordance with really applied interventions.

Keywords: Graph modeling, Dynamic graph model, Social network parameters, Virus transmission, Coronavirus.

AMS Mathematical Subject Classification [2010]: 93A30, 05C80, 37A60.

1 Introduction

A *pandemic* is defined as occurring over a wide geographic area and affecting an exceptionally high proportion of the population [1]. The last major global outbreak of disease was the COVID-19 (Coronavirus) pandemic declared in 2020, which killed millions globally. On 19 February 2020, Iran reported its first confirmed cases of infections in Qom [2]. From 24 February to 11 March 2020, this infection spreads to all cities of Iran [3].

Current information about Coronavirus is indicating that human-to-human transmission is occurring. The routes of transmission of COVID-19 remains unclear at present, but evidence from other *coronaviruses* and respiratory diseases indicates that the disease may spread through large respiratory droplets and direct or indirect contact with infected person [4]. The use of social distancing interventions is embedded within

[1] speaker

the pandemic preparedness plans of most countries [5–7] and also appear in recent WHO recommendations. School closure, household quarantine and reduced workplace, social and community contacts are considered to be key non-pharmaceutical interventions which may readily be used for the early containment of an influenza epidemic [8].

Mathematical modeling is an effective method for analyzing the leading causes of the epidemics and finding essential intervention strategies towards it [9, 10]. In this paper, we use a dynamic graph model to simulate the transmission of the virus in the real world. For this purpose, we need the following terminology and concepts [11].

A *graph* is an ordered pair $G = (V(G), E(G))$ where $V(G)$ is the set of nodes and $E(G)$ is the set of edges. We focus on simple graphs with no self-edges and parallel edges (i.e. between every two vertices at most one edge exists). The *degree* of a vertex v in graph G, denoted $deg_G(u, v)$ is the number of vertices adjacent (connected) to it.

A *path* in graph G is a sequence $v_1, v_2, \ldots, v_k$, where no vertex is repeated and such that (v_i, v_{i+1}) is an edge in $E(G)$. The *distance* between any two vertices u and v in graph G, denoted $d_G(u, v)$, is the number of edges in a shortest path between them. If there is no path connecting them, then we assume that the distant is infinity.

A *random graph*, $G_{N,p}$ of N nodes is constructed by adding edges between nodes at random with probability p. A *network* is a graph where edges and or vertices have attributes (names). More precisely, in a social network, a node in a graph represents a person, and an edge between two nodes represents a relationship between two persons that would allow for disease transmission.

The first and most well-studied random network model is the Erdő-Rényi random graphs [12]. This model has the least possible

In [13] an individual based model of a small community in the developed with detail for precise simulation of household demographics, movement within the community and individual contact patterns. They modelled the spread of pandemic influenza in the community and the effect on daily and final attack rates of four social distancing measures: school closure, increased case isolation, workplace non-attendance and community contact reduction.

A heterogeneous graph modeling approach is designed in [14] to describe the dynamic process of influenza virus transmission by building social network of studied region and embedding an Agent-Based Model to describe the dynamic change of an epidemic. Multiple scenarios for vaccination and school closure strategies were simulated and their performance was analyzed.

A dynamic graph model is designed in [15] for a glance of the dynamics under a public epidemic emergency situation.They demonstrated the impact of asymptomatic transmission in outbreak and showed the effectiveness of city lockdown to halt virus spread within a city. In [16], all the available mathematical models that have been used in predicting the transmission of COVID-19 are summarized.

In this paper, we design a dynamic graph model of the virus transmission through the individuals interaction to study the effect of intervention strategies on the spread of the virus. To determine the parameters of network, we need the exact time and process of interventions plus accurate number of infected cases. Thus, we apply this modeling for the experimental data obtained from district 13 in Isfahan in Iran for Coronavirus pandemic. The results, however, are expandable to other regions in case of availability of enough information.

2 Population Intractions

We construct a graph-based model for interactions in a community to determine the impact of alternative intervention strategies. In this model, we consider sets of schools, workplaces, shopping centers, and mosques referred as contact hubs. Different interventions, namely closure of schools, mosques and shopping centers, and reduction of labor, are simulated to form different plausible scenarios.

Each person in the population corresponds to a node of the graph. If two persons are in a close interaction, then we add an edge between the nodes corresponding to these persons. Thus, it is natural to assume that induced subgraph on the nodes corresponding to every household is a complete graph. In a *complete graph* all pairs of nodes are adjacent.

Based on the chosen community, we could consider different hubs. For every contact hub, based on the age, sex, and contact time people, a set of edges with a probability are added to the graph.

We use real community data from Isfahan municipality to estimate the number of hubs and age/sex distributions of the selected sample population in district 13. District 13 of Isfahan municipality is situated in the southwest of Isfahan. In this district and in an area of 3524 hectares, close to 154300 people in approximately 38700 households are residing (see Fig 1). District 13 includes one major hospital, two main shopping malls, 40 schools, and about 34500 employers. We used a detailed individual-based model of a real small community. Our human contact network has 15,000 households with a population of approximately 48,000 members to simulate the dynamics of the Coronavirus pandemic. Regrading the number of people in each household, there are 100 households with one member, 4300 households with 2 members, 5200 households with 3 members, 3500 households with 4 members, 1500 households with 5 members, and 400 households with 6 members. We believe that this modelled population provides us with a large enough experimental test-bed to capture the daily mobility of individuals.

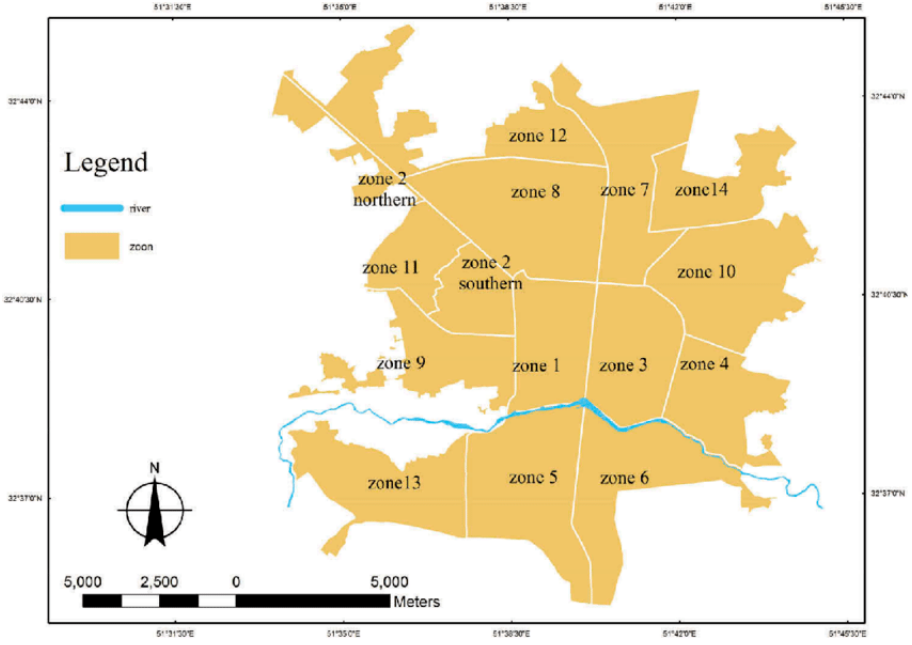


Figure 1: Zoning map related to Isfahan, Iran.

Two main shopping malls (Kowsar-6 and Tavoni Zob-Ahan) in the community are selected as shopping

centers hub. For this population, ten mosques are considered with an average population of 60 people. We also assume that every person with age in range 7 to 18 is a student. Based on the ages of student, we partied them in to three types of schools (elementary, middle and high schools) with at most 100 students in each school. In this model, we consider about 6900 students in 69 schools. For modeling every contact hub, a set of edges are added to the graph, according to following criteria.

Schools hubs

We consider three types of schools as elementary schools, middle schools, and high schools. According to the age of the children, we determine their grades and assign each child to a class in their school. We assume that the schools are as close to the children's home locations as possible. We consider the capacity of each school and each class to be 100 and 20 on average, respectively. Every student would come into close contact with every other member in his/her class. Hence, the induced graph on the nodes in each class is complete. Furthermore, we assume that some random connections may exist between every student and others in the same schools (not necessarily in the same class) in each day.

Workplaces hubs

About 70 percent of adults between the ages of 19 to 65 are considered as employed. Adult students and workers are assigned to adult education institutions and workplaces, respectively. We randomly divide workers into groups of size 2 to 6 members with close connections among the persons in each group. Each person at his/her workplace or public transportation can be in close contact with some people in the city. On average, each person is in close connection with three random persons in the city, for example in the bus-stop or other places.

Shopping centers hubs

Shopping centers are among the busiest places in a city. In modeling the relationship between people in these centers, we assume that the probability of referring each family to such centers in each day is about 10 percent . Then, based on the family members' age, we estimate the probability of each member attending to this hub. In the next step, after daily allocating a part of customers to this hub, we randomly divide the people into subpopulations based on the time of the visits. For selected two main shopping malls, each person is assumed to be in close contact with 2 to 6 customers who are present there at the same time.

Mosques hubs

For each of 10 considered mosques with an average population of 60 people, about 60% of the people are fixed visitors for daily praying and the remaining 40% may vary day to day. We consider the random connection of people in the mosque with 2 or 3 other prayers. Furthermore, due to current social condition of this region, the possibility of attending the mosque is considered to be higher for older adults.

3 Networks parameters

The effect of having hubs are scrutinized by two parameters: average global efficiency and clustering coefficient. The *average global efficiency* of G is

$$E_{glob} = \frac{1}{|V(G)|(|V(G)|-1)} \cdot \sum_{u \neq v} \frac{1}{d(u,v)}, \tag{1}$$

which is simply the average of the efficiencies over all pairs of vertices and quantifies the exchange of information across the whole network where information is concurrently exchanged [17].

The *clustering coefficient* measures the degree of clustering of a typical nodes neighborhood. It is defined as the likelihood that any two nodes with a common neighbor are themselves connected. Evidence suggests that in most real-world networks, and in particular social networks, nodes tend to create tightly knit groups characterized by a relatively high density of ties; this likelihood tends to be greater than the average probability of a tie randomly established between two nodes.

The individual clustering coefficient (local clustering coefficient) for a vertex v is given by [18]:

$$CC(G,v) = \frac{\text{number of triangulars that contain } v}{\frac{\deg(v)(\deg(v)-1)}{2}}. \tag{2}$$

Local clustering can be used as a probe for the existence of so-called structural holes in a network, which are missing links between neighbors of a person. The average clustering coefficient (or clustering coefficient for short) is the average of the local clustering coefficients of all the vertices [19]:

$$CC(G) = \frac{\sum_{v \in V(G)} CC(G,v)}{|V(G)|}. \tag{3}$$

We compute these parameters for the networks by Python 3.7.6 (64 bit) programming.

4 Virus transmission model

The main question is that is there any way to help stop the spread of virus or at least slow it down? (by considering socio-economic costs). To answer this question, we are going to simulate the effective interaction between people by considering different scenarios.

In our simulation, the daily infections are caused by peoples contacts, and the frequency of contacts can be mainly influenced by daily illness attack rate, age, intervention strategies adopted by the government, and environment factors. In addition to household and hub contact, people in the simulation are also engaged in random or untraceable community contacts. This contact was assumed to be local in nature, with contacts between persons from the same or nearby areas being relatively more likely than contact from distant patches.

People are identified according to their dynamic status as susceptible (who are not known to become immune to the disease to which they have been exposed by reason of age, a previous attack, or other natural or artificial process), exposed (are known to have been sufficiently near to an infected person to have been exposed to the transfer of infectious material directly, or exposed to articles freshly soiled with such infectious materials), infected, and removed (dead or immume). This model is called a SEIR model.

The immune system and interaction of people follow a circadian rhythm. Thus, we consider cycles of 24 hours in our simulation. In each cycle, we randomly add some new infections. The epidemic in a large

population is a stochastic event. Virus can be transmitted from an infected person to exposed persons in a stochastic manner during a simulation cycle.

By Bernoulli trails, we randomly change the state of exposed persons to infected. More precisely, we calculate the probability of infection transmission between an infected person X_i to exposed person X_e at the time of contact (i.e. t), with the following transmission function.

$$P_t(X_i, X_e) = \beta \times A(X_i, t) \times A(X_e). \tag{4}$$

All of these interventions affect the rate at which people are exposed (β). The effects of all public health interventions are calculated separately to measure each intervention's impact on β. More precisely, for the effect of each intervention, the approximate number of close contacts with the probability of transfer in one day was considered. The results indicate which intervention we are allowed to reduce in the current situation. In [10], a modified SEIR epidemic spreading model was used to describes the spread of the virus and computes the number of infected individuals in Iran (see also [20–22]). In this model, if the interventions are applied (quarantine), the value of β is estimated to be 0.34.

By considering some factors such as space, exposure time, ventilation status, mobility, and crowding, we calculate contact environment risk score for each hub [23]. Note that, with each intervention, the corresponding impact is added to 0.34.

Table 1: Impact of interventions on β.

Contact group	Contacts (per day)	Contact environment risk score	Risk adjusted score (per 1000 people)	Impact on β
Schools	28	10	0.28	0.15
Shopping centers	20	15	0.3	0.16
Workplaces	75	16	1.2	0.64
Mousque	6	17	0.102	0.05

We define the disease ineffectively parameter $A(X_i, t)$ that depends on the time of contact. This parameter is assumed to be 1 for the peak period of infection and then to 0.5 for the rest of the ineffectively period. We consider the period of transportation of an infected person to be 21 days, that 5 days (the first symptoms) $A(X_i, t) = 0.5$, in the next 14 days (the peak time of the disease) $A(X_i, t) = 1$, and in the remaining days it is 0.5. The exposure parameter $A(X_e)$ is function directly dependent on the age of the exposed person. Age-dependent effects in the transmission COVID-19 epidemics is done in [24]. The COVID-19 pandemic has shown a markedly low proportion of cases among children.

Finally, the efficiency of the proposed model is determined by using root mean square error ($RMSE$). *Root Mean Square Error* ($RMSE$) is a standard way to measure the error of a model in predicting quantitative data. Formally it is defined as follows [25].

$$RMSE = \sqrt{\frac{1}{n} \cdot \sum_{t=1}^{n} (p_t - r_t)^2}, \tag{5}$$

where p_t is the predicted value for day t of a regression's dependent variable r_t, and with n is a variable to show the observed days. We simulated some different non-pharmaceutical intervention measures in Table 3.

5 Results

We apply model 4 for the experimental data obtained from district 13 in Isfahan in Iran for Coronavirus pandemic. The information of infected people resident in district 13, Isfahan, Iran, who have referred to medical centers from 2 March 2020 to 2 July 2020 is available locally and obtained from the Isfahan COVID-19 Registry (I-CORE) which is a registry for COVID-19 patients in Isfahan and is accessible via request.

The effect of active hubs in the community is scrutinized by measuring the average global efficiency and clustering coefficient parameters. In Table 2, we compute these parameters for the networks with different active hubs. The constructed graph in the first row only contains the households (which means quarantine without any single hub). In each row, the graph grows by having new hubs which are released from the quarantine. For each graph in the rows, average global efficiency and average clustering are reported in columns of Table 2.

Table 2: Average global efficiency and average clustering for networks with different combination of hubs.

Networks	#edges	Average global efficiency	Average clustering
Households	61300	0.00053435331	0.81628392484
Households + Schools hubs	143153	0.02972751398	0.76933720155
Households + Workplaces hubs, (workforce= 80%)	150212	0.15342580578	0.383289671471
Households + Workplaces hubs, (workforce= 25%)	93046	0.08120269200	0.59505103618
Households + Shopping centers hubs	87853	0.00092563548	0.73276179781
Households + Mosques hubs	64841	0.00070533191	0.79865607218
Households + Shopping centers hubs+ Workplaces hubs	176659	0.16993136426	0.35785043249
Households + All defined hubs	261257	0.19064642164	0.31148489676

In order to show the effect of interventions on the number of affected people, the numbers of active cases per day in the selected small community is estimated. In Simulation A, it is assumed that general health interventions are not applied and COVID-19 continued at its normal mode. In that case, the average number of active cases in this district is estimated to be about 123.78 people per day. Accordingly, interventions like school closure (Simulation S), mosque closure (Simulation M), reduction of the workforce to 25% (Simulation W),reduction of physical shopping to 5% (Simulation P), and different combinations of such interventions are considered. Figures 2 to 6 show the graph for the number of daily affected people during 120 days from the start of the pandemic. In Fig 2, the case of null intervention (Simulation A) is shown along with existence of only one intervention (Simulation S, M, W and P) and real data observed in the small community. Similarly, Fig 3 shows existence of two interventions (Simulation SM, SW, SP, WP, MW, and MP) and Fig 4 demonstrates application of three interventions (or existence of only one active hub) with Simulation SWM, SMP, WPM, and SWP. Application of all four mentioned interventions (Simulation SMWP), complete quarantine (Simulation N), a moderate version of mentioned interventions in Simulation SMWP$\star$ (with reduction of workforce to 60%, and opening of mosques with 50%) are also compared to the real data in the selected small community in Fig 5. Finally, Fig 6 shows an specific simulation which fits the real data. In this simulation, for the first 15 days, no intervention is applied. After that, tough decisions are made such as school and mosque closure, reducing the workforce to 25%, and reducing the rate of physical

shopping to 5%. In the last 50 days, the interventions are the school closures, reducing the workforce to 60%, and reducing the rate of physical presence in malls and mosques.

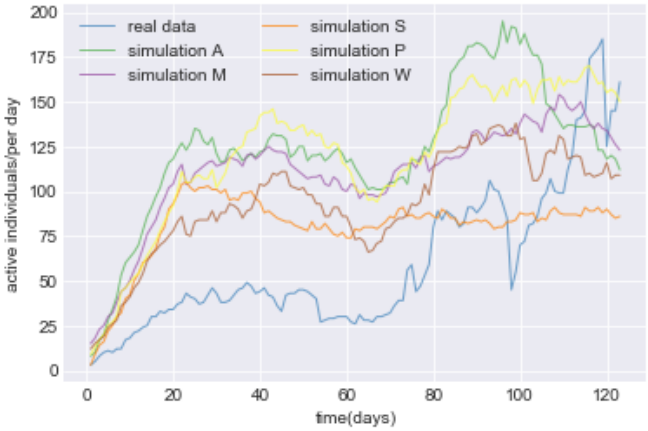


Figure 2: The simulations with at least three active hubs in normal mode.

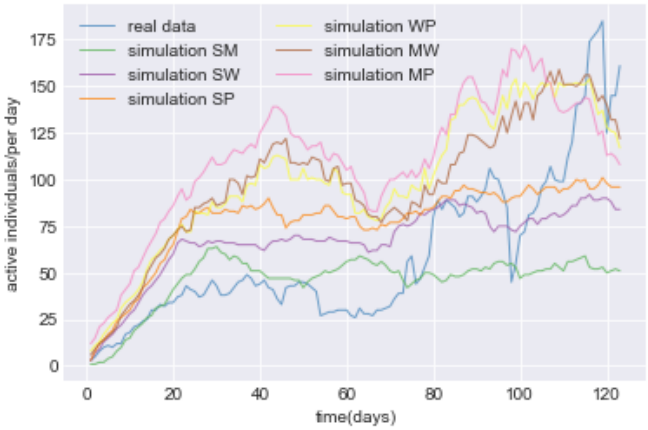


Figure 3: The simulations with two active hubs in normal mode.

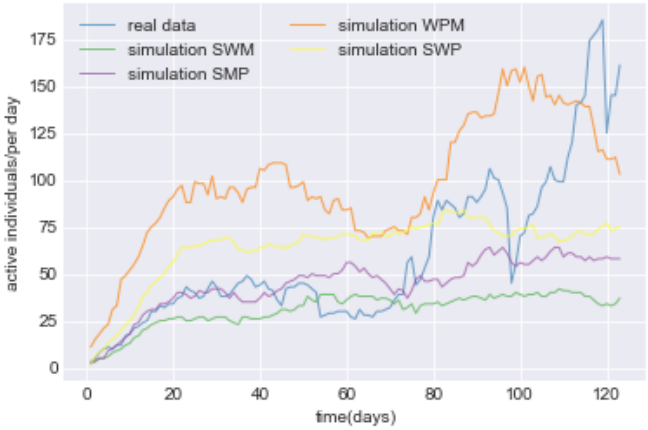


Figure 4: The simulations with one active hub in normal mode.

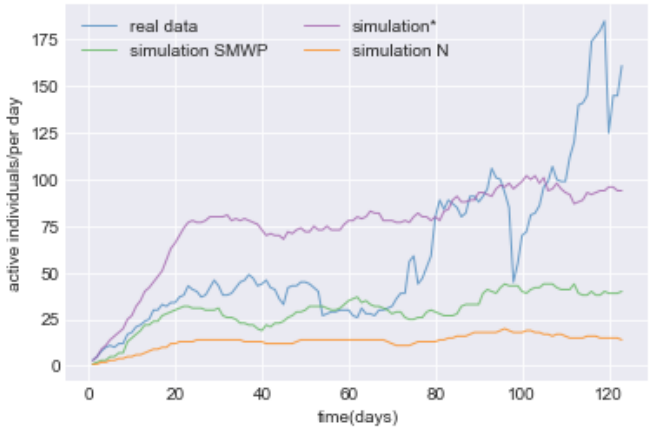


Figure 5: The simulations with no active hubs in normal mode.

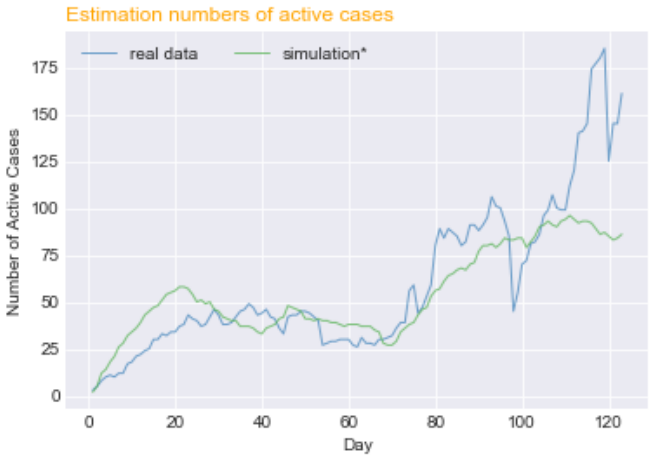


Figure 6: Compare the near-real simulation with the real values.

To demonstrate the effect of interventions on number of active infected individuals, Table 3 shows the peak of infections and the average number of affected people per day for each simulation. Furthermore, the RMSE value is reported to show how similar is the mentioned simulation is to real number of daily active people in the community. All results are means of 30 independent randomly seeded simulation runs.

Discussion and conclusion

Average clustering is a probe for the existence of structural holes in a network and the growth in average clustering specify the desired social distancing to lead less contamination. Furthermore, the parameter of average global efficiency quantifies the exchange of information across the whole network and any reduction in average global efficiency indicates a decrease in spread of the disease. As it can be expected, Table 2 demonstrates that the household quarantine exhibits highest average clustering and lowest average global efficiency. It is obvious that having all hubs in active format, on the other hand, yields to minimum of average clustering and maximum of average global efficiency. As it can be seen in Table 2, opening the workplace hubs with workforce of 80%, reduces the average clustering significantly and increases the spread

Table 3: Different simulations based on various interventions.

Simulations	Status	Average of daily active infections	Peak daily active infections	RMSE
A	All hubs are active and in normal mode	123.39	95	74.11
S	Schools closure	80.46	105	43.21
M	Mosque closure	110.44	155	71.77
W	Workforce=25%	93.49	137	58.81
P	Physical shopping= 5%	120.99	170	67.81
SW	Schools closure+ (Workforce= 25%)	67.09	90	31.03
SP	School closure+ (Physical shopping=5%)	77.88	97	36.10
SM	School closure+ Mosque closure	46.24	65	39.40
WP	(Workforce=25%)+ (Physical shopping= 5%)	100.54	152	48.76
MW	Mosque closure+ (Workforce= 25%)	98.79	160	47.52
MP	Mosque closure+ (Physical shopping= 5%)	111.18	171	61.76
MWP	Mosque closure+ (Workforce= 25%)+ (Physical shopping= 5%)	98.87	160	48.89
SMW	School and mosque closure+ (Workforce= 25%)	30.94	38	46.65
SMP	School and mosque closure+ (Physical shopping= 5%)	44.61	65	36.20
SWP	School closure+ (Workforce= 25%)+ (Physical shopping= 5%)	64.0	82	35.20
SMWP	School and mosque closure+ (Workforce= 25%)+ (Physical shopping= 5%)	29.81	45	46.23
N	Quarantine (no hub is active)	13.23	21	60.47
SMWP$\star$	Schools closure+ (Workforce= 60%)+ (Physical shopping= 5%)+ (Mosque= 50%)	74.97	101	34.79
near-real	15 days simulation A+ 55 days simulation SMWP+ 50 days simulation SMWP$\star$	54.21	95	24.75

of disease with high average global efficiency. Moreover, opening the schools lead to moderate decrease in average clustering and relatively high rise in average global efficiency. Accordingly, intervention like school closure can be considered worth-while on transmitting the disease.

Figures 2 to 6 show the effect of interventions on the number of affected people during 120 days from the start of the pandemic. Interventions like school closure, mosque closure, reduction of the workforce to 25%, reduction of physical shopping to 5%, along with complete quarantine, a moderate version of mentioned interventions and the real data in the selected small community are considered. The mentioned figures show how effective could be an intervention by reducing the number of affected people. Furthermore, similarity of the simulation depicted as near-real data in Fig 6 to strategies that was really hold during the mentioned period of time indicates that the proposed method is capable of correct modelling of the interventions.

The results of Table 3 show that household quarantine reduces the average number of daily affected people to 13.23 people per day which is considerably lower than the case of no intervention which reaches to 123.39 individuals per day. In is interesting that according to the simulations, when considering only one

intervention at the time, the most effective intervention is school closure strategy that reduces the average number of active cases to 80.46 persons per day. However, the most effective intervention strategy seems to be Simulation SMWP with school and mosque closure and reduction of work force and physical shopping to 25% and 5%, respectively. It is expected that the average number of affected people would fall into 29.81 people per day in such a case.

The average number of active cases for the real data is about 54 person per day. The simulation named near-real shows the lowest RMSE in Table 3 and as demonstrated in Fig 6, is the best simulation that its outputs are near the real data.

Acknowledgments

The authors are grateful to Raheleh Kafieh for providing useful comments. We are also grateful to Atefeh Vaezi and Shaghayegh Haghjooy Javanmard for their assistance with data collection.

References

[1] Marriam Webster Dictionary. Pandemic. Available at: https://www.merriam-webster.com/dictionary/pandemic. (Accessed 2 November 2020).

[2] Iran Reports Its First 2 Cases of the New Coronavirus. New York Times. Archived from the original on 19 February 2020. Retrieved 19 February 2020.

[3] Coronavirus Kills Record-Breaking Number of Iranians in 24 Hours. IFP News. 10 March 2020. Archived from the original on 11 March 2020. Retrieved 11 March 2020.

[4] Public Health England. COVID-19: epidemiology, virology and clinical features. https://www.gov.uk/government/publications/wuhan-novel-coronavirus-background-information/wuhan-novel-coronavirus-epidemiology-virology-and-clinical-features (Accessed 14 March 2020).

[5] Australian Commonwealth Department of Health and Aging: Australian Health Management Plan for pandemic Influenza [http://flupandemic.gov.au/internet/panflu/publishing.nsf/Content/ahmppl-1]

[6] US Department Of Health and Human Services: Pandemic Influenza Plan [http://hhs.gov/pandemicflu/plan/]

[7] United Kingdom Department of Health: Pandemic flu: A national framework for responding to an influenza pandemic [http://dh.gov.uk/en/Publicationsandstatistics/Publications/ PublicationsPolicyAndGuidance/DH_080734]

[8] World Health Organization: Pandemic influenza preparedness and response [http://who.int/csr/disease/influenza/pipguidance2009/en/index.html]

[9] Thieme, H. R. Mathematics in population biology (Vol. 12). Princeton University Press; 2018.

[10] Sahafizadeh, E., Khajeian, M. A. Modeling the Dynamics and Forecasting the fourth Peak of COVID-19 in Iran Using PSO Algorithm. Epidemiology and Health System Journal, 2021; 8(4), 140-145.

[11] Bondy, J. A. and Murty, U. S. R. Graph theory. 2008.

[12] Erdő, P., and Rényi, A. On random graphs. Publicationes Mathematiques, 1959;6, 290–297.

[13] Milne, G. J., Kelso, J. K., Kelly, H. A., Huband, S. T., and McVernon, J. A small community model for the transmission of infectious diseases: comparison of school closure as an intervention in individual-based models of an influenza pandemic. PloS one, 2008;3(12), e4005.

[14] Guo, D., Li, K. C., Peters, T. R., Snively, B. M., Poehling, K. A., and Zhou, X. Multi-scale modeling for the transmission of influenza and the evaluation of interventions toward it. Scientific reports, 2015;5(1), 1–9.

[15] Yang, X., Xu, T., Jia, P., Xia, H., Guo, L., Zhang, L. and Ye, K., Transportation, germs, culture: a dynamic graph model of COVID-19 outbreak. Quantitative Biology 8.3, 2020;238–244.

[16] AlArjani, A., Nasseef, M.T., Kamal, S.M., Rao, B.S., Mahmud, M. and Uddin, M.S., Application of mathematical modeling in prediction of COVID-19 transmission dynamics. Arabian Journal for Science and Engineering, 2022; 47(8), 10163–10186.

[17] Latora, V., and Marchiori, M. Efficient behavior of small-world networks. Physical review letters, 2001;87(19), 198–701.

[18] Watts, D. J., and Strogatz, S. H. Collective dynamics of small-worldnetworks. Nature, 1998;393(6684), 440–442.

[19] Kemper, A. Valuation of network effects in software markets: A complex networks approach. Springer Science & Business Media, 2009.

[20] Li, M. Y., Graef, J. R., Wang, L., Karsai J. Global dynamics of a SEIR model with varying total population size. Mathematical biosciences. 1999;160(2),191–213.

[21] Diekmann, O., Heesterbeek, H., Britton, T. Mathematical tools for understanding infectious disease dynamics. Princeton University Press; 2012 .

[22] Ma, S. and Xia, Y. Mathematical understanding of infectious disease dynamics. World Scientific; 2009.

[23] Jones, N. R., Qureshi, Z. U., Temple, R. J., Larwood, J. P., Greenhalgh, T., and Bourouiba, L. Two metres or one: what is the evidence for physical distancing in covid-19?. bmj, 2020; 370.

[24] Davies, N. G., Klepac, P., Liu, Y., Prem, K., Jit, M., Eggo, R. M. Age-dependent effects in the transmission and control of COVID-19 epidemics. Nature medicine, 2020;26(8), 1205–1211.

[25] Barnston, A. G. Correspondence among the correlation, RMSE, and Heidke forecast verification measures; refinement of the Heidke score. Weather and Forecasting, 1992;7(4), 699–709.

e-mail: m.vahiddastjerdi@gmail.com
e-mail: bomoomi@iut.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Tikhonov regularization matrices based on some proper conditions

Somaieh Mohammady[1]
Department of Mathematics, Roudehen branch, Islamic Azad university, Roudehen, Iran

Abstract

Regularization methods are used to deal with difficulties of machine learning, image deblurring, ill-posed problems, etc. Tikhonov regularization is a well known one. In this research, some new Tikhonov regularization matrices are proposed. These new ones are considered based on some conditions which are proper to have a good regularization matrix. These matrices can improve the solution of the problem in which regularization method is employed.

Keywords: Tikhonov regularization, Singular value decomposition, Condition number, Filter factors.
Mathematics Subject Classification [2010]: 47A52, 65F22, 65F35

1 Introduction

Many science fields such as image deblurring, acoustics, quantum mechanics, air and water quality control and optimal control theory deal with ill-posed problems. So, researchers have focused on the solution of such problems.
A linear discrete ill-posed problem is the discretization of an ill-posed one and is considered as the following least-square problem:

$$\min_{x\in\mathbb{R}^n} \|Ax-b\|^2, \quad A\in\mathbb{R}^{m\times n}, \quad m\geq n, \tag{1}$$

where $\|.\|$ denotes the Euclidean vector norm,

$$b=\overline{b}+e, \tag{2}$$

and $e\in R^m$ represents the unknown noise vector.
The problem is approximating $\overline{x}$ which is the solution of $Ax=\overline{b}$, but $\overline{b}$ is unavailable. Therefore, approximating $\overline{x}$ will be done by solving the available problem (1). Since b is a noisy vector and A is an ill-conditioned matrix, hence the noise in the data may give rise to significant errors in $\overline{x}$. Researchers bilieve that regularization methods are essential to deal with such problems and the system must be regularized.

Theorem 1.1. *(Singular value decomposition) Suppose A be an $m\times n$ matrix. Then there exists a factorization, called singular value decomposition (SVD) of A of the form*

$$A=U\Sigma V^T, \tag{3}$$

where $\Sigma=diag[\sigma_1,\sigma_2,\cdots,\sigma_n]\in R^{m\times n}$ that $\sigma_1\geq\sigma_2\geq\cdots\geq\sigma_l>\sigma_{l+1}=\cdots=\sigma_n=0$ and $rank(A)=l$, $U=[u_1,u_2,\cdots,u_m]\in R^{m\times m}$, $U^TU=I$ and $V=[v_1,v_2,\cdots,v_n]\in R^{n\times n}$ in which $V^TV=I$.

[1]speaker

Proof. The reader can find the proof in [7]. □

Using the SVD of A, the solution of (1) is

$$x = \sum_{i=1}^{l} \frac{u_i^T b}{\sigma_i} v_i. \tag{4}$$

The organization of this paper is as follows. Reviewing the Tikhonov regularization (TR) methods and some new researchs on TR matrices are considered in Section 2. In Section 3, some new TR matrices based on some proper conditions are proposed. The advantages of these new matrices are shown by solving some numerical examples in Section 4.

2 Tikhonov regularization method and some new research aspects

The most well known approach of regularization is Tikhonov regularization (TR) [1–5], which is the replacement of the ill-posed problem by a nearby one that is less sensitive to perturbation. In general, Tikhonov regularization is the following least square problem:

$$\min_{x \in \mathbb{R}^n} \|Ax - b\|^2 + \|L_\lambda x\|^2, \tag{5}$$

and the solution of (5) by normal equation is

$$x_\lambda = (A^T A + L_\lambda^T L_\lambda)^{-1} A^T b, \tag{6}$$

where L_λ is called regularization matrix and λ is the regularization parameter. This parameter determines how well x_λ approximates $\overline{x}$ and how x_λ is sensitive to the error e in the available data b [14]. There are some methods to determine the regularization parameter λ. For more details, we refer the reader to [5, 8, 12, 13]. By choosing $L_\lambda = \lambda I$ in (5), the standard form of Tikhonov regularization (STR) could be obtained:

$$\min_{x \in \mathbb{R}^n} \|Ax - b\|^2 + \|\lambda x\|^2, \tag{7}$$

and the solution of STR is

$$x_\lambda = (A^T A + \lambda^2 I)^{-1} A^T b. \tag{8}$$

After using SVD, the regularized solution could be written as

$$x_{reg} = \sum_{i=1}^{l} f_i \frac{u_i^T b}{\sigma_i} v_i, \tag{9}$$

where $f_i, 1 \leq i \leq l$ are filter factors which show how the components are modified by TR method. It is clear that $0 \leq f_i \leq 1$ [1]. The filter factors of STR are:

$$f_i = \frac{\sigma_i^2}{\sigma_i^2 + \lambda^2}, \quad 1 \leq i \leq l. \tag{10}$$

By an appropriate choice of filter factors, the more desired results can be calculated by regularization. According to (6), selecting the regularization matrix have a great roll in regularized solution. This issue has been considered by researchers in the recent years. For instance, the authors of [6] constructed a new TR method and substitute (3) in (5)

$$\min_{x \in \mathbb{R}^n} \left\|U\Sigma V^T x - b\right\|^2 + \|L_\lambda x\|^2. \tag{11}$$

They supposed the following consideration

$$\widetilde{x} := V^T x, \quad \widetilde{b} := U^T b, \quad L_\lambda := D_\lambda V^T, \tag{12}$$

and therefore (11) can be converted to

$$\min_{\widetilde{x}} \left\| \Sigma\widetilde{x} - \widetilde{b} \right\|^2 + \|D_\lambda \widetilde{x}\|^2. \tag{13}$$

The solution of (13) is

$$\widetilde{x} = (\Sigma^T\Sigma + D_\lambda^2)^{-1}\Sigma^T\widetilde{b}. \tag{14}$$

Then the authors in [6] have proposed D_λ^2 as follows

$$D_\lambda^2 = diag[\underbrace{0, \cdots, 0}_{k}, \lambda^2 - \sigma_{k+1}^2, ..., \lambda^2 - \sigma_n^2]. \tag{15}$$

Now if k is chosen so that $\sigma_{k+1} < \lambda \leq \sigma_k$, then $\Sigma^T\Sigma + D_\lambda^2$ is obtained as

$$\Sigma^T\Sigma + D_\lambda^2 = diag[\sigma_1^2, \sigma_2^2, \cdots, \sigma_k^2, \lambda^2, \cdots, \lambda^2] \in R^{n\times n}, \tag{16}$$

Here, (15) is called new Tikhonov regularization matrix (NTR).
To have a good TR matrix, some conditions should be considered [10]: Decreasing the condition number $\Sigma^T\Sigma + D_\lambda^2$ prevents further propagation of noise in the solution. Also, it is important to decrease the norm of D_λ with the goal of making $\Sigma^T\Sigma + D_\lambda^2$ close to $\Sigma^T\Sigma$. Moreover, controlling the filter factors and keeping them in the interval $[0, 1]$ is necessary, as mentioned earlier.
To measure the norm of D_λ, the Frobenius norm is chosen in this research and this norm is calculated for a matrix $D \in \mathbb{R}^{n\times n}$ by

$$\|D\|_F = \sqrt{trace(D^T D)}.$$

The condition numbers and Frobenius norms of STR and NTR are presented below:

$$\|D_{STR}\|^2 = \left\|\lambda^2 I\right\| = \sum_{i=1}^{n} \lambda^2 = n\lambda^2, \qquad cond_{STR} = \frac{\sigma_1^2 + \lambda^2}{\sigma_n^2 + \lambda^2},$$

$$\|D_{NTR}\|^2 = (n-k)\lambda^2 - \sum_{i=k+1}^{n} {\sigma_i}^2, \qquad cond_{NTR} = \frac{\sigma_1^2}{\lambda^2}.$$

3 Some new suggestions as Tikhonov regularization matrices

In this research, two new regularization matrices are proposed according to the mentioned points in the previous section. To introduce these regularization matrices, (11) and (12) are considered. So the following diagonal matrix is suggested as below:

$$\Sigma^T\Sigma + D_{PTR1}^2 = diag[\sigma_1^2, \sigma_2^2, \cdots, \sigma_k^2, \sigma_{k+1}^2 + u^2, \cdots, \sigma_n^2 + u^2], \tag{17}$$

in which

$$D_{PTR1}^2 = diag[\underbrace{0, \cdots, 0}_{k1}, u^2, \cdots, u^2], \tag{18}$$

where $u^2 = \frac{n\lambda^2}{n-k1}$ and the index $k1$ is chosen so that the diagonal entries get non-increasing. Here, (18) is called PTR1 as the first new proposed Tikhonov regularization matrix.

The Frobenius norms and condition numbers of PTR1 are:

$$\|D_{PTR1}\|^2 = \sum_{i=k1+1}^{n} u^2 = n\lambda^2, \qquad cond_{PTR1} = \frac{\sigma_1^2}{\sigma_n^2 + u^2}.$$

The aim of PTR1 is that the Frobenius norms of STR and PTR1 are the same, but the condition number of PTR1 is less than the STR's one.
To introduce the second TR matrix, consider the following diagonal matrix:

$$\Sigma^T\Sigma + D_{PTR2}^2 = diag[\sigma_1^2 + \lambda^2, \sigma_2^2 + \lambda^2, \cdots, \sigma_k^2 + \lambda^2, 0, \cdots, 0], \tag{19}$$

in which

$$D_{PTR2}^2 = diag[\underbrace{\lambda^2, \cdots, \lambda^2}_{k}, -\sigma_{k+1}^2, \cdots, -\sigma_n^2], \tag{20}$$

where the index k is chosen so that $\sigma_{k+1} < \lambda \leq \sigma_k$. Here, (20) is called PTR2 as the second new proposed Tikhonov regularization matrix.
The Frobenius norms and condition numbers of PTR2 are presented below:

$$\|D_{PTR2}\|^2 = k\lambda^2 - \sum_{i=k+1}^{n} {\sigma_i}^2, \qquad cond_{PTR2} = \frac{\sigma_1^2}{\sigma_k^2 + \lambda^2}.$$

As can be easily seen, the aim of PTR2 is that not only the Frobenius norm, but also the condition number of PTR2 is less than the STR's ones. This shows that PTR2 has better property than STR.
Again, it is mentioned that filter factors must be in the interval $[0, 1]$. Now, these factors for STR, NTR, PTR1 and PTR2 are presented in the following:

$$f_i^{STR} = \frac{\sigma_i^2}{\sigma_i^2+\lambda^2} \quad i \geq 1,$$

$$f_i^{NTR} = \begin{cases} 1 & i \leq k, \\ \frac{\sigma_i^2}{\lambda^2} & i > k, \end{cases}$$

$$f_i^{PTR1} = \begin{cases} 1 & i \leq k1, \\ \frac{\sigma_i^2}{\lambda^2+u^2} & i > k1, \end{cases}$$

$$f_i^{PTR2} = \begin{cases} \frac{\sigma_i^2}{\sigma_i^2+\lambda^2} & i \leq k, \\ 0 & i > k. \end{cases}$$

The reader can easily verify that filter factors of PTR1 and PTR2 are in the interval $[0, 1]$.

4 Numerical expriments

We apply the Tikhonov regularization matrices to some test problems taken from the Regtools package [9]. All the computations were carried out in Matlab. In these examples the coefficient matrices are 100 by 100. A white Gaussian noise vector $e \in \mathbb{R}^m$ with zero mean is added to $\bar{b}$ according to (2) to yield the right-hand side b. The noise vector e is scaled to obtain a specified noise level defined by

$$\varepsilon = \frac{\|e\|}{\|\bar{b}\|}.$$

The relative error is computed by $\frac{\|x^{app}-\bar{x}\|}{\|\bar{x}\|}$ in which x^{app} shows the approximated solution of each TR methods of STR, NTR, PTR1 and PTR2.
In Tables 1,2 and 3, the average relative errors of test problems for different noise levels (100 runs for each noise level) are presented. The smallest average relative errors among previous works belong to PTR1 and PTR2.

Example 4.1. *The Fredholm integral equation of the first kind of problem* ***Deriv2*** *discussed in [3] is*

$$\int_0^1 k(s,t)f(t)dt = g(s), \quad 0 \le s \le 1. \tag{21}$$

The kernel is

$$k(s,t) = \begin{cases} s(t-1) & s < t, \\ t(s-1) & s \ge t, \end{cases}$$

where

$$f(t) = \begin{cases} t & s < 1/2, \\ 1-t, & s \ge 1/2, \end{cases}$$

and the right-hand side g is given by

$$g(s) = \begin{cases} (4s^3 - 3s)/24 & s < 1/2, \\ (-4s^3 + 12s^2 - 9s + 1)/24, & s \ge 1/2, \end{cases}$$

This problem is discretized by Galerkin method with orthonormal box functions which leads to produce a linear system with the coefficient matrix $A \in \mathbb{R}^{n\times n}$ and the right-hand side vector $\bar{b} \in \mathbb{R}^n$.

Table 1: The average relative error of **Deriv2** test problem for noise level 50% (Example 4.1).

	ETR	NTR	PTR1	PTR2
Relative error	$1.78 \cdot 10^{-1}$	$2.06 \cdot 10^{-1}$	$1.74 \cdot 10^{-1}$	$1.49 \cdot 10^{-1}$

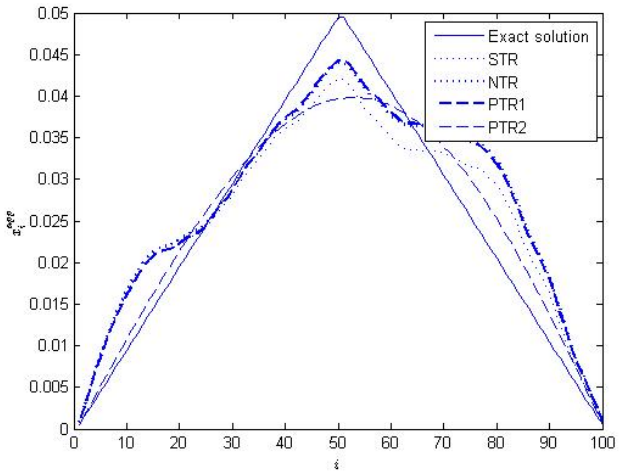


Figure 1: The approximated solutions for **Deriv2** test problem with noise level 50% (Example 4.1).

Example 4.2. *Consider* ***Heat*** *[2, 4], the inverse heat equation which is a Volterra integral equation of the first kind:*

$$\int_0^1 k(s,t)f(t)dt = g(s), \quad -\pi \le s \le \pi, \tag{22}$$

with kernel $k(s,t) = K(s-t)$, where

$$K(t) = \frac{t^{-\frac{3}{2}}}{2\sqrt{\pi}} \exp(-\frac{1}{4t}).$$

The exact solution is taken to be

$$f(t) = \begin{cases} \frac{300}{4}t^2 & 0 \le t \le \frac{1}{10}, \\ \frac{3}{4} + (20t-2)(3-20t) & \frac{1}{10} < t \le \frac{3}{20}, \\ \frac{3}{4}e^{2(3-20t)} & \frac{3}{20} < t \le \frac{1}{2}, \\ 0 & \frac{1}{2} < t \le 1. \end{cases}$$

The discretization of this problem is done by means of simple quadrature (midpoint rule) and a linear system with the coefficient matrix $A \in \mathbb{R}^{n\times n}$ and exact solution $\bar{x} \in \mathbb{R}^n$ is produced. The right-hand side vector $\bar{b} \in \mathbb{R}^n$ is obtained by $\bar{b} := A\bar{x}$.

Table 2: The average relative error of **Heat** test problem for noise level 0.01% (Example 4.2).

	ETR	NTR	PTR1	PTR2
Relative error	$1.82 \cdot 10^{-2}$	$1.89 \cdot 10^{-2}$	$1.72 \cdot 10^{-2}$	$1.78 \cdot 10^{-2}$

Example 4.3. *The Fredholm integral equation of the first kind of problem **Phillips** discussed in [11] is*

$$\int_{-6}^{6} k(s,t)f(t)dt = g(s), \quad -6 \le s \le 6. \tag{23}$$

The kernel is

$$k(s,t) = x(s-t),$$

where

$$x(t) = \begin{cases} 1+\cos(\frac{\pi}{3}t) & |t| < 3, \\ 0 & \textit{elsewhere}\ , \end{cases}$$

and the right-hand side g is given by

$$g(s) = (6-|s|)(1+\frac{1}{2}cos(s\frac{\pi}{3})) + \frac{9}{2\pi}sin(|s|\frac{\pi}{3}).$$

The exact solution is $f(t) = x(t)$. It is discretized by Galerkin method and the matrix $A \in \mathbb{R}^{m\times n}$ and $\bar{b} \in \mathbb{R}^m$ are obtained.

Table 3: The average relative error of **Phillips** test problem for noise level 10% (Example 4.3).

	ETR	NTR	PTR1	PTR2
Relative error	$8.46 \cdot 10^{-2}$	$8.23 \cdot 10^{-2}$	$7.98 \cdot 10^{-2}$	$7.91 \cdot 10^{-2}$

5 Conclusions

In this study, Some new Tikhonov regularization matrices are proposed. The proposed ones is based on some recent works on TR method and proper conditions. The reported numerical examples show that the proposed matrices have the smallest average relative error among previous works. Therefore the most accurate computed solutions are obtained by these matrices.

References

[1] J. Baumeister, Stable Solution of Inverse Problems, Vieweg, Braunschweig, 1987.

[2] A. S. Carasso, Determining surface temperatures from interior observations, SIAM J. Appl. Math., 42 (1982), pp. 558-574.

[3] L. M. Delves, J. L. Mohamed, "Computational Methods for Integral Equations", Cambridge University Press, 1985, p. 310.

[4] L. Eldén, The numerical solution of a non-characteristic Cauchy problem for a parabolic equation; in P. Deuflhart, E. Hairer (Eds.), Numerical Treatment of Inverse Problems in Differential and Integral Equations, BirkhÄauser, Boston, 1983.

[5] H.W. Engl, M. Hanke, A. Neubauer, Regularization of Inverse Problems, Kluwer, Dordecht, 1996.

[6] M. Fuhry, L. Reichel, A new Tikhonov regularization method, J. Numer. Algorithms., 59 (2012), pp. 433-445.

[7] G. H. Golub and C. F. Van Loan, Matrix Computations, Third Edition, the Johns Hopkins University Press, Baltimore, MD, 1996.

[8] P. C. Hansen, Rank-Deficient and Discrete Ill-Posed Problems: Numerical Aspects of Linear Inversion, SIAM, Philadelphia, 1997.

[9] P. C. Hansen, Regularization tools version 4.0 for Matlab 7.3, J. Numer. Algorithms., 46 (2007), pp. 189-194.

[10] S. Mohammady, M.R. Eslahchi, Extension of Tikhonov regularization method using linear fractional programming, J. Comput. Appl. Math., 371 (2020), p. 112677.

[11] D. L. Phillips, A technique for the numerical solution of certain integral equations of the first kind, J. Assoc. Comput. Mach., 9 (1962), pp. 84-97.

[12] M. Rezghi, S. M. Hosseini, A new variant of L-curve for Tikhonov regularization, J. Comput. Appl. Math., 231 (2009), pp. 914-924.

[13] L. Reichel, H. Sadok, A new L-curve for ill-posed problems, J. Comput. Appl. Math., 219 (2008), pp. 493-508.

[14] A. N. Tikhonov, Solution of incorrectly formulated problems and the regularization method, Soviet Math. Dokl., 4 (1963), pp. 1035-1038; English translation of Dokl. Akad. Nauk. SSSR., 151 (1963), pp. 501-504.

Email: s.mohammady@modares.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A Survey on Lee Weight

Farzaneh Farhang Baftani[a 1]
Ali Bagheri Vakilabad[a]
Nastaran Valizadeh[a]

[a] Department of Mathematics, Ardabil Branch, Islamic Azad University, Ardabil, Iran.

Abstract

Motivated by finding the differences and similarity between Hamming weight and Lee weight, we decided to investigate Lee weight and Generalized Lee Weight (GLW). Lee weight and its generalization have not only similar theorems but also different theorems as Hamming weight has. In this paper, some of them have been declared.

Keywords: Lee Weight, Generalized Lee Weight, Linear Code, Minimum Lee Weight

AMS Mathematical Subject Classification [2010]: 94B65

1 Introduction

Suppose that $\mathbb{Z}_m$ is code alphabet. For any i, $0 \leq i \leq m$, we denote the Lee weight of i by $wt_L(i)$ and define it as $wt_L(i) = min\{i, m-i\}$. For instance, if $m = 4$, namely in $\mathbb{Z}_4$, we have

$$wt_L(0) = min\{0, 4-0\} = min\{0, 4\} = 0$$

$$wt_L(1) = min\{1, 4-1\} = min\{1, 3\} = 1$$

$$wt_L(3) = min\{3, 4-3\} = min\{3, 1\} = 1$$

$$wt_L(2) = min\{2, 4-2\} = min\{2, 2\} = 2.$$

In brief, we have

$$wt_L(0) = 0, wt_L(1) = wt_L(3) = 1, wt_L(2) = 2.$$

The Lee metric on Z_m^n is defined by

$$wt_L(a) = \Sigma_{i=1}^{n} wt_L(a_i),$$

where the sum is defined in N_0, the set of non-negative integers, and a_i is the $i-$ th coordinate of a. Also, Lee distance is defined as $d_L(x, y) = wt_L(x - y)$. For more information, see [8].
The concept of Generalized Hamming Weight (GHW) introduced by V. K. Wei in [9]. After this work, several papers were published on this topic, See [1], [4] and [5]. Moreover, Generalized Lee Weight (GLW)

[1] speaker

for codes over $\mathbb{Z}_4$ introduced by B. Hove in [7] for the first time. The relationship between GHW and GLW has been presented in this paper. After him, several authors investigated this concept, see[2], [3] and [6].
A code of length n over $\mathbb{Z}_4$ is a subset of the free module $\mathbb{Z}_4^n$ and it is called linear if it is a $\mathbb{Z}_4-$ submodule of $\mathbb{Z}_4^n$.
Let C be a linear code of length n over $\mathbb{Z}_4$ and Let $M(C)$ be the $|C| \times n$ array of all code words in C. The code word in first row of $M(C)$ has 0, 1, 2 or 3 as its coordinates. Since any multiplication of these coordinates will be in next rows, so the following matrix is a part of $M(C)$:

$$\mathrm{M}' = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The other parts of $M(C)$ are the permutation of matrix M'. Note that the number of columns and rows of this matrix depend on the lenght and the number of code words of code C.(Author)
Now, we can have the following definition:

Let C be a linear code of length n over Z_4 and Let $M(C)$ be the $|C| \times n$ array of all code words in C. Each arbitrary column of $M(C)$, say c, corresponds to the following three cases:
i) c contains only 0
ii) c contains 0 and 2 equally often
iii) c contains all elements of Z_4 equally often,

We define the Lee support weight of these columns as 0, 2 and 1, respectively. Also, we define the Lee support weight of code C, denoted by $wt_L(C)$, as the sum of the Lee support weights of all columns of $M(C)$. As an example, let $C = \{(0,0,0),(1,2,3),(3,2,1),(2,2,1),(1,2,2),(2,0,3),(3,0,0),(0,0,2)\}$. Hence we have

$$M(C) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 2 & 2 \\ 2 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

If c_i be the i-th column of $M(C)$, then we have $wt_L(c_1) = 1$, $wt_L(c_2) = 2$ and $wt_L(c_3) = 1$. Hence we obtain that $wt_L(C) = 1 + 2 + 1 = 4$.

Let C be a code of length n over ring Z_4. The rank of C, denoted by $rank(C)$, is defined as the minimum number of generators of C, See [2]. For $1 \leq r \leq rank(C)$, the r-th generalized Lee weight with respect to $rank$ (GLWR) for C, denoted by $d_r^L(C)$, is defined as follows

$$d_r^L(C) = min\{wt_L(D); D \text{ is a } Z_4 - \text{submodule of C with rank(D)} = r\}.$$

In this paper we will show by $C = [n, k]$, the linear code C of length n and $rank = k$.

There is another extension of Lee Weight which represented by B. Yildiz, but note that it is different than the above definition. For more details, see [10]

2 Main results

Remark 2.1. Let $x = (x_1, x_2, ..., x_n) \in Z_4^n$. Then, we have $wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$.

Remark 2.2. Let C be a code of one generator, say x, then, we have $wt_L(C) = wt_L(x)$. (Author)

Proof. We have $C =< x >$. So, $wt_L(C) = wt_L < x >$. Let $M(< x >)$ is the array of code words of C. Since $wt_L(x) = \sum_{i=1}^{n} wt_L(x_i)$ and $wt_L(< x >)$ is based on $M(< x >)$, it is sufficient to compare $wt_L(x_i)$ and the Lee support weight of the corresponding columns in $M(< x >)$, $i-$ th column. If 1 is the $i-$ th coordinate of x, then we will have $1 = wt_L(x_i)$. Moreover, $i-$ th column of $M(< x >)$ contains all elements of Z_4 since this columns is made by 1. So, the Lee wight of this column is 1. Also, if 2 is the $i-$ th coordinate of x, then we will have $2 = wt_L(x_i)$. Moreover, $i-$ th column of $M(< x >)$ is composed of $0, 2$ equally since it is made by 2. Hence, the Lee weight of this column is 2.
We have the similar method for 0 and 3. Finally, $wt_L(x_i) = wt_L(c_i)$, where c_i is the $i-$ th column in $M(C)$. So, the result will be obtained.(Author) □

Remark 2.3. For code C of lenght n, we have $d_1^L(C) = wt_L(C) = wt_L(x)$.(Author)

Proof. Let $d_1^L(C) = t$ and s is the minimum Lee weight of the code. From definition of GLW, we have

$$\exists D; D \leqslant C, rank(D) = 1, wt_L(D) = t.$$

Let $x \in D$ is a generator of D. So, $D =< x >$. Then, we have

$$wt_L(C) \leqslant wt_L(D) = wt_L(< x >) = wt_L(x) = t \Rightarrow$$

$$wt_L(C) \leqslant t \Rightarrow s \leqslant t. \tag{1}$$

On the other hand, s is the minimum Lee weight of code C, then we have

$$\exists x \in C; wt_L(x) = s.$$

Now, let $D' =< x >$. We obtain

$$d_1^L(C) \leqslant wt_L(D') = wt_L(< x >) = wt_L(x) = s \Rightarrow$$

$$d_1^L(C) \leqslant s \Rightarrow t \leqslant s. \tag{2}$$

Finally, by using Eqs 1 and 2, we obtain that $t = s$. □

Here is a detailed proof written by author for the following theorem presented in [2]

Theorem 2.4. *[2] Let C be a code of length n over $\mathbf{Z_4}$ in which ,$rank(C) = 2$. Then, there exists $v \in C$ that*

$$wt_L(v) \leqslant wt_L(C).$$

Proof. Let C is a code of length n over $\mathbb{Z}_4$ and $C =< x, y >$. In the other words, x, y are the generators of code C. Consider that $rank(C) = 2$. Let $(x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$. For any arbitrary $i, 1 \leqslant i \leqslant n$, we have the following cases

(1) $x_i = 0, y_i = 2$
(2) $x_i = 2, y_i = 0$
(3) $x_i = 2, y_i = 2$

By calculating $x_i + y_i$ for the above cases, respectively, we will gain

$x_i + y_i = 2$
$x_i + y_i = 2$
$x_i + y_i = 0.$

By means of definition of $wt_L(C)$, the construction of $M(C)$ and the definition of $wt_L(x+y)$, it is clear that $wt_L(x+y) \leq wt_L(C)$,for the above cases. Now, we consider the cases that the values of x_i and y_i will be chosen from the set $\{1,3\}$. Let the number of i' s in which $x_i = y_i = 1$ equals n_1 and the number of i' s in which $x_i = y_i = 3$ equals n_2. Moreover, the number of i' s in which $x_i = 1, y_i = 3$ equals n_3 and the number of i' s in which $x_i = 3, y_i = 1$ equals n_4. we have the following cases:
(i) If

$$|\{i : x_i = y_i = 1\text{or}3\}| \leq |\{i : \{x_i, y_i\} = \{1,3\}\text{or}\{3,1\}|$$

the value which is added to $wt_L(C)$ is $n_1 + n_2 + n_3 + n_4$ but the value which is added to $wt_L(x+y)$ is $2(n_1+n_2)$. So, we have

$$wt_L(x+y) = 2(n_1+n_2) = n_1+n_2+n_1+n_2 \leq n_1+n_2+n_3+n_4 = wt_L(C).$$

Finally, we have $wt_L(x+y) \leq wt_L(C)$.
(ii) If

$$|\{i : x_i = y_i = 1 \text{ or } 3\} \geq |\{i : \{x_i, y_i\} = \{1,3\}\text{or}\{3,1\}|$$

by the similar method in previous case, we have $wt_L(x+y) \geq wt_L(C)$. By calculating $wt_L(x+3y)$, all coordinates of the left side set are zero and all coordinates of the right side set are 2, so the value $2(n_3+n_4)$ is added to $wt_L(x+3y)$. From the construction of $M(C)$, it is clear that the value $n_1+n_2+n_3+n_4$ is added to $wt_L(C)$. So, we have

$$wt_L(x+3y) = 2(n_3+n_4) = n_3+n_4+n_3+n_4 \leq n_1+n_2+n_3+n_4 = wt_L(C).$$

Finally, we obtain $wt_L(x+3y) \leq wt_L(C)$. Regarding the above investigation, there exists a none- zero code word, say v, in C in which $wt_L(v) \leq wt_L(C)$. □

The following theorem is in [2] and we have written an expanded proof for it that makes it easier to find out.

Theorem 2.5. *[2]*
Let C_1, C_2 be $[n : k_1, k_2]$ codes over $\mathbb{Z}_4$ Then

$$wt_L(C) = \frac{4}{|C|}\sum_{x\in C}(wt_L(x) - wt(x)) = \frac{4}{4^{k_1-1}\times 2^{k_2}}\sum_{x\in C}|\{i : x_i = 2\}|,$$

where $wt(x)$ is the Hamming weight of vector x

Proof. Let $M(C)$ is the array of code words of C, n_0 is the number of the columns that have 0 and 2 equally and n_1 is the number of the columns that have the elements of $\mathbb{Z}_4$ equally. It is clear that

$$wt_L(C) = 2n_0 + n_1.$$

Now, we calculate $\Sigma wt_L(x)_{x\in C}$. We acclaim that

$$\sum_{x\in C} wt_L(x) = n_0|C| + n_1|C|.$$

For $\sum_{x\in C} wt_L(x)$, we calculate the sum of the Lee weight of all coordinates. Any column which contains 0 and 2 equally, will add $|C|$ to the recent summation. Note that $wt(2) = 2$, $wt(0) = 0$, and this causes that $wt_L(2)$ cover the $wt_L(0)$ in this column. Since the number of the columns of this type is n_0, then $n_0|C|$ will be added to $\sum_{x\in C} wt_L(x)$.

Similar to the above, in the columns that contain the elements of $\mathbb{Z}_4$ equally, the coordinates belonging to the set $\{1,3\}$ add 1+1 and the coordinates belonging to the set $\{0,2\}$ add 0+2 together to above summation. Therefore, these columns add $n_1|C|$. Finally, we have

$$\sum_{x\in C} wt_L(x) = n_0|C| + n_1|C| = n_0\frac{|C|}{2}\times 2 + n_1(\frac{|C|}{4} + \frac{|C|}{4}\times 2 + \frac{|C|}{4}).$$

On the other hand, when we calculate the sum of Hamming weights of code words of C, $\sum_{x\in C} wt(x)$, any column that have 0 and 2 equally, will add $\frac{|C|}{2}$ to $\sum_{x\in C} wt(x)$. Note that $wt(0) = 0$ and $wt(2) = 1$. So, all of columns of this type, will add $n_0\frac{|C|}{2}$ to $\sum_{x\in C}(wt(x))$. Moreover, the number of zero's in the columns that have the elements of $\mathbb{Z}_4$ equally, is $\frac{1}{4}\ |C|$ and the number of non - zero elements is

$$|C| - \frac{1}{4}|C| = \frac{3}{4}|C|.$$

Finally, all of these columns will add $n_1\frac{3}{4}|C|$ to

$$\sum_{x\in C} wt(x).$$

Hence, we obtain

$$\sum_{x\in C} wt(x) = n_0\frac{|C|}{2} + n_1\frac{3}{4}|C| = n_0\frac{|C|}{2} + n_1(\frac{|C|}{4} + \frac{|C|}{4} + \frac{|C|}{4})$$

Therefore,

$\sum_{x\in C}(wt_L(x) - wt(x)) = \frac{|C|}{4}[(4n_0 + 4n_1) - (2n_0 + 3n_1) =$

$$\frac{|C|}{4}(2n_0 + n_1) = \frac{|C|}{4}wt_L(C) \Longrightarrow \sum_{x\in C}(wt_L(x) - wt(x)) = \frac{|C|}{4}wt_L(C)$$

$$\Longrightarrow\ wt_L(C) = \frac{4}{|C|}\sum_{x\in C}(wt_L(x) - wt(x)) = \frac{4}{4^{k_1}\times 2^{k_2}}\sum_{x\in C}(wt_L(x) - wt(x)).$$

Since

$$wt_L(0) = 0 = wt(0),$$
$$wt_L(1) = 1 = wt(1),$$
$$wt_L(3) = 1 = wt(3),$$

for 0, 1 and 3, we have $wt_L(x) - wt(x) = 0$ but for 2, we have

$$2 = wt_L(2) \neq wt(2) = 1 \Longrightarrow\ wt_L(2) - wt(2) = 2 - 1 = 1,$$

Hence, we obtain

$$\sum_{x\in C}(wt_L(x) - wt(x)) = \sum_{x\in C}|\{i : x_i = 2\}|$$

In the other words, only 2 add the value 1 to

$$\sum_{x\in C}(wt_L(x) - wt(x)).$$

□

The following theorems are similar to that we have on Hamming weight and Generalized Hamming Code (GHW) for ocde.

Theorem 2.6. *[3] For any x and y in ring $\mathbb{Z}_m$,m is an arbitrary power of 2, we have*

$$wt_L(x) + wt_L(y) \geq wt_L(x+y) \geq wt_L(x) - wt_L(y).$$

Theorem 2.7. *[6] Let C_i be linear codes of length n_i over $\mathbb{Z}_4$ for $i = 1, 2$. Let $C = C_1 \oplus C_2$, then we have*

$$d_1^L(C) = min\{d_1^L(C_1), d_1^L(C_2)\}.$$

$$d_2^L(C) = min\{d_2^L(C_1), d_2^L(C_2), \frac{1}{4}[d_1^L(C_1) + d_1^L(C_2)]\}.$$

Acknowledgment

Authors would like to thank all members of the conference committee who make great attempt to hold this conference every year.

References

[1] S. T. Dougherty and S. Han, *Higher Weights and Generalized MDS Codes*, Korean Math. Soc ,No. 6(2010), pp. 1167-1182.

[2] S.T. Dougherty, M. K. Gupta and K. Shiromoto, *On Generalized weights for codes over Z_k, $Australian Journal of Mathematics, Vol.31, (2005), 231-248$.*

[3] F. Farahang Baftani, Lee Weight and Generalized Lee Weight for Codes over $\mathbf{Z_{2^n}}$, Mathematics Interdisciplinary Research, Vol 8, Issue 1(2023), 27-33.

[4] F. Farhang Baftani, GHW for (x, x+y)- construction of codes, Advanced Studies: Euro-Tbilisi Mathematical Journal, Vol 16, Issue 1(2023), 1-6.

[5] F. Farhang Baftani and H. R. Maimani, The Weight Hierarchy of Ham (r, q), Italian Journal of Pure and applied Mathematics, No 45, May 2021.

[6] F. Farhang Baftani, Lee Weight for Direct Sum of Codes, Communications in Combinatorics, Cryptography Computer Science 2021 (1), 44-49.

[7] B.Hove , Generalized Lee Weights for Codes over $\mathbf{Z_4}$, IEEE,1997.

[8] J. H. Van Lint, *Introduction to Coding Theory, Springer- Verlag, **(1999)**.*

[9] V. K. Wei, Generalized Hamming Weights for linear codes, IEEE Trans. Inform. Theory 37(1991) ,no.5,1412-1418

*[10] B.Yildiz, Z. Odemis Ozger, A Generalization of the Lee Weight to Z_{p^k}, TWMS J. App. Eng. Math **2(2)**(2012)* $145-153$

e-mail: farhangfarzaneh1006@gmail.com
e-mail: fa.farhang@iau.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Connected Ramsey number of stars in multicolorings

Ghaffar Raeisi[1]
Department of Mathematical Sciences, Shahrekord University, Shahrekord, Iran

Abstract

Graph G is called totally connected if both G and G^c (the complement of G) are connected. For two graphs G and H, the connected Ramsey number $R_c(G,H)$ is defined as the smallest positive integer p such that there exists a totally connected graph on p vertices, and if K is a totally connected graph on at least p vertices, then either K contains a copy of G or K^c contains a copy of H. In this paper, we generalize this definition to the multicolor case and we give the exact value of the connected Ramsey number of arbitrary stars.

Keywords: Ramsey number, Connected Ramsey number , Totally connected, Star graph
Mathematics Subject Classification [2010]: 05C15, 05C55

1 Introduction

In this paper, we are only concerned with undirected simple finite graphs and we follow [2] for terminology and notations not defined here. Recall that an *edge coloring* of a graph $G = (V, E)$ is assigning colors to each edge $e \in E$ so that any adjacent edges receive different colors. The minimum number of colors required for an edge coloring of G is called the *edge chromatic number* of G and denoted by $\chi'(G)$.

For given graphs A and B, the *Ramsey number* $R(A, B)$ is the smallest integer p such that for any graph G of order at least p, either $A \subseteq G$ or $B \subseteq G^c$, where $A \subseteq G$ means that A is a subgraph of G and G^c denotes the complement of G. In the other words, $R(A, B)$ is defined as the smallest positive integer p such that if the edges of the complete graph K_p are colored with two colors, say red and blue, then K_p contains either a red copy of A or a blue copy of B. In general, let $G_1, G_2, \ldots, G_t$ be given graphs. The *multicolor Ramsey number* $R(G_1, G_2, \ldots, G_t)$, is defined to be the smallest positive integer p such that if the edges of the complete graph K_p are colored in any fashion with t colors, then for some i, $1 \leq i \leq t$, the spanning subgraph whose edges are colored with the i-th color, contains a copy of G_i.

Since their time, and particularly since the 1970's, Ramsey theory has grown into one of the most active areas of research within combinatorics, overlapping variously with graph theory, number theory, geometry and logic. A survey including many results on Ramsey theory, can be found in [7]. Frequently, the lower bounds for the multicolor Ramsey numbers are obtained from canonical types of graphs where in any case one of the colors induced a disconnected graph. Thus, it seems that if the restriction that both G and G^c be connected graphs is placed on our graphs, then we may not need to require $R(A, B)$ vertices in G in order to insure that $A \subseteq G$ or $B \subseteq G^c$. This possibility was investigated by Sumner [8].

Formally, a graph G is called *totally connected* if both G and G^c are connected. For two graphs G and H, the *connected Ramsey number* $R_c(G, H)$ is the smallest integer p such that there exists a totally

[1]speaker

connected graph of order p, and if K is a totally connected graph on at least p vertices, then K contains a copy of G or K^c contains a copy of H. Clearly $R_c(G,H) \leq R(G,H)$. Sumner [8] proved that if G and H contains no bridges, then $R_c(G,H) = R(G,H)$. In addition, the author determine the exact value of $R_c(P_m,P_n)$, where P_n denotes a path with n vertices. Since every totally connected graph contains a copy of P_4, so $R_c(P_4,G) = 4$, for all graphs G. Note that there are some graphs such that the difference between the connected Ramsey number and the ordinary Ramsey number of these graphs is sufficiently large. For instance, for given n-vertex graph G, $R_c(P_3,G) = 4$ but $R(P_3,G) \geq n$. In [9], $R_c(G,H)$ is calculated where G is a path and H is either a cycle, star or a complete graph and also in the case that G is a star and H is a complete graph.

We say that an edge coloring of K_p with t colors is *totally connected* if the induced subgraph on edges in each color is a connected spanning subgraph of K_p. By this definition, the connected Ramsey number $R_c(G,H)$ is the smallest positive integer p such that K_p has a totally connected two-edge coloring and any totally connected two-edge coloring of K_p contains either a copy of G in color one or a copy of H in color two. We can extend this concept for more than two graphs. For given graphs $G_1, G_2, \ldots, G_t$, the *multicolor connected Ramsey number* $R_c(G_1, G_2, \ldots, G_t)$ is the smallest positive integer p such that K_p has a totally connected t-edge coloring and for any totally connected t-edge coloring of K_p, there exists a copy of G_i in color i, for some i, $1 \leq i \leq t$. In this note, we follow the recent notations to calculate the exact value of the multicolor connected Ramsey number $R_c(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t})$, where $K_{1,n}$ is the star graph with n leaves.

2 Connected Ramsey number of stars

In this section, we determine the exact value of the connected Ramsey number $R_c(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t})$. For this purpose, we need some definitions and notations. A graph G is called *H-free* if it does not contain H as a subgraph. We denote by $ex(p,H)$, the maximum possible number of edges in a graph on p vertices which is H-free. It is easy to see that

$$ex(p, K_{1,n}) \leq \frac{p(n-1)}{2}.$$

To establish the main result, we give some useful lemmas.

Lemma 2.1. Let l be a positive integer. Then,

(i) The graph K_{2l} can be decomposed into l hamiltonian paths.

(ii) The graph K_{2l+1} can be decomposed into l hamiltonian cycles.

Proof. (i) Let $V = \{v_1, v_2, \ldots, v_{2l}\}$ denote the vertex set of the complete graph K_{2l}. For $i \in \{1, 2, \ldots, l\}$, set $P_i = v_i v_{i-1} v_{i+1} v_{i-2} \ldots v_{i+p-1} v_{i+l}$, where all subscripts are taken modulo $2l$. It is easy to see that $P_1, P_2, \ldots, P_l$ are p edge-disjoint hamiltonian paths decomposing K_{2l}

(ii) By the previous part, we can decompose K_{2l} into l hamiltonian paths. Adding the last vertex of K_{2l+1} yields l hamiltonian cycles, which decompose K_{2l+1}.

■

Lemma 2.2. Assume that $G_1, G_2, \ldots, G_t$ are arbitrary graphs and let H_i, $1 \leq i \leq t$, be a subgraph of G_i. Then,

(i) $R_c(G_1, G_2, \ldots, G_t) \geq 2t$.

(ii) $R_c(H_1, H_2, \ldots, H_t) \leq R_c(G_1, G_2, \ldots, G_t)$.

Proof. (i) We prove that K_{2t} is the smallest graph which can be decomposed into t connected spanning subgraphs, which means that $2t$ is the smallest integer such that K_{2t} has a totally t-edge coloring. To see this, let K_n decomposed into t connected spanning subgraphs. Since each subgraph has at least $n-1$ edges, then $\frac{n(n-1)}{2} \geq t(n-1)$ and hence, $n \geq 2t$. Also, by Lemma 2.1, K_{2t} has t connected spanning subgraph. Therefore, $R_c(G_1, G_2, \ldots, G_t) \geq 2t$.

(ii) By the definition, every totally connected t-edge coloring of $K_{R_c(G_1,G_2,\ldots,G_t)}$ contains a copy of G_i in color i for some i, $1 \leq i \leq t$, and hence contains a copy of H_i in color i. ■

In the following theorem, we give the exact value of the connected Ramsey number of P_4 versus arbitrary graphs.

Theorem 2.3. Let $G_2, G_3, \ldots, G_t$ be arbitrary graphs. Then

$$R_c(P_4, G_2, \ldots, G_t) = 2t.$$

Proof. The lower bound follows from part (i) of Lemma 2.2. Moreover, any totally connected t-edge coloring of K_{2t} contains a copy of P_4 in color one as a subgraph. So, we obtain that $R_c(P_4, G_2, \ldots, G_t) \leq 2t$, completing the proof. ■

Combining Lemma 2.2 and Theorem 2.3, we obtain the following corollary.

Corollary 2.4. Let $G_2, G_3, \ldots, G_t$ be arbitrary graphs. Then

$$R_c(K_{1,2}, G_2, \ldots, G_t) = 2t.$$

It is well-known that for odd n, the edge chromatic number of the complete graph on n vertices is n. Let $V = \{v_0, v_1, \ldots, v_{n-1}\}$ be the vertex set of K_n. Put the vertices of K_n in the form of a regular polygon and color the edge v_iv_j with color α_{i+j}, where all subscripts are taken modulo n. Assigning these colors to edges of K_n, yields an n-edge coloring of K_n, where n is odd. Now consider the complete graph on n vertices when n is even. The subgraph $K_n - v_{n-1}$ is $(n-1)$-edge colorable, by the above method. By this coloring, the color which is not appeared to the edges incident to v_i is α_{2i}, where subscripts are taken modulo $n-1$. For each $i \in \{0, 1, 2, \ldots, n-2\}$ let $\beta_i := \alpha_{2i} \pmod{n-1}$. Since $n-1$ is odd, we have $\beta_i \neq \beta_j$, when $i \neq j$. Thus, assigning β_i to edge v_iv_{n-1}, we obtain an $(n-1)$-edge coloring of K_n when n is even. From now on, when we say the "desired edge coloring of K_n" we mean the mentioned edge colorings of K_n.

Lemma 2.5. Assume that $n_1, n_2, \ldots, n_t$ are integers grater than two and Σ denotes $\Sigma_{i=1}^{t}(n_i - 1)$. Then, $K_{\Sigma+1}$ can be decomposed into t connected spanning $(n_i - 1)$-regular subgraphs if and only if Σ is odd or Σ is even and all n_i's are odd.

Proof. Let Σ be odd or Σ be even and all n_i's be odd. In any case, we establish the existence of the desired subgraphs which decompose $K_{\Sigma+1}$. First, assume that Σ is odd. Since Σ is odd, so $\Sigma + 1$ is even and by the desired coloring of $K_{\Sigma+1}$, there exists a proper edge coloring of $K_{\Sigma+1}$ with Σ colors $\alpha_1, \alpha_2, \ldots, \alpha_\Sigma$. Partition the above Σ colors into t classes $V_1, V_2, \ldots, V_t$ of sizes $n_1 - 1, n_2 - 1, \ldots, n_t - 1$, respectively. Let H_i be the subgraph of $K_{\Sigma+1}$ induced by the edges of color $\alpha \in V_i$. Since $n_i \geq 3$, each H_i is connected and clearly is a spanning $(n_i - 1)$-regular subgraph of $K_{\Sigma+1}$. Obviously, $H_1, H_2, \ldots, H_t$ decompose $K_{\Sigma+1}$, which completes the proof of lemma in this case.

Now, assume that Σ is even and all n_i's are odd. Since $\Sigma+1$ is odd, by part (ii) of Lemma 2.1, $K_{\Sigma+1}$ can be decomposed into $\frac{\Sigma}{2}$ hamiltonian cycles. Partition these hamiltonian cycles into t classes $V_1, V_2, \ldots, V_t$ of sizes $(n_1 - 1)/2, (n_2 - 1)/2, \ldots, (n_t - 1)/2$, respectively. Assume that H_i is the subgraph of $K_{\Sigma+1}$ induced by the edges in V_i. Clearly, each H_i is a connected spanning subgraph of $K_{\Sigma+1}$ which is $(n_i - 1)$-regular and all H_i's decompose K_Σ.

For the converse, suppose that $K_{\Sigma+1}$ is decomposed into t connected spanning (n_i-1)-regular subgraphs. On the contrary, let Σ and at least one n_i be even. Without lose of generality, we may assume that n_t is even. Let H be the connected spanning (n_t-1)-regular subgraph of $K_{\Sigma+1}$ which appear in the decomposition of $K_{\Sigma+1}$. Since H is a spanning subgraph of $K_{\Sigma+1}$, so H has odd number of vertices. Also the degree of each vertex of H is odd, since H is (n_t-1)-regular and n_t is even. Since we are seeking a regular graph of odd order and degree, such a graph does not exist, a contradiction. This contradiction shows that Σ is odd or Σ is even and all n_i's are odd, which completes the proof of lemma.

■

Now, we are ready to establish the main result, which determine the exact value of the multicolor connected Ramsey number of stars.

Theorem 2.6. Assume that $n_1, n_2, \ldots, n_t$ are integers grater than two, Σ denotes $\Sigma_{i=1}^{t}(n_i-1)$ and R_c denotes the connected Ramsey number $R_c(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t})$.

(i) If either Σ is odd or Σ is even and all n_i are odd, then $R_c = \Sigma + 2$.

(ii) If Σ is even and at least one n_i is even, then $R_c = \Sigma + 1$.

Proof. First, we give a totally connected t-edge coloring of K_{R_c-1} with colors $\alpha_1, \alpha_2, \ldots, \alpha_t$ such that for $i = 1, 2, \ldots, t$, the complete graph K_{R_c-1} contains no copy of K_{1,n_i} in color α_i.

(i) Assume that Σ is odd or Σ be even and all n_i are odd. Set $\Sigma y = \Sigma+1$. By Lemma 2.5, K_y can be decomposed into t connected subgraphs $H_1, H_2, \ldots, H_t$ such that each H_i is a connected spanning (n_i-1)-regular graph. For $i = 1, 2, \ldots, t$, color all edges of H_i with color α_i. This gives a totally connected t-edge coloring of K_y such that the i-th color class contains no copy of K_{1,n_i} as a subgraph, which means that $R_c \geq \Sigma+2$.

(ii) Assume that Σ is even and at least one n_i is even. Without loss of generality, we may assume that n_t is even. Since Σ is even, we can consider the desired edge coloring of K_Σ with $\Sigma-1$ colors. We partition the above $\Sigma-1$ colors into t classes $V_1, V_2, \ldots, V_t$ such that V_t contains n_t-2 colors and for $i = 1, 2, \ldots, t-1$, each V_i contains n_i-1 colors from the available $\Sigma-1$ colors. Let H_i be the subgraph of K_Σ induced by the edges of color $\alpha \in V_i$. Since $n_t \geq 4$ and for $1 \leq i \leq t-1$, $n_i \geq 3$, each H_i is a connected spanning subgraph of K_Σ. Coloring all edges of H_i by color α_i, yields a totally connected t-edge coloring of K_Σ such that the i-th color class contains no copy of K_{1,n_i}. This edge coloring of K_Σ shows that $R_c \geq \Sigma + 1$.

Now it remains to prove the upper bound for R_c in each case. Let $c : E(K_p) \longrightarrow \{1, 2, \ldots, t\}$ be an arbitrary edge coloring of K_p with t colors such that the induced subgraph on each color class is a connected spanning subgraph. Suppose m_i is the number of edges in color i in c. To avoid the existence a copy of K_{1,n_i} in color i, we must have $m_i \leq ex(K_{1,n_i}, p) = \frac{p(n_i-1)}{2}$, for each i. Now summing these inequalities, we obtain $\binom{p}{2} \leq \frac{p\Sigma}{2}$ and hence $p \leq \Sigma + 1$. So if $p \geq \Sigma + 2$, then any totally connected edge coloring of K_p with t colors, contains a copy of K_{1,n_i} in color i, for some i i.e $R_c \leq \Sigma + 2$. Note that equally holds if and only if there exists a t-edge coloring of $K_{\Sigma+1}$ such that the induced subgraph on each color class is (n_i-1)-regular connected spanning subgraph of $K_{\Sigma+1}$. By Lemma 2.5, such a coloring exists if and only if Σ is odd or Σ is even and all n_i's are odd. Hence in both cases, we obtain the desired upper bound, which completes the proof of theorem. ■

The exact value of the generalized Ramsey number for stars calculated in [1] as follows.

Theorem 2.7. ([1]) Let $n_1, n_2, \ldots, n_t$ be positive integers and Σ denote $\Sigma_{i=1}^{t}(n_i-1)$.

(i) If Σ is odd, then $R(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t}) = \Sigma + 2$.

(ii) If Σ is even and all n_i are odd, then $R(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t}) = \Sigma + 2$.

(iii) If Σ is even and at least one n_i is even, then $R(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t}) = \Sigma + 1$.

Combining Theorem 2.6 and Theorem 2.7, we obtain the following corollary, which determine when the connected Ramsey and ordinary Ramsey number of stars are equal.

Corollary 2.8. Suppose that $n_1 \geq n_2 \geq \ldots \geq n_t$ are positive integers.

(i) If $n_t \geq 3$, then $R_c(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t}) = R(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t})$.

(ii) If $n_t \leq 2$, then $R_c(K_{1,n_1}, K_{1,n_2}, \ldots, K_{1,n_t}) = 2t$.

References

[1] S. A. Burr, J. A. Roberts, On Ramsey Numbers for Stars, *Util. Math.* 4 (1973), 217-220.

[2] R. Diestel, Graph Theory (3rd edition), Springer, Berlin 2005.

[3] G. A. Dirac, Some theorems on abstract graphs, *Proc. Landon Math. Soc.* 3(2) (1952), 69-81.

[4] R. J. Faudree, R. H. Schelp, Path Ramsey numbers in multicolorings, *J. Combin. Theory, Ser. B* 19 (1975), 150-160.

[5] A. Gyárfás, M. Ruszinkó, G. Sárközy, E. Szemerédi, Three-color Ramsey numbers for paths, *Combinatorica* 27 (1) (2007), 35-69;

[6] Z. Kemin, Z. shusheng, The Ramsey numbers for stars and stripes, *Acta Math. Sci.* 25 A(7) (2005), 1067-1072.

[7] S. P. Radziszowski, Small Ramsey numbers, *Electronic J. Combin.* 1 (1994), Dynamic Surveys, DS1.12 (August 4, 2009).

[8] D. P. Sumner, The connected Ramsey number, *Discrete Math.* 22 (1978), 49-55.

[9] R. J. Fauree, R. H. Schelp, Some connected Ramsey numbers, *J. Graph Theory* 2 (1978), 119-128.

Email: g.raeisi@sku.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Monochromatic matchings in graphs with large minimum degree

Ghaffar Raeisi[1]
Department of Mathematical Sciences, Shahrekord University, Shahrekord, Iran

Gholam Reza Omidi
Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, Iran

Abstract

Let $n_1, n_2, \dots n_c$ be positive integers and $n_1 = \max\{n_1, n_2, \dots n_c\}$. In this note, we prove that if G is a graph on at least $n_1 + \sum_{i=1}^{c}(n_i - 1) + 1$ vertices such that $\delta(G) \geq \sum_{i=1}^{c}(n_i - 1) + 1$, then, in every c-coloring of the edges of G there exists a monochromatic copy of $n_i K_2$, for some i, $1 \leq i \leq c$. In addition, it is proved that the bound presented for $\delta(G)$ is best possible.

Keywords: Matching, Star, Minimum degree, Ramsey number.
Mathematics Subject Classification [2010]: 05C15, 05C55

1 Introduction

In this paper, we only concerned with undirected simple finite graphs and we follow [1] for terminology and notations not defined here. For a graph G, we denote its vertex set, edge set, minimum degree and chromatic number by $V(G)$, $E(G)$, $\delta(G)$ and $\chi(G)$, respectively. If $v \in V(G)$, we use $\deg_G(v)$ (or simply $\deg(v)$) and $N(v)$ to denote the degree and neighbors of v in G, respectively. The complement graph of a graph G is denoted by $\overline{G}$ and as usual, a complete graph, cycle, path and a star on n vertices are denoted by K_n, C_n, P_n and S_{n-1}, respectively. Also, we use nK_2 to denote a matching (stripe) of size n, i.e., n pairwise disjoint edges.

An edge colored graph is a graph that has a colore assigned to each edge. An alternating cycle in a edge colored graph is a cycle such that no two consecutive edges have the same color. We say that vertex v separates colors if no component of $G - v$ is joined to v by at least two edges of different colors. Grossman and Häggkvist gave a sufficient condition under which a two-edge colored graph must have an alternating cycle. In [6] Grossman and Häggkvist proved that if G is a graph whose edges are colored either red or blue and there is no alternating cycle in G, then the following holds. Either there is a vertex which is incident only with edges of the same color or there is a separating vertex z such that no connected component of $G - z$ is joined to z with both red and blue edges.

J. Bang-Jensen and G. Gutin asked whether Grossman and Häggkvist's result could be extended to edge-colored graphs in general, where there is no constraint on the number of colors. In [10] Yeo gave an affirmative answer to this question as follows.

Theorem 1.1. *([10]) If G be a c-edge-colored graph, $c \geq 2$, with no alternating cycle, then there is a vertex $v \in V(G)$ such that no connected component of $G - v$ is joined to v with edges of more than one color, i.e G contains a vertex separating colors.*

[1] speaker

For given graphs $G_1, G_2, \ldots, G_c$, the *Ramsey number* $R(G_1, G_2, \ldots, G_c)$ is the smallest integer n such that if the edges of a complete graph K_n are partitioned into c disjoint color classes giving c graphs $H_1, H_2, \ldots, H_c$, then at least one H_i has a subgraph isomorphic to G_i. The existence of such a positive integer is guaranteed by Ramsey's classical result [9]. Since the 1970's, Ramsey theory has grown into one of the most active areas of research within combinatorics, overlapping variously with graph theory, number theory, geometry and logic. For a survey, we reffer the reader to the regularly updated survey by Radziszowski [8]. There is very little known about $R(G_1, G_2, \ldots, G_c)$ for $c \geq 3$ even for very special graphs. In this paper we consider the case when G_i's are either arbitrary stars or stripes. The Ramsey number for any number of matchings was determined in [3] as $R(n_1K_2, \ldots, n_cK_c) = n_1 + \sum_{i=1}^{c}(n_i - 1) + 1$ for $n_1 \geq n_2 \cdots \geq n_c$, in particular, $R(n_1K_2, n_2K_2) = 2n_1 + n_2 - 1$ for $n_1 \geq n_2$. Gyarfas and Sarkozy [7] extends this result as the Ramsey number for two matchings does not change if a graph of maximum degree $n_1 - 1$ is deleted from $K_{2n_1+n_2-1}$. More precisely, Gyarfas and Sarkozy proved the following theorem.

Theorem 1.2. ([7]) For given positive integers $n_1 \geq n_2 \geq 1$ and $t \geq 1$,

$$R(S_t, n_1K_2, n_2K_2) = \max\{t, n_1\} + n_1 + n_2 - 1.$$

The aim of this note is to give a bound on the minimum degree of a graph G such that in every c-coloring of the edges of G there exists a monochromatic copy of n_iK_2, for some i, $1 \leq i \leq c$. The proof of this theorem is based on the Ramsey number of a star and many matchings which is given in section 2.

Theorem 1.3. *Let $n_1, n_2, \ldots n_c$ be positive integers, $n_1 = \max\{n_1, n_2, \ldots n_c\}$, and let G be a graph on at least $R(n_1K_2, n_2K_2, \ldots, n_cK_2)$ vertices such that $\delta(G) \geq \sum_{i=1}^{c}(n_i - 1) + 1$. Then, in every c-coloring of the edges of G there exists a monochromatic copy of n_iK_2, for some i, $1 \leq i \leq c$.*

2 Proof of the Main Result

In this section, we give a proof for the main Theorem of the paper. For this purpose, we start with the following theorem.

Theorem 2.1. *If $n_1, n_2, \ldots n_c$ are positive integers and $n_1 = \max\{n_1, n_2, \ldots n_c\}$ then*

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) = \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1.$$

Proof. To see that the Ramsey number can not be less than claimed in the Theorem, consider a partition of $n = \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1$ vertices into sets $V, V_1, V_2, \ldots, V_c$ of size $\max\{t, n_1\}, n_1 - 1, n_2 - 1, \ldots, n_c - 1$ respectively. Color with the color α_0 all edges which are incident with two vertices of V and for each $i = 1, 2, \ldots, c$ color with α_i the edges having two vertices in V_i or one vertex in V_i and one in V_j where $j < i$. This yields a $c + 1$-coloring of K_n that does not have a monochromatic star S_t with color α_0 and no matching of size n_i in color α_i, $i = 1, 2, \ldots, c$. Therefore

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) \geq \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1.$$

To prove the other direction, Suppose that counterexamples exist; that is, there are positive integers $t, n_1, n_2, \ldots, n_c$, with $n_1 = \max\{n_1, n_2, \ldots n_c\}$ and a complete graph on at least $n = \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1$ vertices which colored by colors $\alpha_0, \alpha_1, \ldots, \alpha_c$ so that the subgraph induced by the edges of color α_0 does not contains S_t and also the subgraph induced by the edges of color α_i, $1 \leq i \leq c$, does not contains matching of size n_i.

Among the counterexamples let G be a minimal one in the following sense:

(1) G is colored with $c+1$ colors and no counterexample is colored with less than c colors.

(2) Among the counterexamples satisfying (1), G is one having a minimal number of vertices.

It is easily seen that these conditions imply that G has exactly

$$\max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1$$

vertices. In fact for any subgraph of G having this number of vertices is also a counterexample and so, because of the minimal properties of G, it coincides with G.

Now the analysis depends on the study of certain circuits in G. These are the ones colored with some colors α, $\alpha \in \{, \alpha_1, \ldots, \alpha_c\}$, having no two adjacent edges of the same color. If C is one of these subgraphs which has l_i edges colored by α_i, for each $i = 1, \ldots c$, then it has $\sum_{i=1}^{l} l_i$ vertices. For each i, the l_i edges colored by α_i form a subgraph of C isomorphic to l_iK_2. If C' is the complementary graph to C in G, then the number of vertices in C' is

$$\max\{t, n_1\} + \sum_{i=1}^{c}(n_i - l_i - 1) + 1.$$

Suppose that the numbers $n_i - l_i$, $i = l, \ldots, c$, are $m_1, m_2, \ldots, m_c$ in decreasing order. As $m_1 = \max\{m_1, \ldots, m_c\}$ and C is a proper subgraph of G we deduce from the minimality of G that C' has a subgraph isomorphic to S_t with color α_0 or has a subgraph isomorphic to $(n_i - l_i)K_2$ colored by α_i, for one $i = 1, \ldots, c$. In the second case, combining this with the subgraph of C isomorphic to l_iK_2 and colored by the same color, we obtain in G a subgraph isomorphic to n_iK_2 and colored by α_i, which is impossible. Now, the rest of the proof is devoted to prove a proper circuit exists.

Claim 1. $n_1 \leq \sum_{i=2}^{c}(n_i - 1) + 1$.

On the contrary, let $n_1 \geq \sum_{i=2}^{c}(n_i - 1) + 2$. It is easy to see that

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) \leq R(S_t, n_1K_2, \Big(\sum_{i=2}^{c}(n_i - 1) + 1\Big)K_2).$$

But By Theorem 1.2, we have

$$R(S_t, n_1K_2, (\sum_{i=2}^{c}(n_i - 1) + 1)K_2) = \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1$$

which implies that

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) \leq \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1$$

a contradiction. Thus $n_1 \leq \sum_{i=2}^{c}(n_i - 1) + 1$.

Claim 2. If $t \geq n_1$, then $t \leq \sum_{i=1}^{c}(n_i - 1) + 1$.

On the contrary, let $t \geq \sum_{i=2}^{c}(n_i - 1) + 2$. It is easy to see that

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) \leq R(S_t, \Big(\sum_{i=1}^{c}(n_i - 1) + 1\Big)K_2).$$

But By Theorem 1.2, we have

$$R(S_t, (\sum_{i=1}^{c}(n_i - 1) + 1)K_2) = t + \sum_{i=1}^{c}(n_i - 1) + 1$$

which implies that

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) \leq t + \sum_{i=1}^{c}(n_i - 1) + 1$$

a contradiction. Thus $t \leq \sum_{i=1}^{c}(n_i - 1) + 1$.

Claim 3. The induced subgraph H on the edges of color $\alpha_1, \ldots, \alpha_c$ is hamiltonian.

Since G has no S_t in color α_0, so $\delta(H) \geq \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) - t + 1$. Using Claim 2, one can easily check that $\delta(H) \geq \frac{|V(H)|}{2}$. Therefore, by the Dirak's Theorem H is a hamiltonian graph.

Claim 4. The induced subgraph H on the edges of color $\alpha_1, \ldots, \alpha_c$ has no cut vertex separating colors.

On the contrary, let H has a cut vertex v separating colors. This means that all edges of H incident to v have the same color, say α_i. Set $G' = G \setminus \{v\}$. We deduce from the minimality of G that G' has a subgraph H_{α_i} isomorphic to $(n_i - 1)K_2$ with color α_i. Note that $\deg_H(v) \geq \sum_{i=1}^{c}(n_i - 1) + 1$, and so by Claim 1, we obtain that $\deg_H(v) \geq 2n_1 - 1 \geq 2n_i - 1$. This means that there is a vertex $u \in N_H(v)$ which is unsaturated by the matching $(n_i - 1)K_2$ in H_{α_i}. Thus adding edge uv to the existence matching $(n_i - 1)K_2$ form a copy of n_iK_2 in color α_i, a contradiction.

Using Claim 4, Theorem [10] implies that G has an alternating cycle which is impossible. This contradiction shows that

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) = \max\{t, n_1\} + \sum_{i=1}^{c}(n_i - 1) + 1,$$

which completes the proof.

■

Proof of Theorem 1.3. Set $t = n - \sum_{i=1}^{c}(n_i - 1) - 1$. Clearly $t \geq n_1$ and so by Theorem 2.1, we have

$$R(S_t, n_1K_2, n_2K_2, \ldots, n_cK_2) = n.$$

Since G has n vertices and $\delta(G) \geq \sum_{i=1}^{c}(n_i - 1) + 1$, we have $\Delta(\bar{G}) \leq t - 1$, which means that $\bar{G}$ is a S_t-free graph and so the assertion holds by the above equation. ■

References

[1] J. A. Bondy, U. S. R. Murty, Graph Theory With Applications, American Elsevier Publishing Co. INC, 1976.

[2] S. A. Burr, J. A. Roberts, On Ramsey Numbers for Stars, *Util. Math.* 4 (1973), 217-220.

[3] E. J. Cockayne, P. J. Lorimer, The Ramsey number for stripes. *J. Austral. Math. Soc.* 19 (1975), 252-256

[4] E. J. Cockayne, P. J. Lorimer, On Ramsey graph numbers for stars and stripes, *Canadian Math. Bull.* 18 (1975), 31-34.

[5] G. A. Dirac, Some theorems on abstract graphs, *Proc. London Math. Soc.* 2 (1952), 69-81.

[6] J. W. Grossman and R. Haäggkvist, Alternating cycles in edge-partitioned graphs, *J. Combin. Theory Ser. B* 34(1983), 77-81

[7] S A. Gyarfas, G. Sarkozy, Star Versus Two Stripes Ramsey Numbers and a Conjecture of Schelp, *Combinatorics, Probability and Computing* 21 (2012), 179–186.

[8] S. P. Radziszowski, Small Ramsey numbers, *Electronic J. Combin.* 1 (1994), Dynamic Surveys, DS1.12 (August 4, 2009).

[9] F. P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc. 2nd Ser.* 30 (1930), 264-286.

[10] A. Yeo, Alternating cycles in edge-coloured graphs, *J. Combin. Th. Ser. B* 69 (1997), 222-225.

Email: g.raeisi@sku.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Novel Fuzzy Topological Descriptors for Characterizing Aromatic Hydrocarbons

Mehri Hasani[1]
Semnan University, Semnan, Iran

Masoud Ghods
Semnan University, Semnan, Iran

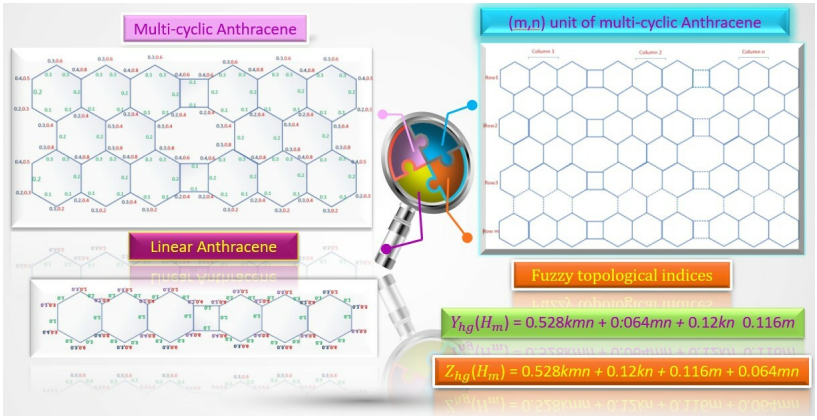
Abstract

Fuzzy graphs have gained significant attention in diverse scientific fields, including mathematics and chemistry, owing to their superior accuracy and adaptability compared to conventional models. This study delves into a theoretical exploration of the fuzzy graph representation of aromatic hydrocarbons, focusing on the computation of several fuzzy-based degree topological indices. Novel definitions are introduced for the first Zagreb fuzzy index, Forgotten index, and Y-index, alongside a generalized formula for fuzzy topological indices of linear and cyclic aromatic hydrocarbons, incorporating edge degrees. Moreover, a comprehensive formula is derived to calculate specific topological indices of hydrocarbons based on the number of benzene rings. This methodology empowers researchers to predict and estimate compounds' physical and chemical properties by leveraging topological indices and precise calculations of bond lengths and atomic masses facilitated by computational software.

Keywords: Fuzzy graph, Topological indices, Zagreb index, Randic index, Aromatic hydrocarbons

AMS Mathematical Subject Classification [2010]: 05C72, 05C09, 05C31

Graphical Abstract



[1]speaker

1 Introduction

Graph theory, a branch of mathematics, has found significant applications in various scientific disciplines, including physics, chemistry, and engineering [5, 13, 43]. A particular application, chemical graph theory, merges the principles of chemistry and graph theory to represent chemical structures as mathematical models. By employing mathematical theorems and chemical methodologies, this discipline enables the resolution of complex chemical problems. In molecular graphs, atoms and bonds are abstractly represented as vertices and edges, respectively. Graph theory's utility in chemistry extends to tasks such as isomer enumeration and molecular structure generation. Pioneering figures in the field of chemical graph theory include Alexander Balaban, Ante Graovac, Ivan Gutman, Haruo Hosoya, Milan Randi, and Nenad Trinajsti [10, 33, 39].
In many real-world systems, it is often challenging to precisely define the relationships between entities. To address this limitation, fuzzy graph theory offers a flexible framework for representing uncertainty and imprecision in graph structures. By allowing vertices and edges to have degrees of membership, fuzzy graphs enable a more nuanced and realistic modeling of complex systems. Fuzzy graph theory has found wide-ranging applications across diverse fields, including neural networks, artificial intelligence, computer networks, engineering sciences, transportation network design, and electrical circuits. In particular, fuzzy graph theory has been instrumental in analyzing the structure of communication networks and circuits where design ambiguity exists [26]. The concept of membership in a set is based on the binary evaluation of connection or non-connection. However, in fuzzy sets, elements have membership degrees in the interval $[0, 1]$. Membership values of vertices and edges are not certain in fuzzy graph theory, which differs from a crisp approach.

Topological indices are numerical representations of molecular structures that can predict chemical properties without the need for experimentation. Topological indices, numerical representations of molecular structures, have found widespread applications in theoretical chemistry for predicting physical and chemical properties. Furthermore, they leveraged topological indices and MATLAB programming to predict the physicochemical properties of drugs designed to combat Parkinson's disease [17]. Extending their research in 2024, they analyzed the quantitative structure-property relationship (QSPR) of certain drugs used to treat heart calcium channel-blocking cardiac drugs and beta-blockers diseases [15, 16]. Additionally, they employed entropy graphs weighted by topological indices and MATLAB programming to investigate the QSPR of pyelonephritis drugs [18].

Topological indices, numerical descriptors derived from the graph-theoretical representation of molecules, have been instrumental in quantitative structure-activity relationship (QSAR) studies. This brief overview traces the evolution of key topological indices, from their inception for crisp graphs to their extension to fuzzy graphs. Wiener, in 1947, introduced the Wiener index to characterize alkanes [44]. The concept of fuzzy sets, introduced by Zadeh in 1965, paved the way for the development of fuzzy graph theory [46]. J. Xu's seminal work in 1997 marked a significant milestone by highlighting the initial application of fuzzy graph theory to the field of chemistry [45]. In the realm of crisp graphs, the Zagreb indices and the Forgotten index emerged in the early 1970s [12, 8, 40]. The extension of topological indices to fuzzy graphs began in the 21st century. Researchers have investigated various indices, including the Wiener index, F-index, and connectivity indices, for fuzzy graphs [2, 26]. Additionally, studies have explored these indices for bipolar fuzzy graphs and their applications in various fields, such as chemistry and materials science [35, 37, 21, 22, 23, 24].

In 2022, Shi et al. investigated the dominant energies within the visual phase diagram and their practical uses [41].Simultaneously, Morderson and Peng provided an overview of the potential applications of fuzzy graph theory, highlighting its utility in various domains, including chemistry [27].
Carbon nanotubes, discovered by S. Iijima in 1991 [34], are cylindrical carbon nanostructures with exceptional mechanical properties [20, 42]. Their unique structures, resembling planar hexagonal networks, have implications in the chemistry of benzenoid hydrocarbons [11]. Additionally, acenes, a class of polycyclic aromatic hydrocarbons, have potential applications in optoelectronics. Recent research has explored these indices for various compounds, including nanotubes, fuzzy graphs, and linear and multi-acyclic hydrocarbons. In 2024, Faraz et al. determined the entropy of silicon nanotubes using degree-based topological descriptors [7].
Inspired by previous studies [19, 26, 31], this research aims to investigate several topological indices for a series of aromatic hydrocarbons, including Naphthalene, Anthracene, Tetrasene, Pentacene, Hexacene, Heptacene, Octacene, Nanocene, Decacene, and Undecacene. The primary objectives are to derive new formulas for the first fuzzy Zagreb index, Forgotten index, and Y-index, considering edge degrees, and to develop a general formula for fuzzy topological indices of aromatic hydrocarbons. Our method can help researchers predict and estimate the physical and chemical properties of chemical compounds using software and precise calculations of bond lengths and atomic mass with the help of topology indices.

2 Framework of the article

This paper is structured as follows: Section 1 provides a comprehensive literature review, outlining our research motivation and objectives. Section 3 presents essential definitions and concepts related to fuzzy graphs and topological indices, as well as introduces new definitions for the first Zagreb fuzzy index, Forgotten index, and Y-index. In Section 4, we delve into a theoretical investigation of fuzzy topological indices for linear aromatic hydrocarbons, deriving a general formula for their extension. Section 5 focuses on cyclic aromatic hydrocarbons, presenting their fuzzy topological indices and a general formula for extension. Finally, Section 6 concludes the paper by discussing the implications and potential applications of the studied indices.

3 Preliminaries

In this section, some basic definitions necessary for the development of our results are presented [19, 32].

Definition 3.1. Suppose X is a finite set. The graph fuzzy G with vertices set $V(G)$ and edges set $E(G) = \{uv \mid \mu(uv) > 0, \forall u, v \in V(G)\}$, is a triplet, $G = (V, \sigma, \mu)$, where V is a nonempty finite subset of X with a pair of functions σ and μ such that

$$\sigma : V \longrightarrow [0, 1]$$

$$\mu : V \times V \longrightarrow [0, 1] \quad \forall u, v \in V(G)$$

satisfying

$$\mu(u,v) \leq \sigma(u) \wedge \sigma(v),$$

where $\wedge$ represents the minimum.

Definition 3.2. Suppose $u \in V$, and $N(u)$ denotes the set of neighbors of u, then the degree of u in a fuzzy graph is defined by

$$d_G(u) = \sum_{v \in N(u)} \mu(uv)$$

Also, Order of G in a fuzzy graph is defined by

$$Order(G) = \sum_{u_i \in V(G)} \sigma(u_i)$$

and Size of G in a fuzzy graph is denoted by

$$Size(G) = \sum_{uv \in E(G)} \mu(uv)$$

where $\mu(uv) = \mu(u,v)$.

Definition 3.3. [12] Suppose G is a crisp graph. Then the first Zagreb index is shown by $M_1(G)$ and defined as follows:

$$M_1(G) = \sum_{i=1}^{n} [d(u_i)]^2 = \sum_{u_i u_j \in E(G)} [d(u_i) + d(u_j)]$$

Definition 3.4. [12] Suppose G is a crisp graph. Then the second Zagreb index is shown by $M_2(G)$ and defined as follows:

$$M_2(G) = \sum_{u_i u_j \in E(G)} d(u_i) d(u_j)$$

Definition 3.5. [6] Suppose G is a crisp graph. Then the Forgotten index (F-index) is denoted by $F(G)$ and defined as follows:

$$F(G) = \sum_{i=1}^{n} [d(u_i)]^3 = \sum_{u_i u_j \in E(G)} \left[d(u_i)^2 + d(u_j)^2\right]$$

Definition 3.6. [1] Let G be a crisp graph. Then the Y-index is denoted by $Y(G)$ and defined as follows:

$$Y(G) = \sum_{i=1}^{n} [d(u_i)]^4 = \sum_{u_i u_j \in E(G)} \left[d(u_i)^3 + d(u_j)^3\right]$$

Definition 3.7. [26] Assume G is the fuzzy graph. Then the first Zagreb index for fuzzy graphs is denoted by $M(G)$ and is defined as follows:

$$M_1^*(G) = \sum_{i=1}^{n} \sigma(u_i)[d(u_i]^2$$

We define the first Zagreb index for fuzzy graphs as follows:

Definition 3.8. Assume G is the fuzzy graph. Then the first Zagreb index for fuzzy graphs is indicated by $Z_\mu(G)$ and is defined by:

$$Z_\mu(G) = \sum_{u_iu_j \in E(G)} \mu(u_iu_j)\left[\sigma(u_i)d(u_i) + \sigma(u_j)d(u_j)\right]$$

It is simply proved that Definitions 3.7 and 3.8 are equal.

Definition 3.9. [26] Assume G is the fuzzy graph. Then the second Zagreb index is shown by $M^*(G)$ and is defined by:

$$M_2^*(G) = \frac{1}{2}\sum_{u_iu_j \in E(G)} \sigma(u_i)d(u_i)\sigma(u_j)d(u_j) \qquad \forall i \neq j$$

.

We have provided another definition of the F-index in fuzzy graphs as follows:

Definition 3.10. Assume G is the fuzzy graph. Then the F-index for fuzzy graphs is shown $F^*(G)$ and is introduced as follows:

$$F^*(G) = \sum_{i=1}^{n} \sigma(u_i)\left[d(u_i)\right]^3$$

Definition 3.11. Assume G is the fuzzy graph. Then the F-index for fuzzy graphs is indicated by $F_\mu(G)$ and is defined by:

$$F_\mu(G) = \sum_{u_iu_j \in E(G)} \mu(u_iu_j)\left[\sigma(u_i)d(u_i)^2 + \sigma(u_j)d(u_j)^2\right]$$

It is easy to prove that definitions 3.10 and 3.11 are equivalent.

We have provided another definition of the Y-index in fuzzy graphs.

Definition 3.12. [25] Suppose G is a fuzzy graph. Then the Y-index is denoted by $Y*(G)$ and is introduced by:

$$Y^*(G) = \sum_{i=1}^{n} \sigma(u_i)[d(u_i]^4$$

Definition 3.13. Assume G is the fuzzy graph. Then the Y-index for fuzzy graphs is indicated by $Y_\mu(G)$ and is defined as follows:

$$Y_\mu(G) = \sum_{u_iu_j \in E(G)} \mu(u_iu_j)\left[\sigma(u_i)d(u_i)^3 + \sigma(u_j)d(u_j)^3\right]$$

It is simple to show that definitions 3.12 and 3.13 are equivalent.

Definition 3.14. [31] Suppose G is a fuzzy graph. The Randić index is shown by $\Re^*(G)$ and is defined as

$$\Re^*(G) = \frac{1}{2}\sum_{u_iu_j \in E(G)} \left[(\sigma(u_i)d(u_i)\sigma(u_j)d(u_j))\right]^{\frac{-1}{2}} \qquad \forall i \neq j$$

Definition 3.15. [31] Let G be a fuzzy graph. The Harmonic index is shown by $H^*(G)$ and is defined by:

$$H^*(G) = \frac{1}{2}\sum_{u_iu_j \in E(G)} \left[\sigma(u_i)d(u_i) + \sigma(u_j)d(u_j)\right]^{-1} \qquad \forall i \neq j$$

Table 1: The topological indices for fuzzy graphs

Index	Abbreviations
The first zagreb index	M_1^*, Z_μ
The second Zagreb index	M_2^*
The Forgotten index	F^*, F_μ
The Y- index	Y^*, Y_μ
The Harmonic index	H^*, H_μ
The Randic index	$\Re^*$

Abbreviations

4 Topological indices of fuzzy graphs of linear hydrocarbons

In this section, some topological indices of linear hydrocarbons in fuzzy graphs are examined, and a general formula based on the number of Benzene rings (K) is presented for its extension. In Table 2, aromatic hydrocarbons are introduced based on the number of Benzene rings. According to Figures 1, 2, and 3, and based on the structure of linear hydrocarbons, the total number of vertices is $4kn+2n$ and the total number of edges is $5kn + 3n - 2$, respectively. The set of all vertices and edges is divided into weight categories, as shown in Tables 3 and 4. Using Table 3, the vertex set with weight 0.2 has a total number of $kn + n$, the vertex set with weight 0.3 has a total number of $2kn$, and the vertex set with weight 0.4 has a total number of $kn + n$.

Table 2: Naming hydrocarbons based on the number of Benzene rings connected

K	Hydrocarbon	Molecular formula
1	Benzene	C_6H_6
2	Naphthalene	$C_{10}H_8$
3	Anthracene	$C_{14}H_{10}$
4	Tetracene	$C_{18}H_{12}$
5	Pantacene	$C_{22}H_{14}$
6	Hexacene	$C_{26}H_{16}$
7	Heptacene	$C_{30}H_{18}$
8	Octacene	$C_{34}H_{20}$
9	Nanocene	$C_{38}H_{22}$
10	Decacene	$C_{42}H_{24}$
11	Undecacene	$C_{46}H_{26}$

Note: K is the number of Benzene rings.

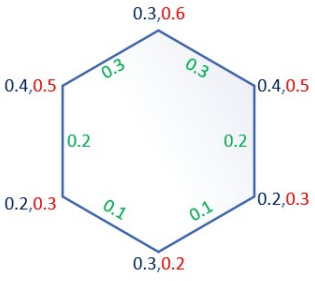


Figure 1: (1,1) unit of fuzzy graph of Benzene

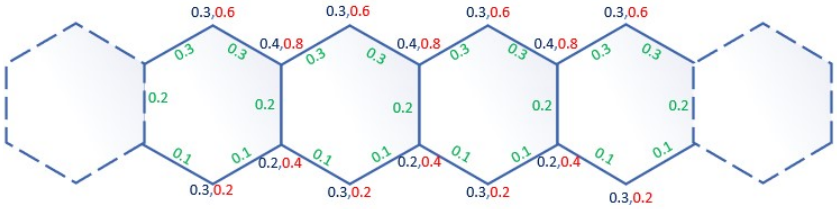


Figure 2: (1,1) unit of the fuzzy graph of linear Hydrocarbon

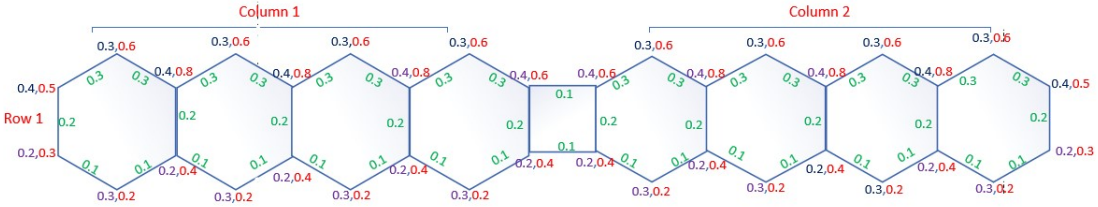


Figure 3: (1,2) unit of the fuzzy graph of linear Tetracene hydrocarbon (K=4)

Theorem 4.1. *Suppose H_l is a linear hydrocarbon fuzzy graph and K is the number of Benzene rings. Then the first Zagreb index of H_l is*
$Z_\mu(H_l) = 0.408kn + 0.064n - 0.116$

Proof. According to Figure 3, and using Table 4 and Definition 3.8, we have

$$Z_\mu(H_l) = \sum_{u_iu_j \in E(G))} \mu(u_iu_j)\left[\sigma(u_i)d(u_i) + \sigma(u_j)d(u_j)\right]$$

$$= 2(0.3)\left[(0.3)(0.6) + (0.4)(0.5)\right] + (2kn - 2n)(0.3)\left[(0.3)(0.6) + (0.4)(0.8)\right]$$

$$+(2n - 2)(0.3)\left[(0.3)(0.6) + (0.4)(0.6)\right] + 2(0.1)\left[(0.3)(0.2) + (0.2)(0.3)\right]$$

$$+(2kn - 2)(0.1)\left[(0.3)(0.2) + (0.2)(0.4)\right] + 2(0.2)\left[(0.2)(0.3) + (0.4)(0.5)\right]$$

$$+(kn - n)(0.2)\left[(0.2)(0.4) + (0.4)(0.8)\right] + (2n - 2)(0.2)\left[(0.2)(0.4) + (0.4)(0.6)\right]$$

$$+(n - 1)(0.1)\left[(0.4)(0.6) + (0.4)(0.6)\right] + (n - 1)(0.1)\left[(0.2)(0.4) + (0.2)(0.4)\right]$$

$$= 0.408kn + 0.064n - 0.116$$

□

Theorem 4.2. *Let H_l be a fuzzy graph of linear Hydrocarbon. Then the second fuzzy Zagreb index of H_l is* $M_2^*(H_l) = 0.0752kn + 0.024n - 0.0476$

Proof. Using Table 4 and Definition 3.9, we have

$$M_2^*(H_l) = \frac{1}{2} \sum_{u_iu_j \in E(G)} \sigma(u_i)d(u_i)\sigma(u_j)d(u_j)$$

Table 3: Partition of vertices for fuzzy graphs of linear hydrocarbons

Weight	**Degree**	**The total number of vertices**
(0.2)	(0.3)	2
	(0.4)	$kn+n-2$
(0.3)	(0.2)	kn
	(0.6)	kn
(0.4)	(0.5)	2
	(0.6)	$2n-2$
	(0.8)	$kn-n$

Table 4: Partitionof edges for fuzzy graphs of linear hydrocarbons

Weight	**Degree**	**The total number of edges**
(0.3,0.4)	(0.6,0.5)	2
	(0.6,0.8)	$2kn-2n$
	(0.6,0.6)	$2n-2$
(0.3,0.2)	(0.2,0.3)	2
	(0.2,0.4)	$2kn-2$
(0.2,0.4)	(0.3,0.5)	2
	(0.4,0.8)	$kn-n$
	(0.4,0.6)	$2n-2$
(0.4,0.4)	(0.6,0.6)	$n-1$
(0.2,0.2)	(0.4,0.4)	$n-1$

$$= \frac{1}{2}\left[2(0.3)(0.6)(0.4)(0.5) + (2kn-2n)(0.3)(0.6)(0.4)(0.8) + (2n-2)(0.3)(0.6)(0.4)(0.6)\right]$$

$$+\frac{1}{2}\left[2(0.3)(0.2)(0.2)(0.3) + (2kn-2)(0.3)(0.2)(0.2)(0.4)\right]$$

$$+\frac{1}{2}\left[2(0.2)(0.3)(0.4)(0.5) + (kn-n)(0.2)(0.4)(0.4)(0.8) + (2n-2)(0.2)(0.4)(0.4)(0.6)\right]$$

$$+\frac{1}{2}\left[(n-1)(0.4)(0.6)(0.4)(0.6) + (n-1)(0.2)(0.4)(0.2)(0.4)\right]$$

$$= 0.0752kn + 0.024n - 0.0476$$

□

Theorem 4.3. *Suppose H_l is a linear hydrocarbon fuzzy graph. Then the Forgotten index of H_l is* $F_\mu(H_l) = 0.2848kn - 0.0192n - 0.0876$

Proof. Using Table 4 and Definition 3.11, we have

$$F_\mu(H_l) = \sum_{u_iu_j \in E(G)} \mu(u_iu_j)\left[\sigma(u_i)d(u_i)^2 + \sigma(u_j)d(u_j)^2\right]$$

$$= 2(0.3)\left[(0.3)(0.6)^2 + (0.4)(0.5)^2\right] + (2kn-2n)(0.3)\left[(0.3)(0.6)^2 + (0.4)(0.8)^2\right]$$

$$+(2n-2)(0.3)\left[(0.3)(0.6)^2 + (0.4)(0.6)^2\right] + 2(0.1)\left[(0.3)(0.2)^2 + (0.2)(0.3)^2\right]$$

$$+(2kn-2)(0.1)\left[(0.3)(0.2)^2+(0.2)(0.4)^2\right]+2(0.2)\left[(0.2)(0.3)^2+(0.4)(0.5)^2\right]$$

$$+(kn-n)(0.2)\left[(0.2)(0.4)^2+(0.4)(0.8)^2\right]+(2n-2)(0.2)\left[(0.2)(0.4)^2+(0.4)(0.6)^2\right]$$

$$+(n-1)(0.1)\left[(0.4)(0.6)^2+(0.4)(0.6)^2\right]+(n-1)(0.1)\left[(0.2)(0.4)^2+(0.2)(0.4)^2\right]$$

$$=0.2848kn-0.0192n-0.0876$$

□

Theorem 4.4. *Let H_l be a linear hydrocarbon fuzzy graph. Then the Y-index of H_l is* $Y_\mu(H_l)=0.2082kn-0.055n-0.0606$

Proof. Using Table 4 and Definition 3.13, we have

$$Y_\mu(H_l)=\sum_{u_iu_j\in E(G)}\mu(u_iu_j)\left[\sigma(u_i)d(u_i)^3+\sigma(u_j)d(u_j)^2\right]$$
$$=2(0.3)\left[(0.3)(0.6)^3+(0.4)(0.5)^3\right]+(2kn-2n)(0.3)\left[(0.3)(0.6)^3+(0.4)(0.8)^3\right]$$
$$+(2n-2)(0.3)\left[(0.3)(0.6)^3+(0.4)(0.6)^3\right]+2(0.1)\left[(0.3)(0.2)^3+(0.2)(0.3)^3\right]$$
$$+(2kn-2)(0.1)\left[(0.3)(0.2)^3+(0.2)(0.4)^3\right]+2(0.2)\left[(0.2)(0.3)^3+(0.4)(0.5)^3\right]$$
$$+(kn-n)(0.2)\left[(0.2)(0.4)^3+(0.4)(0.8)^3\right]$$
$$+(2n-2)(0.2)\left[(0.2)(0.4)^3+(0.4)(0.6)^3\right]$$
$$+(n-1)(0.1)\left[(0.4)(0.6)^3+(0.4)(0.6)^3\right]+(n-1)(0.1)\left[(0.2)(0.4)^3+(0.2)(0.4)^3\right]$$
$$=0.2082kn-0.055n-0.0606$$

□

Theorem 4.5. *Suppose H_l is a linear hydrocarbon fuzzy graph. Then the Randić index of H_l is* $\Re^*(H_l)=21.7253kn+13.0697-3.7293$

Proof. Using Table 4 and Definition 3.14, we have

$$\Re^*(H_l)=\frac{1}{2}\sum_{u_iu_j\in E(G)}\left[(\sigma(u_i)d(u_i)\sigma(u_j)d(u_j)\right]^{\frac{-1}{2}}$$
$$=\frac{1}{2}(2)\left[(0.3)(0.6)(0.4)(0.5)\right]^{\frac{-1}{2}}+\frac{1}{2}(2kn-2n)\left[(0.3)(0.6)(0.4)(0.8)\right]^{\frac{-1}{2}}$$
$$+\frac{1}{2}(2n-2)\left[(0.3)(0.6)(0.4)(0.6)\right]^{\frac{-1}{2}}+\frac{1}{2}(2)\left[(0.3)(0.2)(0.2)(0.3)\right]^{\frac{-1}{2}}$$
$$+\frac{1}{2}(2kn-2)\left[(0.3)(0.2)(0.2)(0.4)\right]^{\frac{-1}{2}}+\frac{1}{2}(2)\left[(0.2)(0.3)(0.4)(0.5)\right]^{\frac{-1}{2}}$$
$$+\frac{1}{2}(kn-n)\left[(0.2)(0.4)(0.4)(0.8)\right]^{\frac{-1}{2}}+\frac{1}{2}(2n-2)\left[(0.2)(0.4)(0.4)(0.6)\right]^{\frac{-1}{2}}$$
$$+\frac{1}{2}(n-1)\left[(0.4)(0.6)(0.4)(0.6)\right]^{\frac{-1}{2}}+\frac{1}{2}(n-1)\left[(0.2)(0.4)(0.2)(0.4)\right]^{\frac{-1}{2}}$$

$$= 21.7253kn + 13.0697 - 3.7293$$

□

Theorem 4.6. *Let H_l be a linear hydrocarbon fuzzy graph. Then the Harmonic index of H_l is* $H^*(H_l) = 10.3928kn + 6.4225n - 4.6359$

Proof. Using Table 4 and Definition 3.15, we have

$$\begin{aligned}
H^*(H_l) &= \frac{1}{2}\sum_{u_iu_j\in E(G)} [\sigma(u_i)d(u_i) + \sigma(u_j)d(u_j)]^{-1} \\
&= \frac{1}{2}\left[\frac{2}{(0.3)(0.6)+(0.4)(0.5)}\right] + \frac{1}{2}\left[\frac{2kn-2n}{(0.3)(0.6)+(0.4)(0.8)}\right] \\
&+\frac{1}{2}\left[\frac{2n-2}{(0.3)(0.6)+(0.4)(0.6)}\right] + \frac{1}{2}\left[\frac{2}{(0.3)(0.2)+(0.2)(0.3)}\right] \\
&+\frac{1}{2}\left[\frac{2kn-2}{(0.3)(0.2)+(0.2)(0.4)}\right] + \frac{1}{2}\left[\frac{2}{(0.2)(0.3)+(0.4)(0.5)}\right] \\
&+\frac{1}{2}\left[\frac{kn-n}{(0.2)(0.4)+(0.4)(0.8)}\right] + \frac{1}{2}\left[\frac{2n-2}{(0.2)(0.4)+(0.4)(0.6)}\right] \\
&+\frac{1}{2}\left[\frac{n-1}{(0.4)(0.6)+(0.4)(0.6)}\right] + \frac{1}{2}\left[\frac{n-1}{(0.2)(0.4)+(0.2)(0.4)}\right] \\
&= 10.3928kn + 6.4225n - 4.6359
\end{aligned}$$

□

5 Topological indices of fuzzy graphs of multi-hydrocarbon

In this section, some topological indices of multi-hydrocarbons in fuzzy graphs are computed, and a general formula based on the number of Benzene rings (K) is presented for it's extension. According to Figures 4 and 5, and based on the structure of multi-hydrocarbons, the total number of vertices is $4kmn + 2mn$ and the total number of edges is $6kmn+3mn-2m-kn$, respectively. The set of all vertices and edges is divided into weight categories, as shown in Tables 5 and 6. Using Table 5, the vertex set with weight 0.2 has a total number of $(k + 1)mn$, the vertex set with weight 0.3 has a total number of $2kmn$, and the vertex set with weight 0.4 has a total number of $(k + 1)mn$.

Table 5: Partition of vertices in fuzzy graphs of multi-hydrocarbons

Weight	**Degree**	**The total number of vertices**
(0.2)	(0.3)	$2m$
	(0.4)	$m(kn + n - 2)$
(0.3)	(0.2)	kn
	(0.4)	$kn(m - 1)$
	(0.6)	kn
	(0.8)	$kn(m - 1)$
(0.4)	(0.5)	$2m$
	(0.6)	$2m(n - 1)$
	(0.8)	$(k - 1)mn$

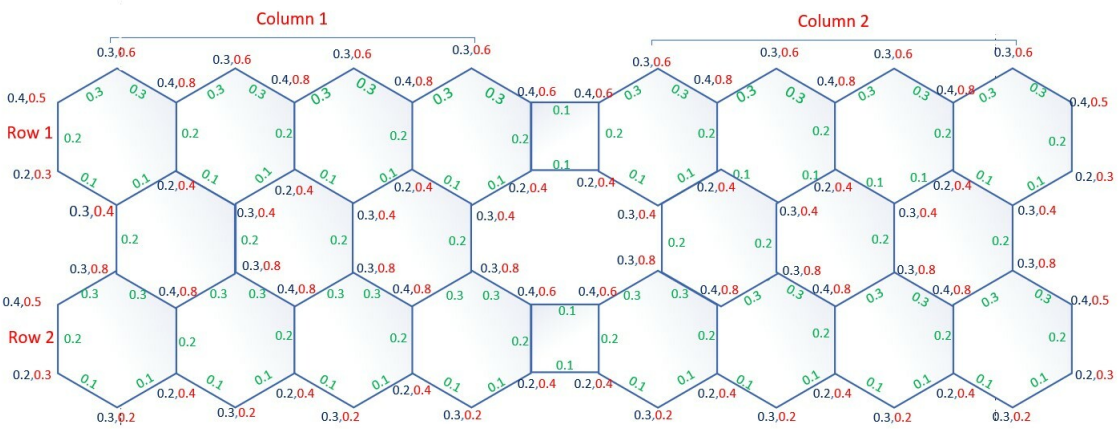


Figure 4: (2,2) unit of the fuzzy graph of Tetracene Hydrocarbon (K=4)

Table 6: Partition of edges in fuzzy graphs of multi-hydrocarbons

Weight	**Degree**	**The total number of edges**
(0.3,0.4)	(0.6,0.5)	2
	(0.6,0.8)	$2kn-2n$
	(0.6,0.6)	$2n-2$
	(0.8,0.5)	$2m-2$
	(0.8,0.8)	$(2kn-2n)(m-1)$
	(0.8,0.6)	$(m-1)(2n-2)$
(04,0.2)	(0.5,0.3)	$2m$
	(0.8,0.4)	$(k-1)mn$
	(0.6,0.4)	$2m(n-1)$
(0.2,0.3)	(0.3,0.4)	$2m-2$
	(0.4,0.4)	$(m-1)(2kn-2)$
	(0.3,0.2)	2
	(0.4,0.2)	$2kn-2$
(0.4,0.4)	(0.6,0.6)	$m(n-1)$
(0.2,0.2)	(0.4,0.4)	$m(n-1)$
(0.3,0.3)	(0.4,0.8)	$kn(m-1)$

Theorem 5.1. *Suppose H_m is a multi-hydrocarbon fuzzy graph and K is the number of Benzene rings. Then the first Zagreb index of H_m is*

$$Z_\mu(H_m) = 0.528kmn - 0.12kn - 0.116m + 0.064mn$$

Proof. Using Table 6 and Definition 3.8, we have

$$Z_\mu(H_m) = \sum_{u_iu_j \in E(G))} \mu(u_iu_j)\left[\sigma(u_i)d(u_i) + \sigma(u_j)d(u_j)\right]$$

$$= 2(0.3)\left[(0.3)(0.6) + (0.4)(0.5)\right] + (2kn-2n)(0.3)\left[(0.3)(0.6) + (0.4)(0.8)\right]$$

$$+(2n-2)(0.3)\left[(0.3)(0.6) + (0.4)(0.6)\right] + (2m-2)(0.3)\left[(0.3)(0.8) + (0.4)(0.5)\right]$$

$$+(2kn-2n)(m-1)(0.3)\left[(0.3)(0.8) + (0.4)(0.8)\right] + (m-1)(2n-2)(0.3)\left[(0.3)(0.8) + (0.4)(0.6)\right]$$

$+(2m)(0.2)\left[(0.4)(0.5)+(0.2)(0.3)\right]+(k-1)mn(0.2)\left[(0.4)(0.8)+(0.2)(0.4)\right]$

$+(0.2)(2m)(n-1)\left[(0.4)(0.6)+(0.2)(0.4)\right]+(2m-2)(0.1)\left[(0.2)(0.3)+(0.3)(0.4)\right]$

$+(0.1)(m-1)(2kn-2)\left[(0.2)(0.4)+(0.3)(0.4)\right]+2(0.1)\left[(0.2)(0.3)+(0.3)(0.2)\right]$

$+(0.1)(2kn-2)\left[(0.2)(0.4)+(0.3)(0.2)\right]+(0.1)m(n-1)\left[(0.4)(0.6)+(0.4)(0.6)\right]$

$+(0.1)m(n-1)\left[(0.2)(0.4)+(0.2)(0.4)\right]+(0.2)kn(m-1)\left[(0.3)(0.4)+(0.3)(0.8)\right]$

$=0.528kmn-0.12kn-0.116m+0.064mn$

□

Theorem 5.2. *Let H_m be a fuzzy graph of multi-hydrocarbon. Then the second fuzzy Zagreb index of multi-hydrocarbons is*

$$M_2^*(H_m)=0.1136kmn+0.0192mn-0.0384kn-0.0944m+0.0048n+0.468$$

Proof. Using Table 6 and Definition 3.9, we have

$$M_2^*(H_m)=\frac{1}{2}\sum_{u_iu_j\in E(G)}\sigma(u_i)d(u_i)\sigma(u_j)d(u_j)$$

$=\frac{1}{2}[2(0.3)(0.6)(0.4)(0.5)+(2kn-2n)(0.3)(0.6)(0.4)(0.8)$

$+(2n-2)(0.3)(0.6)(0.4)(0.6)+(2m-2)(0.3)(0.8)(0.4)(0.5)$

$+(2kn-2n)(m-1)(0.3)(0.8)(0.4)(0.8)+(m-1)(2n-2)(0.3)(0.8)(0.4)(0.6)$

$+(2m)(0.4)(0.5)(0.2)(0.3)+(k-1)mn(0.4)(0.8)(0.2)(0.4)$

$+2m(n-1)(0.4)(0.6)(0.2)(0.4)+(2m-2)(0.2)(0.3)(0.3)(0.4)$

$+(m-1)(2kn-2)(0.2)(0.4)(0.3)(0.4)+2(0.2)(0.3)(0.3)(0.2)$

$+(2kn-2)(0.2)(0.4)(0.3)(0.2)+m(n-1)(0.4)(0.6)(0.4)(0.6)$

$+m(n-1)(0.2)(0.4)(0.2)(0.4)+kn(m-1)(0.3)(0.4)(0.3)(0.8)]$

$=0.1136kmn+0.0192mn-0.0384kn-0.0944m+0.0048n+0.468$

□

Theorem 5.3. *Suppose H_m is a fuzzy graph of multi-hydrocarbon. Then the Randić index of multi-hydrocarbons is*

$$\Re * (H_m) = 19.8858kmn - 8.1605kn + 12.9783mn - 4.5704m + 0.0914n + 10.8411$$

Proof. Using Table 6 and Definition 3.14, we have

$$\begin{aligned}
\Re^*(G) &= \frac{1}{2}\sum_{u_iu_j\in E(G)} [(\sigma(u_i)d(u_i)\sigma(u_j)d(u_j)]^{\frac{-1}{2}} \\
&= \frac{1}{2}(2)\,[(0.3)(0.6)(0.4)(0.5)]^{\frac{-1}{2}} + \frac{1}{2}(2kn-2n)\,[(0.3)(0.6)(0.4)(0.8)]^{\frac{-1}{2}} \\
&+\frac{1}{2}(2n-2)\,[(0.3)(0.6)(0.4)(0.6)]^{\frac{-1}{2}} + \frac{1}{2}(2m-2)\,[(0.3)(0.8)(0.4)(0.5)]^{\frac{-1}{2}} \\
&+\frac{1}{2}(2kn-2)(m-1)\,[(0.3)(0.8)(0.4)(0.8)]^{\frac{-1}{2}} \\
&+\frac{1}{2}(m-1)(2n-2)\,[(0.3)(0.8)(0.4)(0.6)]^{\frac{-1}{2}} \\
&+\frac{1}{2}(2m)\,[(0.4)(0.5)(0.2)(0.3)]^{\frac{-1}{2}} + \frac{1}{2}(k-1)mn\,[(0.4)(0.8)(0.2)(0.4)]^{\frac{-1}{2}} \\
&+\frac{1}{2}2m(n-1)\,[(0.4)(0.6)(0.2)(0.4)]^{\frac{-1}{2}} + \frac{1}{2}(2m-2)\,[(0.2)(0.3)(0.3)(0.4)]^{\frac{-1}{2}} \\
&+\frac{1}{2}(m-1)(2kn-2)\,[(0.2)(0.4)(0.3)(0.4)]^{\frac{-1}{2}} + \frac{1}{2}(2)\,[(0.2)(0.3)(0.3)(0.2)]^{\frac{-1}{2}} \\
&+\frac{1}{2}(2kn-2)\,[(0.2)(0.4)(0.3)(0.2)]^{\frac{-1}{2}} + \frac{1}{2}m(n-1)\,[(0.4)(0.6)(0.4)(0.6)]^{\frac{-1}{2}} \\
&+\frac{1}{2}m(n-1)\,[(0.2)(0.4)(0.2)(0.4)]^{\frac{-1}{2}} + \frac{1}{2}kn(m-1)\,[(0.3)(0.4)(0.3)(0.8)]^{\frac{-1}{2}} \\
&= 19.8858kmn - 8.1605kn + 12.9783mn - 4.5704m + 0.0914n + 10.8411
\end{aligned}$$

□

Theorem 5.4. *Let H_m be a fuzzy graph of multi-hydrocarbon. Then the Harmonic index of multi-hydrocarbons is*

$$H^*(H_m) = 8.0357kmn - 4.7857kn + 6.3442mn - 2.7056m + 0.0783n + 7.844$$

Proof. Using Table 6 and Definition 3.15, we have

$$\begin{aligned}
H^*(G) &= \frac{1}{2}\sum_{u_iu_j\in E(G)} [\sigma(u_i)d(u_i) + \sigma(u_j)d(u_j)]^{-1} \\
&= \frac{1}{2}\left[\frac{2}{(0.3)(0.6)+(0.4)(0.5)}\right] + \frac{1}{2}\left[\frac{(2kn-2n)}{(0.3)(0.6)+(0.4)(0.8)}\right]
\end{aligned}$$

$$+\frac{1}{2}\left[\frac{2n-2}{(0.3)(0.6)+(0.4)(0.6)}\right]+\frac{1}{2}\left[\frac{2m-2}{(0.3)(0.8)+(0.4)(0.5)}\right]$$
$$+\frac{1}{2}\left[\frac{(2kn-2n)(m-1)}{(0.3)(0.8)+(0.4)(0.8)}\right]+\frac{1}{2}\left[\frac{(m-1)(2n-2)}{(0.3)(08)+(0.4)(0.6)}\right]$$
$$+\frac{1}{2}\left[\frac{2m}{(0.4)(0.5)+(0.2)(0.3)}\right]+\frac{1}{2}\left[\frac{(k-1)mn}{(0.4)(0.8)+(0.2)(0.4)}\right]$$
$$+\frac{1}{2}\left[\frac{m(2n-2)}{(0.4)(0.6)+(0.2)(0.4)}\right]+\frac{1}{2}\left[\frac{2m-2}{(0.2)(0.3)+(0.3)(0.4)}\right]$$
$$+\frac{1}{2}\left[\frac{(m-1)(2kn-2)}{(0.2)(0.4)+(0.3)(0.4)}\right]+\frac{1}{2}\left[\frac{2}{(0.2)(0.3)+(0.3)(0.2)}\right]$$
$$+\frac{1}{2}\left[\frac{(2kn-2)}{(0.2)(0.4)+(0.3)(0.2)}\right]+\frac{1}{2}\left[\frac{m(n-1)}{(0.4)(0.6)+(0.4)(0.6)}\right]$$
$$+\frac{1}{2}\left[\frac{m(n-1)}{(0.2)(0.4)+(0.2)(0.4)}\right]+\frac{1}{2}\left[\frac{kn(m-1)}{(0.3)(0.4)+(0.3)(0.8)}\right]$$

$$= 8.0357kmn - 4.7857kn + 6.3442mn - 2.7056m + 0.0783n + 7.844$$

□

Theorem 5.5. *Suppose H_m is a multi-hydrocarbon fuzzy graph and K is the number of Benzene rings. Then the Y- index of H_m is*

$$Y_\mu(H_m) = 0.528kmn + 0.064mn - 0.12kn - 0.116m$$

Proof. Using Table 6 and Definition 3.13, we have

$$Y_\mu(H_m) = \sum_{u_iu_j\in E(G))} \mu(u_iu_j)\left[\sigma(u_i)d(u_i)^3 + \sigma(u_j)d(u_j)^3\right]$$

$$= 2(0.3)\left[(0.3)(0.6)^3 + (0.4)(0.5)^3\right] + (2kn-2n)(0.3)\left[(0.3)(0.6)^3 + (0.4)(0.8)^3\right]$$

$$+(2n-2)(0.3)\left[(0.3)(0.6)^3 + (0.4)(0.6)^3\right] + (2m-2)(0.3)\left[(0.3)(0.8)^3 + (0.4)(0.5)^3\right]$$

$$+(2kn-2n)(m-1)(0.3)\left[(0.3)(0.8)^3 + (0.4)(0.8)^3\right] + (m-1)(2n-2)(0.3)\left[(0.3)(0.8)^3 + (0.4)(0.6)^3\right]$$

$$+(2m)(0.2)\left[(0.4)(0.5)^3 + (0.2)(0.3)^3\right] + (k-1)mn(0.2)\left[(0.4)(0.8)^3 + (0.2)(0.4)^3\right]$$

$$+(0.2)(2m)(n-1)\left[(0.4)(0.6)^3 + (0.2)(0.4)^3\right] + (2m-2)(0.1)\left[(0.2)(0.3)^3 + (0.3)(0.4)^3\right]$$

$$+(0.1)(m-1)(2kn-2)\left[(0.2)(0.4)^3 + (0.3)(0.4)^3\right] + 2(0.1)\left[(0.2)(0.3)^3 + (0.3)(0.2)^3\right]$$

$$+(0.1)(2kn-2)\left[(0.2)(0.4)^3 + (0.3)(0.2)^3\right] + (0.1)m(n-1)\left[(0.4)(0.6)^3(0.4)(0.6)^3\right]$$

$$+(0.1)m(n-1)\left[(0.2)(0.4)^3 + (0.2)(0.4)^3\right] + (0.2)kn(m-1)\left[(0.3)(0.4)^3 + (0.3)(0.8)^3\right]$$

$= 0.528kmn + 0.064mn - 0.12kn - 0.116m$

□

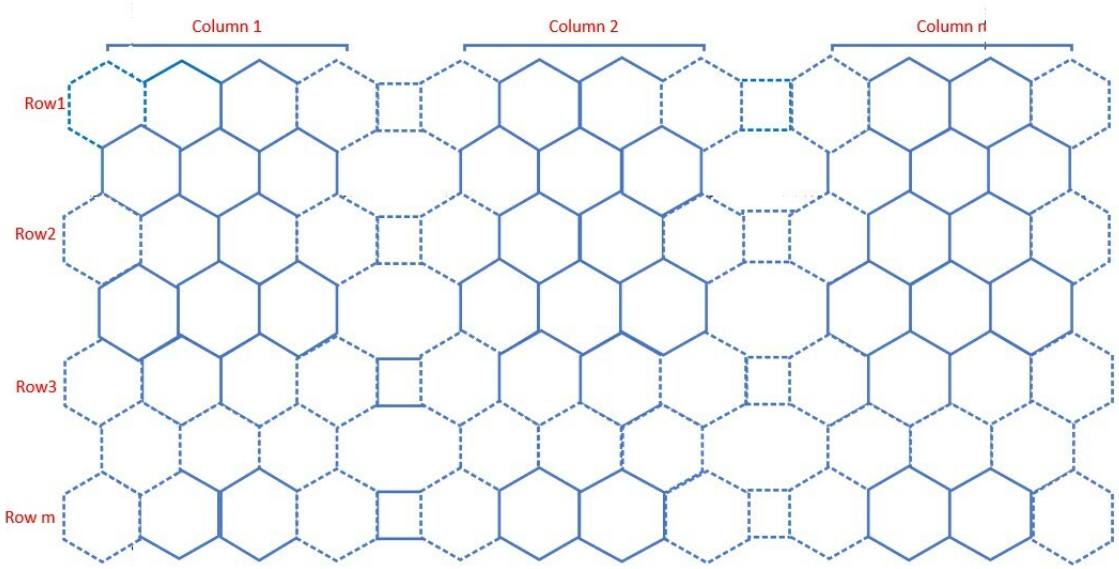


Figure 5: (m,n) unit of fuzzy graphs of multi-Hydrocarbons

6 Conclusion

This study investigated a range of topological indices within the framework of fuzzy graphs, specifically focusing on the first and second Zagreb indices, Randi index, Harmonic index, Forgotten index, and Y-index, as applied to linear and multicyclic aromatic hydrocarbons. Novel definitions were introduced for the first Zagreb index, Forgotten index, and Y-index, alongside generalized formulas based on the number of benzene rings. These formulas systematically calculate topological index values for specific hydrocarbons, enabling comparisons among different compounds. Our findings contribute to the field by offering tools that can assist researchers in predicting and estimating the physicochemical properties of molecules through accurate assessments of bond lengths and atomic masses.

References

[1] A Alameri, N. Al-Naggar, M. Al-Rumaima, M. Alsharafi, *Y-index of some graph operations* Int. J. Appl. Eng. 15(2020), 179.

[2] M. Binu, S. Mathew, J. N. Mordeson, *Connectivity index of a fuzzy graph and its application to human trafficking* Fuzzy Sets Syst. 360(2019), 117136.

[3] P. Bhattacharya, *Some remarks on fuzzy graphs* Pattern recognition letters 6(1987), 297-302.

[4] K. R. Bhutani, *On automorphisms of fuzzy graphs* Pattern Recognition Letters 9(1998), 159-162.

[5] J. A. Bondy, U. S. R. Murthy, *Graph theory with applications* The Macmillan Press Ltd., U.S.A. 1976.

[6] B. Fortual, I. Gutman, *A forgotten topological index* J. Math. Chem. 53(2015), 11841190.

[7] H. M. Fraz, K. Ali, M. F. Nadeem, *Entropy measures of silicon nanotubes using degree based topological indices* Physica Scripta, 100(2024), p. 015202. DOI10.1088/1402-4896/ad94b4

[8] B. Furtula, I. Gutman, *A forgotten topological index* J. Math. Chem. 53(2015), 1184-1190. https://doi.org/10.1007/s10910-015-0480-z

[9] A. N. Gani, S. R. Latha, *On irregular fuzzy graphs* Applied Mathematical Sciences 6(2012), 517-523.

[10] D. Gómez, J. Montero, J. Yáñez, *A coloring fuzzy graph approach for image classification* Information Sciences 176 (2006), 3645-3657

[11] I. Gutman, J. Kennedy, L. Quintas, *Perfect matchings in random hexagonal chain graphs* Journal of mathematical chemistry 6(1991), 377-383

[12] I. Gutman, N. Trinajstic, *Graph theorem and molecular orbitals. Total -electron energy of alternant hydrocarbons* Chem. Phys. Lett. 17(1972), 535538.

[13] J. L. Gross, G. Yellen, *Handbook of graph theory* CRC press, 2013.

[14] M. Hasani, M. Ghods, *M-polynomials and topological indices of porphyrin-cored dendrimers* Chem. Methodol. 7(2023), 288-306. https://doi.org/10.22034/chemm.2023.370497.1626

[15] M. Hasani, M. Ghods, *Topological indices and QSPR analysis of some chemical structures applied for the treatment of heart patients* Int. J. Quantum Chem. (2023) e27234. https://doi.org/10.1002/qua.27234

[16] M. Hasani, M. Ghods, *Calculation of topological indices along with MATLAB coding in QSPR analysis of calcium channel-blocking cardiac drugs*, J. Math. Chem. (2024). https://doi.org/10.1007/s10910-023-01570-9

[17] M. Hasani, M. Ghods, *Predicting the physicochemical properties of drugs for the treatment of Parkinson's disease using topological indices and programming MATLAB* Mol. Phys., (2023). https://doi.org/10.1080/00268976.2023.2270082

[18] M. Hasani, M. Ghods, *QSPR analysis of kidney infection (Pyelonephritis) drugs by entropy graphs weighted with topological indices, and MATLAB programming* Polycyclic Aromatic Compounds. (2024) https://doi.org/https://doi.org/10.1080/10406638.2024.2429638

[19] S. Hayat, M. Imran, *On degree based topological indices of certain nanotubes. Journal of Computational and Theoretical Nanoscience* 12(2015), 1599-1605.

[20] S. Iijima, *Helical microtubules of graphitic carbon* nature 354(1991), 56-58.

[21] S. R. Islam, M. Pal, *First Zagreb index on a fuzzy graph and its application* J. Intell. Fuzzy Syst. 40(2021), 1057510587..

[22] S. R. Islam, M. Pal, *F-index for fuzzy graph with application* To appear in TWMS J. App. Eng, Math (2021).

[23] S. R. Islam, M. Pal, *Hyper-Wiener index for fuzzy graph and its application in share market* J. Intell. Fuzzy Syst. 41(2021), 20732083.

[24] S. R. Islam, M. Pal, *Hyper-connectivity index for fuzzy graph with application* To appear in TWMS J. App. Eng, Math (2021).

[25] S. T. Jalali, M. Ghods, *Computing Y-index for some special graph* J. Discrete Math. Sci. Cryptogr. 1-10 (2022). https://doi.org/10.1080/09720529.2021.1961896

[26] S. Kalathian, S. Ramalingam, S. Raman, N. Srinivasan, *Some topological indices in fuzzy graphs* J. Intell. Fuzzy Syst. 39(2020), 6033-6046. DOI:10.3233/JIFS-189077

[27] J. N. Mordeson, P. Chang-Shyh, *Operations on fuzzy graphs*, Information sciences 79(1994), 159-170.

[28] S. Mondal, N. De, A. Pal, *Topological properties of Graphene using some novel neighborhood degree-based topological indices* Int. J. Math. Ind. 11(2019), 1950006.

[29] S. Mondal, N. De, A. Pal, *On some new neighbourhood degree based indices* Acta Chem. Iasi. 27(2019), 3146.

[30] D. Maji, G. Ghorai, *Computing F-index, coindex and Zagreb polynomials of the kth generalized transformation graphs* Heliyon 6, e05781 (2020)

[31] Z. S. Mufti, E. Fatima, R. Anjum, F. Tchier, Q. Xin, M. Hossain, and et al., *Computing First and Second Fuzzy Zagreb Indices of Linear and Multiacyclic Hydrocarbons* Journal of Function Spaces 2022, (2022)

[32] J. N. Mordeson, S. Mathew, *Advanced Topics in Fuzzy Graph* Springer, Berlin (2019).

[33] M. Pal, S. Samanta, G. Ghorai, *Modern trends in fuzzy graph theory* Springer, (2020).

[34] V. N. Popov, *Carbon nanotubes: properties and application* Materials Science and Engineering: R: Reports 43(2004), 61-102.

[35] S. Poulik, G. Ghorai, *Certain indices of graphs under bipolar fuzzy environment with applications*Soft. Comput. 24(2020), 51195131

[36] S. Poulik, G. Ghorai, *Determination of journeys order based on graphs Wiener absolute index with bipolar fuzzy information* Inf. Sci. 545(2021), 608619

[37] S. Poulik, S. Das, G. Ghorai, *Randic index of bipolar fuzzy graphs and its application in network systems* J. Appl. Math. Comput. (2021). https://doi.org/10.1007/s12190-021-01619-5

[38] M. Pal, S. Samanta, G. Ghorai, *Modern Trends in Fuzzy Graph theory* Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-8803-7

[39] J. Rada, O. Araujo, I. Gutman, *Randić index of benzenoid systems and phenylenes* Croatica Chemica Acta 74(2001), 225-235.

[40] A. Rosenfeld, *Fuzzy graphs, Fuzzy sets and their applications to cognitive and decision processes*, Elsevier, pp. 7795, 1975.

[41] X. Shi, S. Kosari, A. Talebi, S. H., Sadati, H. Rashmanlou, *Investigation of the main energies of picture fuzzy graph and its applications*, International Journal of Computational Intelligence Systems, 15(2022), 31.

[42] K. Shailaja, T. Sameena, S. Sethy, P. Patil, M. O. Ashraf, *Carbon nano tube*, a review. 1, (2013) 2321-5674.

[43] N. Trinajstic, *Chemical Graph Theory*, Second edition, CRC Press, Inc., Boca Raton, Florida, 1992

[44] H. Wiener, *Structural determination of paraffin boiling points*, J. Am. Chem. Soc. 69(1947), 1720.

[45] J. X, *The use of fuzzy graphs in chemical structure research* In: D.H. Rouvry, Ed., Fuzzy Logic in Chemistry, PP. 249-282. Elsevier, 1997

[46] L. Zaheb, *Fuzzy sets, information and control* 8(1965), 338353

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Support Preorder on Finitely Supported Cb-Sets

Mahdiyeh Haddadi
Faculty of Mathematics, Statistics and Computer science, Semnan University, Semnan, Iran

Aliyeh Hosseinabadi[1]
Faculty of Mathematics, Statistics and Computer science, Semnan University, Semnan, Iran

Abstract

This paper investigates the support-preorder, a reflexive and transitive relation that can be defined on any finitely supported **Cb**-set using the notion of support. Finitely supported **Cb**-sets extend the concept of nominal sets. We introduce the category **sp**-(**Cb-Set**)$_{\text{fs}}$ consisting of finitely supported **Cb**-sets and sp-preserving morphisms. We analyze its characteristics, including the existence of products and coproducts, and regularity, highlighting differences from the category of support-preordered nominal sets. A key distinction is the non-equivariance of the support-preorder on finitely supported **Cb**-sets. Our research contributes to a deeper understanding of the structure and interrelations between nominal sets and finitely supported **Cb**-sets, with significant implications for fields such as formal systems and homotopy type theory.

Keywords: Finitely supported M-sets, finitely supported Cb-sets, nominal sets, support-preorder
AMS Mathematical Subject Classification [2010]: 08A30, 08C05, 18A20, 18C35, 20M30, 68Q70

1 Introduction

A permutation π on a countable infinite set $\mathbb{D}$ is said to be *finitary* if it changes only a finite number of elements within $\mathbb{D}$. The group of finitary permutations on $\mathbb{D}$ is denoted by $\mathrm{Perm}_{\mathrm{f}}(\mathbb{D})$. A set X equipped with an action of $\mathrm{Perm}_{\mathrm{f}}(\mathbb{D})$ is called a $\mathrm{Perm}_{\mathrm{f}}(\mathbb{D})$-*set*. An element $x \in X$ is said to have a *finite support* $S \subseteq \mathbb{D}$ if it is invariant (fixed) under the action of any finitary permutation that fixes all elements of S, i.e., for every finitary permutation $\pi \in \mathrm{Perm}_{\mathrm{f}}(\mathbb{D})$,

$$\forall s \in S(\pi(s) = s) \Rightarrow \pi x = x.$$

A $\mathrm{Perm}_{\mathrm{f}}(\mathbb{D})$-set X in which every element has a finite support is known as a *nominal set*. Nominal sets were introduced by Murdoch J. Gabbay and Andrew Pitts in the early 2000s as a foundational framework for reasoning about formal systems involving variable-binding, [6]. Their techniques have been applied in a wide range of applications, including programming languages, type theory, and security. Murdoch J. Gabbay and Martin Hofmann, in their work [4], expanded the concept of nominal sets by employing a broader range of mappings between atoms, which involve arbitrary (possibly non-injective) finite maps on atomes (called

[1] Aliyeh Hosseinabadi

finite renamings) rather than just finite permutations. Gabby et al. further studied substitution using nominal techniques [2, 5]. Pitts, in his work [12], reformulated cubical sets in terms of monoids of finite substitutions, **Sb**, consisting of the maps $\sigma : \mathbb{D} \to \mathbb{D} \cup 2$, where $\mathbb{D}$ is disjoint from $2 = \{0, 1\}$ and the set $\{x \in X \mid \ \sigma(x) \neq x\}$ is finite. Indded, he demonstrated that the category of cubical sets is equivalent to the category of finitely supported **Cb**-sets, where the monoid **Cb** is a submonoid of the monoid **Sb** and consist of injective finite substitutions, i.e. finite substitutions that satify the injectivity condition:

$$(\forall d, d' \in \mathbb{D})\sigma(d) = \sigma(d') \notin 2 \Rightarrow d = d'.$$

Given the connection between **Cb**-sets and cubical sets, along with their applications in computer science, we are particularly interested in the monoid **Cb** and the category of finitely supported **Cb**-sets.

The concept of support is an essential tool for understanding structures with finite support. Prior research has highlighted its importance. For instance, [10] demonstrates how support can be used to define graphs on nominal sets, allowing for the analysis of their algebraic properties. In our previous work [7], we introduced the concept of support-preorder $\preceq_{\mathrm{s}}$ defined by

$$x \preceq_{\mathrm{s}} y \Leftrightarrow \operatorname{supp} x \subseteq \operatorname{supp} y,$$

on nominal sets, which is derived from the notion of support. We then explored the category **spNom** and analyzed the properties and structures induced by this preorder on nominal sets. This paper investigates the category of finitely supported **Cb**-sets equipped with the support-preorder, denoted as sp-fs-**Cb**-sets. We examine the properties of this category, including the behavior of support-preorders and **Cb**-equivariant maps.

The aim of this section is to present the technicalities necessary to follow this paper, to establish notation, and give some preliminary results. We refer readers to [8, 12] for further information.

1.1 M-sets

An (left) *M-set* for a monoid M with identity e is a set X equipped with a map $M \times X \to X, (m, x) \rightsquigarrow mx$, called an *action* of M on X, subject to the rules (i) $ex = x$ and (ii) $m(m'x) = (mm')x$, for all $x \in X$ and $m, m' \in M$.

By the category M-**Set**, we mean the category of all M-sets and all *M-equivariant maps*, i.e. $f : X \to Y$ subject to $f(mx) = mf(x)$, for all $x \in X$ and $m \in M$, between them.

In the category M-**Set**, epimorphisms are exactly surjective M-equivariant maps (see [8, Proposition I.6.15]). An element x of an M-set X is a *fixed* (or *equivariant*) element if $mx = x$, for all $m \in M$. We denote the set of all fixed elements of an M-set X by $\mathrm{Fix}(X)$. An M-set X with *discrete action* is one in which all of its elements are fixed.

A subset Y of an M-set X is an *equivariant subset* (*M-subset*) of Y if $my \in Y$, for all $m \in M$ and $y \in Y$. The subset $\mathrm{Fix}(X)$ of X is always an equivariant subset of X.

A *cyclic M-set* X is an M-set which is generated by only one element. In fact, for some $x \in X$, that takes the form of $Mx = \{mx \mid m \in M\}$.

An equivalence relation ρ on an M-set X is called a *congruence relation* on X if $x \,\rho\, x'$ implies $mx \,\rho\, mx'$, for $x, x' \in X$, $m \in M$. We denote the set of all congruences on X by $\mathsf{Con}(X)$.

1.2 Finite Substitutions monoid Sb and finitely supported Sb-sets

Throughout this paper, we will assume that $\mathbb{D}$ is a fixed, infinite, countable set whose elements are called *atomic names* (or *data values*) disjoint from the two-element set $\mathsf{2} = \{0, 1\}$.

Definition 1.1. ([12, Definition 2.1]) (i) A *finite substitution* is a map $\sigma : \mathbb{D} \to \mathbb{D} \cup \{0, 1\}$ for which the set $\{d \in \mathbb{D} \mid \sigma(d) \neq d\}$ is finite. Let **Sb** be the monoid whose elements are finite substitutions, with the monoid operation given by composition:

$$\sigma \cdot \sigma' \doteq \hat{\sigma}\sigma',$$

where $\hat{\sigma} : \mathbb{D} \cup \mathsf{2} \to \mathbb{D} \cup \mathsf{2}$ maps $\mathsf{0}$ to $\mathsf{0}$, $\mathsf{1}$ to $\mathsf{1}$, and on $\mathbb{D}$ is defined like σ. The identity element of **Sb** is the inclusion $\iota : \mathbb{D} \hookrightarrow \mathbb{D} \cup \mathsf{2}$.

(ii) If $d \in \mathbb{D}$ and $b \in \mathsf{2}$, we denote the finite substitution mapping d to b and acting as the identity an all other elements of $\mathbb{D}$ as (b/d) and call it a *ground substitution*.

(iii) The set GroundSub$\doteq\{\delta = (\mathsf{b}_1/d_1) \cdots (\mathsf{b}_k/d_k) \mid d_i \in \mathbb{D}, \mathsf{b}_i \in \mathsf{2}\}$ is a submonoid of **Sb**. We denote the set $\{d_1, \ldots, d_k\}$ by $\mathbb{D}_\delta$, for every $\delta \in$ GroundSub.

(iv) A *finite permutation* on $\mathbb{D}$ is a bijection map $\pi : \mathbb{D} \to \mathbb{D}$ for which the set $\{d \in \mathbb{D} \mid \pi(d) \neq d\}$ is finite. The set of all finite permutations on $\mathbb{D}$ is denoted by $\mathrm{Perm_f}(\mathbb{D})$ and it is a subgroup of the well-knoen group $\mathrm{Perm}(\mathbb{D})$ consisting of all permutations (bijection maps) on $\mathbb{D}$, and a submonoid of **Sb**.

Definition 1.2. [12, Definition 2.2] Suppose X is a **Sb**-set and $x \in X$.

(i) We say that $A \subseteq \mathbb{D}$ *supports* x if for every finite substitutions $\sigma, \sigma' \in$ **Sb**, we have:

$$\sigma|_A = \sigma'|_A \Rightarrow \sigma x = \sigma' x.$$

(ii) An element $x \in X$ is called a *finitely supported element*, whenever it has a finite support.

(iii) Say X is a *finitely supported* Sb-*set* when every element in X has a finite support.

The full subcategory of **Sb**-Set consisting of all finitely supported **Sb**-sets is denoted by $(\textbf{Sb-Set})_{\mathrm{fs}}$.

1.3 The monoid Cb and finitely supported Cb-sets

In this subsection, to further clarify our work, we will present a more detailed definition of the category of finitely supported **Cb**-sets, consistent with the framework used in this paper.

Definition 1.3. [12, Definition 2.7] (The monoid **Cb**) Let **Cb** $\subseteq$ **Sb** be the subset consisting of finite substitutions σ satisfying an injectivity condition that means

$$(\forall d, d' \in \mathbb{D})\sigma(d) = \sigma(d') \notin \mathsf{2} \Rightarrow d = d'.$$

(ii) A *finitely supported* **Cb**-*set* is a **Cb**-set X all of whose elements have finite supports.

(iii) A *nominal set* is a finitely supported $\mathrm{Perm_f}(\mathbb{D})$-set.

The full subcategory of **Cb-Set** consisting of all finitely supported **Cb**-sets is denoted by $(\mathbf{Cb\text{-}Set})_{\mathrm{fs}}$. The category **Nom** consisting of all nominal sets together with $\mathrm{Perm}_{\mathrm{f}}(\mathbb{D})$-equivariant maps between them is a full subcategory of $(\mathbf{Cb\text{-}Set})_{\mathrm{fs}}$. Furthermore, $(\mathbf{Cb\text{-}Set})_{\mathrm{fs}}$ itself is a full subcategory of $(\mathbf{Cb\text{-}Set})_{\mathrm{fs}}$.

Lemma 1.4. *Suppose X is a finitely supported* **Cb***-set. Then, for each $Y \in \mathcal{P}_{\mathrm{fs}}(X)$, consisting of all subsets of X that have a finite support with the evaluation action,* $\operatorname{supp} Y = \bigcup_{y\in Y} \operatorname{supp} y$.

The following is a direct consequence of Lemma 1.4.

Corollary 1.5. *In the category finitely supported* **Cb***-set, $\mathcal{P}_{\mathrm{fs}}(\mathbb{D}) = \mathcal{P}_{\mathrm{f}}(\mathbb{D})$.*

Lemma 1.6. *Let X be a* **Cb***-set and $Y, Z \in \mathcal{P}_{\mathrm{fs}}(X)$. Then, $Y \cup Z, Y \cap Z \in \mathcal{P}_{\mathrm{fs}}(X)$.*

2 Support-Preordered finitely supported Cb-sets

As stated in [7], using the notion of support, each nominal set becomes a preordered set. In the same way, every finitely supported **Cb**-set X can be thought of as a preordered set by the support-preorder (i.e. the reflexive and transitive binary relation on X) $\preceq_{\mathrm{s}}$ defined by

$$x \preceq_{\mathrm{s}} y \Leftrightarrow \operatorname{supp} x \subseteq \operatorname{supp} y,$$

We say that $(X, \preceq_{\mathrm{s}})$ is a *support-preordered finitely supported* **Cb***-set* or briefly *sp-fs-***Cb***-set* to emphasize this structure.

Definition 2.1. Suppose $(X, \preceq_{\mathrm{s}})$ and $(Y, \preceq_{\mathrm{s}})$ are two sp-fs-**Cb**-sets. A **Cb**-equivariant map $f : X \to Y$ is called *support-preorder preserving* or for convenience *sp-preserving*, whenever $f(x_1) \preceq_{\mathrm{s}} f(x_2)$, for all $x_1 \preceq_{\mathrm{s}} x_2 \in X$.

It is worth noting that a **Cb**-equivariant map between sp-fs-**Cb**-sets does not necessarily preserve support-preorder. So we consider the category of sp-fs-**Cb**-sets and sp-preserving maps between them denoted by $\mathbf{sp}\text{-}(\mathbf{Cb\text{-}Set})_{\mathrm{fs}}$.

Definition 2.2. By a downward (upward) directed finitely supported **Cb**-set, we mean an sp-fs-**Cb**-set $(X, \preceq_{\mathrm{s}})$ in which each pair of elements has a lower (upper) bound. More explicitly, for every $x_1, x_2 \in X$, there exists $x \in X$ with $x \preceq_{\mathrm{s}} x_1$ and $x \preceq_{\mathrm{s}} x_2$ ($x_1 \preceq_{\mathrm{s}} x$ and $x_2 \preceq_{\mathrm{s}} x$).

Definition 2.3. Let $(X, \preceq_{\mathrm{s}})$ be an sp-fs-**Cb**-set and $Y \in \mathcal{P}_{\mathrm{fs}}(X)$. Then we define

$$Y_{\downarrow} \doteq \{x \in X \mid x \preceq_{\mathrm{s}} y, \text{ for some } y \in Y\}$$

and

$$Y^{\uparrow} \doteq \{x \in X \mid y \preceq_{\mathrm{s}} x, \text{ for some } y \in Y\}.$$

In particular, we write $x_{\downarrow}$ and $x^{\uparrow}$ rather than $Y_{\downarrow}$ and $Y^{\uparrow}$, respectively, when $Y \in \mathcal{P}_{\mathrm{fs}}(X)$ is a singleton set $\{x\}$.

Theorem 2.4. *Let $(X, \preceq_{\mathrm{s}})$ be an sp-fs-***Cb***-set and $Y, Z \in \mathcal{P}_{\mathrm{fs}}(X)$. Then*

(i) *$Y_{\downarrow} \cup Z_{\downarrow} = (Y \cup Z)_{\downarrow}$ and $Y^{\uparrow} \cup Z^{\uparrow} = (Y \cup Z)^{\uparrow}$.*

(ii) *$\operatorname{supp} Y_{\downarrow} = \operatorname{supp} Y$, for every $Y \in \mathcal{P}_{\mathrm{fs}}(X)$.*

(iii) *the set $L_{\downarrow X} \doteq \{Y_{\downarrow}, \emptyset, X \mid Y \in \mathcal{P}_{\mathrm{fs}}(X)\}$ is a bounded lattice.*

It is worth noting that for a given sp-fs-**Cb**-set $(X, \preceq_{\mathrm{s}})$ and for $Y \in \mathcal{P}_{\mathrm{fs}}(X)$, $\operatorname{supp} Y$ is not necessarily the support for $Y^{\uparrow}$. Indeed, $x^{\uparrow}$ does not necessarily finitely supported.

Example 2.5. Consider the sp-fs-**Cb**-set X to be $\prod_{i=1}^{3}(\mathbb{D} \cup 2)$. Then, for every $d \in \mathbb{D}$,

$$(d, 0, 1)^{\uparrow} = \{(t_1, t_2, t_3) \mid d \in \{t_1, t_2, t_3\}, t_i \in \mathbb{D} \cup 2\}.$$

We show that $(d, 0, 1)^{\uparrow}$ is not finitely supported. On the contrary, suppose A is a finite support of $(d, 0, 1)^{\uparrow}$. Take $\{d_1, d_3\} \subseteq \mathbb{D} \setminus (A \cup \{d\})$. Since $(0/d_1)|_A = (d_1\ d_3)|_A$, $(0/d_1)(d, 0, 1)^{\uparrow} = (d_1\ d_3)(d, 0, 1)^{\uparrow}$. Also since $(d_3, d, d_1) \in (d, 0, 1)^{\uparrow}$ and $(d_1, d, d_3) = (d_1\ d_3)(d_3, d, d_1)$, $(d_1, d, d_3) \in (d_1\ d_3)(d, 0, 1)^{\uparrow}$. Hence, $(d_1, d, d_3) \in (0/d_1)(d, 0, 1)^{\uparrow}$, which is a contradiction. Because in this case, $(d_1, d, d_3) = (0/d_1)(t_1, t_2, t_3)$ implies $d_1 \notin \operatorname{supp}(d_1, d, d_3)$ and therefore $(d_1, d, d_3) \notin (d, 0, 1)^{\uparrow}$.

Corollary 2.6. *The set $L_{\uparrow X} \doteq \{Y^{\uparrow}, \emptyset, X \mid Y \in \mathcal{P}_{\mathrm{fs}}(X)\}$ is not necessarily a bounded lattice.*

Lemma 2.7. (i) *Let $(X, \preceq_{\mathrm{s}}) \in$ **sp**-(**Cb**-**Set**)$_{\mathrm{fs}}$ be a poset and and $\mathrm{Fix}(X) = \{\theta\}$. Then every sp-preserving map $f : X \to X$ with $f^{-1}(\{\theta\}) = \{\theta\}$ is identity.*

(ii) *The category* **sp**-(**Cb**-**Set**)$_{\mathrm{fs}}$ *is connected.*

(iii) *For each sp-preserving map $f : X \to \mathcal{P}_{\mathrm{f}}(\mathbb{D})$ and $x \in X$, we have $f(x) = \emptyset$ or $f(x) = \operatorname{supp} x$.*

Theorem 2.8. *The coproduct of a family of sp-fs-**Cb**-sets $(X_i, \preceq_{\mathrm{s}})_{i \in I}$ exists if and only if all X_i's are discrete except possibly one.*

Theorem 2.9. *The product of a family of sp-fs-**Cb**-sets $(X_i, \preceq_{\mathrm{s}})_{i \in I}$ exists if and only if all X_i's are discrete except possibly one.*

Acknowledgment

The authors express sincere gratitude to the reviewer for their valuable feedback, which significantly enhanced the paper's clarity and quality. This research was supported by a postdoctoral grant from Semnan University (grant number 20388).

References

[1] M. M. Ebrahimi, K. Keshvardoost, and M. Mahmoudi. Simple and subdirectly irreducible finitely supported cb-sets. *Theoretical Computer Science*, 706:1–21, 2018.

[2] M. J. Gabbay. A study of substitution, using nominal techniques and Fraenkel-Mostowski sets. 410(12-13):1159–1189, 2009.

[3] M. J. Gabbay. Nominal terms and nominal logics: from foundations to meta-mathematics. *Handbook of Philosophical Logic: Volume 17*, pages 79–178, 2014.

[4] M. J. Gabbay and M. Hofmann. Nominal renaming sets. In *Logic for Programming, Artificial Intelligence, and Reasoning: 15th International Conference, LPAR 2008, Doha, Qatar, November 22-27, 2008. Proceedings 15*, pages 158–173. Springer, 2008.

[5] M. J. Gabbay and A. Mathijssen. Capture-avoiding substitution as a nominal algebra. *Formal Aspects of Computing*, 20:451–479, 2008.

[6] M. J. Gabbay and A. M. Pitts. A new approach to abstract syntax with variable binding. *Formal aspects of computing*, 13:341–363, 2002.

[7] A. Hossinabadi, M. Haddadi, and K. Keshvardoost. On nominal sets with support-preorder. *Categories and General Algebraic Structures with Applications*, 17(1):141–172, 2022.

[8] M. Klip, U. Knauer, and A. V. Mikhalev. Monoids, acts and categories with applications to wreath products and graphs, 2000.

[9] S. MacLane and I. Moerdijk. *Sheaves in geometry and logic: A first introduction to topos theory*. Springer Science & Business Media, 2012.

[10] H. Pasbani and M. Haddadi. The fresh-graph of a nominal set. *Discrete Mathematics, Algorithms and Applications*, 15(07):2250161, 2023.

[11] A. M. Pitts. *Nominal sets: Names and symmetry in computer science*. Cambridge University Press, 2013.

[12] A. M. Pitts. Nominal presentation of cubical sets models of type theory. In *20th International Conference on Types for Proofs and Programs (TYPES 2014)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.

e-mail: hossinabadialiya71@semnan.ac.ir
e-mail: m.haddadi@semnan.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Exploring Conjectures in the Theory of Layered Numbers

Daniel Yaqubi[1]
University of Torbat e Jam, Torbat e Jam, Iran

Abstract

A positive integer n is called a Zumkeller number if its divisors can be partitioned into two sets with equal sums. This concept, introduced by Zumkeller in 2003, generalizes the notion of perfect numbers. In this presentation, we'll introduce these numbers and share some new results about them. We'll also talk about how they connect these numbers to other parts of number theory and mention a few unsolved problems and conjectures that people are still trying to figure out.

Keywords: Zumkeller numbers, perfect numbers, layered numbers, arithmetical functions, harmonic mean numbers.
AMS Mathematical Subject Classification [2010]: 11A25, 11B75, 11D99

1 Introduction

Let n be a positive integer. The canonical decomposition of n as a product of primes will always be written as

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

where $p_1 < p_2 \cdots < p_r$. As usual we shall denote the *number of divisors* of n by $\nu(n)$ and the *sum of the divisors* by $\sigma(n)$, so that

$$\nu(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1),$$

and

$$\sigma(n) = \sum_{d|n} d = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

A positive integer n with the property that it coincides with the sum of all positive divisors is called *perfect number*. For example, the numbers $6, 28, 496$ and 8128 are perfect. Euclid have been proved the number

$$n = 2^{m-1}(2^m - 1)$$

is perfect while $2^m - 1$ is a prime number. The prime numbers of the form $2^m - 1$ are called *Mersenne prime*. L. Euler showed that these exhaust all even perfect numbers. It is still unknown whether the set of even perfect numbers is finite or infinite, that is, it is unknown whether the set of Mersenne primes $2^m - 1$ is finite or not. It is also unknown whether or not there are any odd perfect numbers.

[1] speaker

Generalizing the concept of the perfect numbers is *Zumkeller or integer perfect numbers* that introduced by Zumkeller in 2003. The positive integer n is Zumkeller number if its divisors can be partitioned into two sets with the same sum, which will be $\sigma(n)/2$. The some values of these numbers are given in Sloane's sequences of integers (see A083207 in [5]). For example, 20 is a Zumkeller number because its divisors, $1, 2, 4, 5, 10, 20$ can be partitioned in the two sets $A = \{1, 20\}$ and $B = \{2, 4, 5, 10\}$ whose common sum is 21.

Undoubtedly, one of the most important reasons for study of Zumkeller numbers by mathematicians refer to perfect numbers, because each perfect number is a Zumkeller number.

Clearly, the necessary condition for a positive integer n be a Zumkeller number are $\sigma(n) \geq 2n$ and $\sigma(n)$ must be even number. Therefore, the number of positive odd factors of n must be even. Also, the necessary and sufficient condition for positive integer n to be a Zumkeller number is the value of $\frac{\sigma(n)-2n}{2}$ must be either zero or is a sum of distinct positive factors of n excluding n itself [4].

In [1] Clark etal., announced several results about Zumkeller, *Half-Zumkeller* and *practical* numbers and suggested some conjectures. A positive integer n is said to be Half-Zumkeller number if the proper positive factors of n can be partitioned into two disjoint parts so that the sums of the two parts are equal. Also,n is said practical if all positive integers less than n can be represented as sums of distinct factors of n. The first values of Half-zumkeller and practical numbers are given in OEIS codes A246198 and A005153, respectively.

Bhakara Rao and Peng have provided a proof for the first conjectures of Clark etal., and proved the second conjecture in some special cases. Also, they have posed several results and open problems on Zumkeller numbers, for example that $n!$ is a Zumkeller numbers for $n \geq 3$ (see [4, 2]).

In this presentation, we'll introduce these numbers and share some new results about them. We'll also talk about how they connect these numbers to other parts of number theory and mention a few unsolved problems and conjectures that people are still trying to figure out.

2 Concluding Remarks

In this work, we have delved into the fascinating world of Zumkeller and k-layered numbers, exploring their properties and connections to other number-theoretic concepts. We have presented several results characterizing Zumkeller numbers with two and three distinct prime factors, providing a deeper understanding of their structure and distribution.

While our findings contribute to the existing knowledge, numerous avenues for further research remain open. Potential future directions include:

1. **Generalizations of Zumkeller Numbers:** Extending the characterization of Zumkeller numbers to more general classes of integers, such as those with more than three distinct prime factors.

2. **Connections to Other Number Sequences:** Investigating deeper connections between Zumkeller numbers and other well-known number sequences, such as Fibonacci numbers, Lucas numbers, or harmonic mean numbers (see [3]).

3. **Algorithmic Aspects:** Developing efficient algorithms for generating and recognizing Zumkeller numbers.

4. **Statistical Properties:** Analyzing the statistical properties of Zumkeller numbers, such as their distribution and average order.

By exploring these directions, we can further unravel the mysteries of Zumkeller numbers and their place within the rich tapestry of number theory.

References

[1] S. Clark, J. Dalzell, J. Holliday, D. Leach, M. Liatti and M. Walsh, Zumkeller numbers, presented in the Mathematical Abundance Conference at Illinois State Uiversity on April 18th, 2008.

[2] Laborde, Pedro. "A note on the even perfect numbers." The American Mathematical Monthly 62.5 (1955): 348-349.

[3] C. Pomerance. On a problem of Ore: harmonic numbers, unpublished manuscript (1973), Notice Amer.Math.soc. 20(1973),a-648.

[4] Peng, Yuejian, and KPS Bhaskara Rao. "On zumkeller numbers."Journal of Number Theory, 133.4 (2013): 1135-1155.

[5] N. J. A. Sloane, *The On-Line Encyclopaedia of Integer Sequences* (2018) URL http://oeis.org.

e-mail: daniel_yaqubi@yahoo.es
e-mail: yaqubi@tjamcaas.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

On the directed $n-$ power graph of a class of finite groups

Mansour Hashemi[1]
Mathematical Sciences, University of Guilan, Rasht, Iran

Mina Pirzadeh
Mathematical Sciences, University of Guilan, Rasht, Iran

Mojde Afiatdoust
Mathematical Sciences, University of Guilan, Rasht, Iran

Abstract

We consider the finitely presented groups H_m as follows;

$$H_m = \langle a, b | a^{m^2} = b^m = 1, b^{-1}ab = a^{1+m} \rangle, m \geq 2.$$

For integer $n > 1$, the directed $n-$ power graph of a group G is a graph whose vertices are elements of G with an edge from x to y if $y = x^n$. In this paper, we study the $n-$ power graph of H_m.

Keywords: Finite groups, nilpotent groups, power graph, input degree

AMS Mathematical Subject Classification [2010]: 05C25, 05E30

1 Introduction

The power graph $P(G)$ is a graph whose vertices are the elements of the group G, and two vertices are adjacent if one is a power of the other. First, the Power graphs were introduced in [5] by A. V. Kelarev and S. J. Quinn in 2000, and further studied in [1] by I. Chakrabarty, S. Ghosh, and M. K. Sen in 2009.

Definition 1.1. Let G be a finite group. The directed power graph of G, denoted by $\overrightarrow{P}(G)$, is a graph with vertex set G such that there is a directed edge from vertex x to vertex y if and only if x and y are distinct and y is a positive power of x.

Definition 1.2. Let G be a finite group. For $n > 1$, the $n-$ power graph of the group G, denoted by $P_n(G)$, is a graph with vertex set $V = G$, such that $(x, y) \in E$ if and only if $y = x^n$.

Definition 1.3. The in-degree of vertex y in a directed graph, denoted by $\text{Indeg}(y)$, is the number of edges which terminate at y.

[1] speaker

Example 1.4. The 2-power graph of the group K_4 is given by $k_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle = \{e, a, b, c\}$. According to Definition 1.2, we obtain $(k_4)^2 = \{e, a^2, b^2, c^2\} = \{e\}$. Therefore,

$$Indeg(e) = 3, Indeg(a) = Indeg(b) = Indeg(c) = 1.$$

We Consider the finite group H_m defined by the presentation

$$H_m = \langle a, b \mid a^{m^2} = b^m = 1,\ b^{-1}ab = a^{1+m} \rangle,\ m \geq 2.$$

In this paper, we study the $n-$ power graph of H_m. In Section 2, we state some lemmas and theorems are needed in the proofs of main results. Section 3 is devoted to compute the formula for $P_n(G)$, where $G = H_m$. These results can be checked by MATLAB program.

2 Preliminary

In this section, we state lemmas that establishes some properties of groups of nilpotency class two, where $[x, y] = x^{-1}y^{-1}xy$.

Lemma 2.1. *If G is a group and $G' \subseteq Z(G)$, then the following hold for every integer k and $x, y, z \in G$:*

1. $[xy, z] = [x, z][y, z]$ *and* $[x, yz] = [x, y][x, z]$.
2. $[x^k, y] = [x, y^k] = [x, y]^k$.
3. $(xy)^k = x^k y^k [y, x]^{k(k-1)/2}$.
4. *If* $G = \langle x, y \rangle$ *then* $G' = \langle [x, y] \rangle$.

Lemma 2.2. *Let $G = H_m$.*

1. *Every element of H_m may be uniquely represented by $b^j a^i$, where $0 \leq i \leq m^2 - 1$ and $0 \leq j \leq m - 1$.*
2. $Z(G) = G' = \langle a^m \rangle$ *and* $|Z(G)| = m$.
3. $|H_m| = m^3$.
4. $x^s y^r = y^r x^{s+mrs}$.

3 Computations on the directed $n-$ power graph of H_m

In the present part, we consider the Indeg of vertices in the $n-$ power graph of the finite group H_m. First, we need the following Lemma.

Lemma 3.1. *For integers $m, n \geq 2$; If $G = H_m$ and $x \in G$, then*

$$x^n = b^{nj} a^{ni + \frac{mn(n-1)}{2} ij}.$$

Theorem 3.2. *Let $m, n > 1$, $d_1 = (m, n)$, and $d_2 = (m^2, n)$. Assume*

$$A = \left\{ b^j a^i \mid j \in \{d_1, 2d_1, \ldots, \frac{m}{d_1} \times d_1\},\ i \in \{d_2, 2d_2, \ldots, \frac{m^2}{d_2} \times d_2\} \right\}$$

Thus, if $y \in A$, then $Indeg(y) \geq 1$.

Proof. According to Lemma 2.2, let $y = b^j a^i$ be an element of H_m where $1 \leq j \leq m$ and $1 \leq i \leq m^2$. If $y = x^n$ when $x = b^{j_1}a^{i_1} \in H_m$, $1 \leq j_1 \leq m$ and $1 \leq i_1 \leq m^2$, then by Lemma 3.1 we have $b^j a^i = b^{nj_1}a^{ni_1+\frac{mn(n-1)}{2}i_1 j_1}$. By the uniqueness of the representation of elements in H_m, we obtain

$$\begin{cases} nj_1 \equiv j \pmod{m} \\ ni_1 + \dfrac{mn(n-1)}{2}i_1 j_1) \equiv i \pmod{m^2} \end{cases}$$

Let $d_1 = (m, n)$. Then we get

$$\begin{cases} j_1 \equiv (\frac{n}{d_1}) * (\frac{j}{d_1}) \pmod{\frac{m}{d_1}} \\ i_1(n + \frac{mn(n-1)}{2}j_1) \equiv i \pmod{m^2} \end{cases} \tag{1}$$

The first congruence of the system 1, has the solution $j_1 \equiv (\frac{n}{d_1})(\frac{j}{d_1}) \pmod{\frac{m}{d_1}}$ if and only if $d_1|j$. Then $j \in \{d_1, 2d_1, \ldots, \frac{m}{d_1} \times d_1\}$. This means that j has $\frac{m}{d_1}$ choices. Now, assume $d_2 = (m^2, n)$. Consequently, the second congruence in system 1 , we get $i_1(\frac{n}{d_2} + \frac{mn(n-1)}{2d_2}j_1) \equiv \frac{i}{d_2} \pmod{\frac{m^2}{d_2}}$. i_1 has solution if and only if $d_2|i$. Therefore, $i \in \left\{d_2, 2d_2, \ldots, \dfrac{m^2}{d_2} \times d_2\right\}$. Thus, we have $\dfrac{m^2}{d_2}$ choices for i. By this results, we get $y \in \left\{b^j a^i \mid j \in \left\{d_1, 2d_1, \ldots, \dfrac{m}{d_1} \times d_1\right\},\ i \in \left\{d_2, 2d_2, \ldots, \dfrac{m^2}{d_2} \times d_2\right\}\right\}$. Hence, the proof is completed. □

Acknowledgment

The authors would like to thank reviewers for the reading and their useful comments in this paper.

References

[1] I. Chakrabarty, S. Ghosh and M. K. Sen, Undirected power graphs of semigroups, Semigroup Forum, 78 (2009), 410-426. 30, 45, 46, 61, 64, 69

[2] M. Hashemi , M. Pirzadeh, *A generalization of the $n^{th}-$ commutativity degree in finite groups, Journal of Computational Sciences and Engineering* , 1 (2022), no. 2, 33-40.

[3] M. Hashemi , M. Pirzadeh and S. A. Gorgian, *The probability that the commutator equation $[x, y] = g$ has solution in a finite group, Journal of Algebra and Related Topics*, 7 (2020), no. 2, 47-61.

[4] M.Hashemi and M. Pirzadeh, *$t-$nacci sequences in some special groups of order m^3.* Mathematical Reports 20(4)(2018), 389-399.

[5] G. A. Jones, J. M. Jones, Elementary Number Theory, Springer, New Delhi, 2005. 30, 64.

e-mail: m_hashemi@guilan.ac.ir
e-mail: m_pirzadeh@phd.guilan.ac.ir
e-mail: mojde.afiatdoust@gmail.com

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

On the commuting conjugacy class graphs of some finite groups

Mehdi Rezaei[1]
Department of Mathematics, Buein Zahra Technical University, Buein Zahra, Qazvin, Iran

Abstract

Let G denote a finite non-abelian group. The commuting conjugacy class graph, denoted as $\Gamma(G)$, is defined such that its vertices correspond to the non-central conjugacy classes of G. Two distinct vertices A and B in $\Gamma(G)$ form an edge if there exist elements $a \in A$ and $b \in B$ satisfying the condition $ab = ba$. In this paper, we concentrate on the commuting conjugacy class graph of the group $PSL(2, 2^k)$ for $k \geq 2$ and explore certain properties associated with it.

Keywords: Commuting conjugacy class graph, Normalized Laplacian spectrum, Signless Laplacian spectrum
Mathematics Subject Classification [2010]: 05C25, 05C50, 20D60

1 Introduction

A graph Γ consists of a finite, non-empty set of objects known as vertices, accompanied by a collection of unordered pairs of distinct vertices referred to as edges. The vertex set of Γ is denoted by $V(\Gamma)$, while the edge set is denoted by $E(\Gamma)$. In this paper, it is assumed that all graphs are simple, finite, and undirected. The adjacency matrix $A(\Gamma) = (a_{ij})$ is defined as an n-square $(0,1)$-matrix where $a_{ij} = 1$ if and only if v_i and v_j are adjacent, with $V(\Gamma) = \{v_1, \ldots, v_n\}$. The degree of vertex v_i is represented by $d_\Gamma(v_i)$, and the degree matrix $D(\Gamma)$ is formulated as $D(\Gamma) = \mathrm{diag}(d_\Gamma(v_1), d_\Gamma(v_2), \ldots, d_\Gamma(v_n))$, serving as the diagonal matrix of vertex degrees. Accordingly, the Laplacian, signless Laplacian, and normalized Laplacian matrices of graph Γ are defined as $L(\Gamma) = D(\Gamma) - A(\Gamma)$, $Q(\Gamma) = D(\Gamma) + A(\Gamma)$, and $\mathcal{L}(\Gamma) = (\mathcal{L}_{ij})$, respectively, where

$$\mathcal{L}_{ij} = \begin{cases} 1 & i = j \text{ and } d_\Gamma(v_i) \neq 0, \\ -\frac{1}{\sqrt{d_\Gamma(v_i) d_\Gamma(v_j)}} & v_i v_j \in E(\Gamma), \\ 0 & \text{otherwise.} \end{cases}$$

Recall that the Laplacian spectrum, signless Laplacian spectrum and normalized Laplacian spectrum of graph Γ denoted by $Spec_L(\Gamma) = \{\lambda_1^{a_1}, \lambda_2^{a_2}, \ldots, \lambda_l^{a_l}\}$, $Spec_Q(\Gamma) = \{\mu_1^{b_1}, \mu_2^{b_2}, \ldots, \mu_m^{b_m}\}$ and $Spec_{\mathcal{L}}(\Gamma) = \{\gamma_1^{c_1}, \gamma_2^{c_2}, \ldots, \gamma_n^{c_n}\}$, respectively, where $\lambda_1, \lambda_2, \ldots, \lambda_l$ are the eigenvalues of $L(\Gamma)$ with multiplicities $a_1, a_2, \ldots, a_l$; $\mu_1, \mu_2, \ldots, \mu_m$ are the eigenvalues of $Q(\Gamma)$ with multiplicities $b_1, b_2, \ldots, b_m$ and $\gamma_1, \gamma_2, \ldots, \gamma_n$ are the eigenvalues of $\mathcal{L}(\Gamma)$ with multiplicities $c_1, c_2, \ldots, c_n$ (see [2]). Recent studies have presented findings on the spectrum of Laplacian and signless Laplacian for various graphs. For instance, see [4], [6], [9], [10], [11].

Over the past few years, two types of conjugacy class graphs have emerged by focusing on non-central conjugacy classes of a group G as their vertices, and constructing the edge set based on specific criteria related to either the sizes of the conjugacy classes or the orders of the class representatives (see [3] and [18], respectively). Extensive investigations have been conducted into the properties of these graphs (refer to [5], [7]–[8], [14], [15]). Subsequently, Herzog, Longobardi, and Maj in [12] explicated the structure of

[1] speaker

the commuting conjugacy class graph $\Gamma(G)$. This graph is defined such that its vertex set comprises the non-central conjugacy classes of G, where two distinct vertices A and B are connected by an edge if there exist elements $a \in A$ and $b \in B$ satisfying $ab = ba$. They proved that $\Gamma(G)$ has no edges if and only if G is isomorphic to one of the groups D_8, Q_8, or S_3. Furthermore, Mohammadian, Erfanian, Farrokhi D. G., and Wilkens in [13] provided a classification of all finite groups G such that $\Gamma(G)$ is triangle-free. In addition, Rezaei and Foruzanfar in [16] determined the structure of the commuting conjugacy class graph for groups G with the condition that $\frac{G}{Z(G)}$ is isomorphic to a Frobenius group of order pq or p^2q. This paper aims to explore the commuting conjugacy class graph of group $PSL(2, 2^k)$ for $k \geq 2$ and to calculate its Laplacian spectrum, signless Laplacian spectrum, and normalized Laplacian spectrum. This work provides new information about the commuting conjugacy class graphs. It is important to note that throughout this study, G is considered to be a finite group.

2 Preliminaries

In this section, we give some preliminary results that will be used in the proof of our main results.

Proposition 2.1. *(Proposition 3.21 of [1]) Let $G = PSL(2, q)$, where q is a p-power (p prime) and let $k = gcd(q - 1, 2)$. Then*
(1) a Sylow p-subgroup P of G is an elementary abelian group of order q and the number of Sylow p-subgroups of G is $q + 1$.
(2) G contains a cyclic subgroup A of order $t = \frac{q-1}{k}$ such that $N_G(\langle u\rangle)$ is a dihedral group of order $2t$ for every non-trivial element $u \in A$.
(3) G contains a cyclic subgroup B of order $s = \frac{q+1}{k}$ such that $N_G(\langle u\rangle)$ is a dihedral group of order $2s$ for every non-trivial element $u \in B$.
(4) The set $\{P^x, A^x, B^x | x \in G\}$ is a partition of G. Suppose a is a non-trivial element of G.
(5) If $q > 5$ and $q \equiv 1$ mod 4, then

$$C_G(a) = \begin{cases} N_G(\langle a\rangle) & \text{if } a^2 = 1 \text{ and } a \in A^x \text{ for some } x \in G, \\ A^x & \text{if } a^2 \neq 1 \text{ and } a \in A^x \text{ for some } x \in G, \\ B^x & \text{if } a \in B^x \text{ for some } x \in G, \\ P^x & \text{if } a \in P^x \text{ for some } x \in G. \end{cases}$$

(6) If $q > 5$ and $q \equiv 3$ mod 4, then

$$C_G(a) = \begin{cases} N_G(\langle a\rangle) & \text{if } a^2 = 1 \text{ and } a \in B^x \text{ for some } x \in G, \\ B^x & \text{if } a^2 \neq 1 \text{ and } a \in B^x \text{ for some } x \in G, \\ A^x & \text{if } a \in A^x \text{ for some } x \in G, \\ P^x & \text{if } a \in P^x \text{ for some } x \in G. \end{cases}$$

(7) If $q \equiv 0$ mod 4, then

$$C_G(a) = \begin{cases} A^x & \text{if } a \in A^x \text{ for some } x \in G, \\ B^x & \text{if } a \in B^x \text{ for some } x \in G, \\ P^x & \text{if } a \in P^x \text{ for some } x \in G. \end{cases}$$

Definition 2.2. A group G is called a CA-group if $C_G(x)$ is abelian for all $x \in G - Z(G)$.

Lemma 2.3. *(Lemma 3.1 of [17]) Let G be a CA-group. The non-central conjugacy classes x^G and y^G of G are adjacent in $\Gamma(G)$ if and only if $C_G(x)$ and $C_G(y)$ are conjugate in G.*

Theorem 2.4. *(Theorem 3.3 of [17]) If G is a CA-group, then*

$$\Gamma(G) = \cup_{\frac{C_G(x)}{\sim} \in A(G)} K_{\frac{nC_G(x)}{\sim}}$$

where

$$\frac{nC_G(x)}{\sim} = \frac{|C_G(x)| - |Z(G)|}{[N_G(C_G(x)) : C_G(x)]}, \quad A(G) = \frac{Cent(G) \setminus \{G\}}{\sim}$$

and $\sim$ is an equivalence relation on $Cent(G) \setminus \{G\}$ by $C_G(x) \sim C_G(y)$ if and only if $C_G(x)$ and $C_G(y)$ are conjugate in G.

It is well-known that the Laplacian spectrum, signless Laplacian spectrum and normalized Laplacian spectrum of the complete graph K_n on n vertices are given by

$$Spec(K_n) = \{(-1)^{n-1}, (n-1)^1\}, Spec_L(K_n) = \{0^1, n^{n-1}\}, Spec_Q(K_n) = \{(2n-2)^1, (n-2)^{n-1}\}$$
$$and \quad Spec_{\mathcal{L}}(K_n) = \{0^1, (\frac{n}{n-1})^{n-1}\}$$

Further, if $\Gamma = K_{m_1} \cup K_{m_2} \cup \ldots \cup K_{m_l}$, where K_{m_i} are complete graphs on m_i vertices for $1 \leq i \leq l$, then

$$Spec(\Gamma) = \{(-1)^{\sum_{i=1}^{l} m_i - l}, (m_1-1)^1, (m_2-1)^1, \ldots, (m_l-1)^1\},$$
$$Spec_L(\Gamma) = \{0^l, m_1^{m_1-1}, m_2^{m_2-1}, \ldots, m_l^{m_l-1}\},$$
$$Spec_Q(\Gamma) = \{(2m_1-2)^1, (m_1-2)^{m_1-1}, (2m_2-2)^1, (m_2-2)^{m_2-1}, \ldots, (2m_l-2)^1, (m_l-2)^{m_l-1}\}$$
$$and \quad Spec_{\mathcal{L}}(\Gamma) = \{0^l, (\frac{m_1}{m_1-1})^{m_1-1}, (\frac{m_2}{m_2-1})^{m_2-1}, \ldots, (\frac{m_l}{m_l-1})^{m_l-1}\}.$$

3 Main results

In this section, we state our main results.

Proposition 3.1. *The group $G = PSL(2, 2^n)$ is a CA-group.*

Proof. Let $G = PSL(2, 2^n)$. Then G is a non-abelian group of order $2^n(2^{2n}-1)$ with trivial center. By Proposition 2.1, the set of centralizers of non-trivial elements of G is given by $\{A^x, B^x, P^x | x \in G\}$, where P is an elementary abelian 2-subgroup of order 2^n and A, B are cyclic subgroups of G having orders $2^n - 1$ and $2^n + 1$, respectively. Therefore, $G = PSL(2, 2^n)$ is a CA-group. □

Theorem 3.2. *Let $G = PSL(2, 2^n)$. Then the commuting conjugacy class graph of G is given by $\Gamma(G) = K_1 \cup K_{2^{n-1}-1} \cup K_{2^{n-1}}$.*

Proof. Let $G = PSL(2, 2^n)$. By Proposition 3.1, $G = PSL(2, 2^n)$ is a CA-group and the set of centralizers of non-trivial elements of G is given by $\{A^x, B^x, P^x | x \in G\}$, where P is an elementary abelian 2-subgroup of order 2^n and A, B are cyclic subgroups of G having orders 2^n-1 and 2^n+1, respectively. Also, By Proposition 2.1, the number of conjugates of P, A and B in G are $2^n + 1$, $2^{n-1}(2^n + 1)$ and $2^{n-1}(2^n - 1)$, respectively. Thus, by Theorem 2.4, $A(G) = \{\frac{A}{\sim}, \frac{B}{\sim}, \frac{P}{\sim}\}$ and $\frac{nA}{\sim} = \frac{|A|-|Z(G)|}{[N_G(A):A]} = 2^{n-1} - 1$, $\frac{nB}{\sim} = \frac{|B|-|Z(G)|}{[N_G(B):B]} = 2^{n-1}$ and $\frac{nP}{\sim} = \frac{|P|-|Z(G)|}{[N_G(P):P]} = 1$. Therefore, we conclude that $\Gamma(G) = K_1 \cup K_{2^{n-1}-1} \cup K_{2^{n-1}}$. □

For example, the commuting conjugacy class graph of $G = PSL(2, 8)$ is shown below.

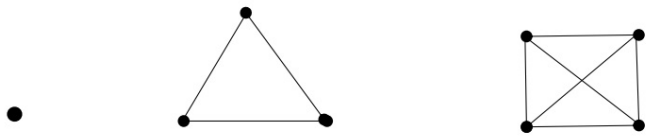


Figure 1: Commuting conjugacy class graph of $PSL(2, 8)$

Theorem 3.3. *Let $G = PSL(2, 2^n)$. Then we have:*

(*i*) *The Laplacian spectrum of the commuting conjugacy class graph of G is given by*

$$\{0^3, (2^{n-1}-1)^{2^{n-1}-2}, (2^{n-1})^{2^{n-1}-1}\}.$$

(*ii*) *The signless Laplacian spectrum of the commuting conjugacy class graph of G is given by*

$$\{0^1, (2^n-4)^1, (2^{n-1}-3)^{2^{n-1}-2}, (2^n-2)^1, (2^{n-1}-2)^{2^{n-1}-1}\}.$$

(*iii*) *The normalized Laplacian spectrum of the commuting conjugacy class graph of G is given by*

$$\{0^3, (\frac{2^{n-1}-1}{2^{n-1}-2})^{2^{n-1}-2}, (\frac{2^{n-1}}{2^{n-1}-1})^{2^{n-1}-1}\}.$$

Proof. The results follow by Theorem 3.2 and the last paragraph of section 2. □

References

[1] A. Abdollahi, S. Akbari, H. R. Maimani, *Non-commuting graph of a group*, J. Algebra, 298 (2006), pp. 468–492.

[2] Abdussakir, R. R. Elvierayani and M. Nafisah, *On the spectra of commuting and non commuting graph on dihedral group*, Cauchy-Jurnal Mat. Murni dan Apl., 4 (2017), pp. 176–182.

[3] E. A. Bertram, M. Herzog and A. Mann, *On a graph related to conjugacy classes of groups*, Bull. Lond. Math. Soc., 22(6) (1990), pp. 569–575.

[4] Y. Chen, R. Pan and X. Zhang, *The Laplacian spectra of graphs and complex networks*, J. Univ. Sci. Technol. China, 40(12) (2010), pp. 1236–1244.

[5] D. Chillag, M. Herzog and A. Mann, *On the diameter of a graph related to conjugacy classes of groups*, Bull. Lond. Math. Soc., 25(3) (1993), pp. 255–262.

[6] S. Y. Cui and G. X. Tian, *The spectrum and the signless Laplacian spectrum of coronae*, Linear Algebra Appl., 437(7) (2012), pp. 1692–1703.

[7] M. Fang and P. Zhang, *Finite groups with graphs containing no triangles*, J. Algebra, 264(2) (2003), pp. 613–619.

[8] Z. Foruzanfar and M. Rezaei, *On EPO-groups with a given property on their conjugacy classes*, Comm. Algebra, 50(4) (2022), pp. 1441–1445.

[9] R. Grone, R. Merris and V. S. Sunder, *The Laplacian spectrum of a graph*, SIAM J. Matrix Anal. Appl., 11(2) (1990), pp. 218–238.

[10] R. Grone and R. Merris, *The Laplacian spectrum of a graph II*, SIAM J. Discret. Math., 7(2) (1994), pp. 221–229.

[11] G. Guo and G. Wang, *On the (signless) Laplacian spectral characterization of the line graphs of lollipop graphs*, Linear Algebra Appl., 438(12) (2013), pp. 4595–4605.

[12] M. Herzog, P. Longobardi and M. Maj, *On a commuting graph on conjugacy classes of groups*, Comm. Algebra, 37(10) (2009), pp. 3369–3387.

[13] A. Mohammadian, A. Erfanian, M. Farrokhi D. G. and B. Wilkens, *Triangle-free commuting conjugacy class graphs*, J. Group Theory, 19(6) (2016), pp. 1049–1061.

[14] A. Moreto, G. Qian and W. Shi, *Finite groups whose conjugacy class graphs have few vertices*, Arch. Math. (Basel), 85(2) (2005), pp. 101–107.

[15] M. Rezaei and Z. Foruzanfar, *Classification of solvable groups with a given property*, Bull. Iranian Math. Soc., 43(6) (2017), pp. 1791–1800.

[16] M. Rezaei and Z. Foruzanfar, *The commuting conjugacy class graphs of finite groups with a given property*, Georgian Math. J., 31(1) (2024), pp. 121–127.

[17] M. A. Salahshour and A. R. Ashrafi, *Commuting conjugacy class graph of finite CA-groups*, Khayyam J. Math., 6(1) (2020), pp. 108–118.

[18] X. Z. You and G. H. Qian, *A new graph related to conjugacy classes of finite groups*, Chinese Ann. Math. Ser. A, 28(5) (2007), pp. 631–636.

Email: mehdrezaei@gmail.com, m_rezaei@bzte.ac.ir
ORCID iD: 0000-0001-6999-9703

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Study of $Gt - EDB$ GRAPHS

Zohreh Aliannejadi[1]
Department of mathematics, Islamic Azad university, South-Branch, Tehran, Iran.

Somayeh Shafiee Alamoti
Department of mathematics, Islamic Azad university, South-Branch, Tehran, Iran.

Abstract

In this article, we explore the concept of a generalized $t-$edge distance-balanced graph, which is a connected and non-empty graph where the number of edges closer to one endpoint of an edge is equal to t times the number of edges closer to the other endpoint, or vice versa. We identify different types of such graphs and examine their edge-szeged index.

Keywords: Generalized t-edge distance-balanced graphs, Generalized t-nicely edge distance-balanced graphs, Edge-szeged index, Complete bipartite graphs

AMS Mathematical Subject Classification [2010]: 05C12, 05C25

1 Introduction

The notion of graph is a pivotal tool to make use of the modelling of the phenomena and it is taken into consideration in many studies in a recent decades. One of the optimal uses of graphs theory is to classify graphs based on discriminating quality. This phenomenon can be best observed in distance-balanced graphs has been determined by [13]. Also, it is investigated in some papers, we refer the reader to ([1],[2],[3],[4],[5],[6],[10],[11],[14]-[19]) and references therein.

We consider A is a connected, finite and undirected graph throughout of this paper, in which its vertex set is $V(A)$ and its edge set is $E(A)$. In graph A, the interval among vertices $\alpha, \beta \in V(A)$ is introduced the number of edges in the least interval joining them and it is indicated by $d_A(\alpha, \beta)$ (see [4, 8]). For every two desired vertices α, β of $V(A)$ we indicate $n_\alpha^A(f) = |W_{a,\beta}^A| = |\{a \in V(A)|d_A(a, \alpha) < d_A(a, \beta)\}|$. In the same way, we would define $n_\beta^A(f) = |W_{\beta,\alpha}^A|$. We name A distance-balanced (DB) while for adjacent vertices α and β of A, we have $|W_{\alpha,\beta}^A| = |W_{\beta,\alpha}^A|$.

For each two desired edges $f = \alpha\beta$, $\acute{f} = \acute{\alpha}\acute{\beta}$, the distance between f and $\acute{f}$ is introduced via:

$$d_A(f, \acute{f}) = \min\{d_A(\alpha, \acute{f}), d_A(\beta, \acute{f})\} = \min\{d_A(\alpha, \acute{\alpha}), d_A(\alpha, \acute{\beta}), d_A(\beta, \acute{\alpha}), d_A(\beta, \acute{\beta})\}.$$

[1] speaker

Set $M_{\alpha}^{A}(f) = \{\acute{f} \in E(A) | d_A(\alpha, \acute{f}) < d_A(\beta, \acute{f})\}$ and $m_{\alpha}^{A}(f) = |M_{\alpha}^{A}(f)|$,
$M_{\beta}^{A}(f) = \{\acute{f} \in E(A) | d_A(\beta, \acute{f}) < d_A(\alpha, \acute{f})\}$ and $m_{\beta}^{A}(f) = |M_{\beta}^{A}(f)|$,
and $M_{0}^{A}(f) = \{\acute{f} \in E(A) | d_A(\alpha, \acute{f}) = d_A(\beta, \acute{f})\}$ and $m_{0}^{A}(f) = |M_{0}^{A}(f)|$.

Presume that $f = \alpha\beta \in E(A)$. For every two integers i, j we consider:

$$\acute{D}_{j}^{i}(f) = \{\acute{f} \in E(A) | d_A(\acute{f}, \alpha) = i, d_A(\acute{f}, \beta) = j\}.$$

A "distance partition" of $E(A)$ is concluded by sets $\acute{D}_{j}^{i}(f)$ due to the edge $f = \alpha\beta$. Merely the sets $\acute{D}_{i}^{i-1}(f)$, $\acute{D}_{i}^{i}(f)$ and, $\acute{D}_{i-1}^{i}(f)$, for each $(1 \leqslant i \leqslant d)$ might be nonempty according to the triangle inequality (The diameter of the graph A is d), as well as $\acute{D}_{0}^{0}(f) = \phi$.

A graph A is said to be generalized t-edge distance-balanced for $t \in \mathbb{N}$ and $t > 1$, so that for each edge $f = \alpha\beta$ of $E(A)$, either $m_{\alpha}^{A}(f) = tm_{\beta}^{A}(f)$ or $m_{\beta}^{A}(f) = tm_{\alpha}^{A}(f)$. For convenience, we would write $Gt - EDBG$ instead of generalized t-edge distance-balanced graph and also $Gt - EDB$ instead of generalized t-edge distance-balanced. In the same way, we define generalized t-distance-balanced graphs ($Gt-DB$), in which $n_{\alpha}^{A}(f) = tn_{\beta}^{A}(f)$, or $n_{\beta}^{A}(f) = tn_{\alpha}^{A}(f)$.

We also remind that the sets $W_{\alpha,\beta}^{A}$ and $M_{\alpha}^{A}(f)$ become visible as the well-known Szeged index and edge-Szeged index of a graph A in the chemical graph theory, in which $S_z(A) = \sum_{\alpha\beta \in E(A)} |W_{\alpha,\beta}|.|W_{\beta,\alpha}|$ and $S_{z_e}(A) = \sum_{\alpha\beta \in E(A)} m_{\alpha}^{A}(f).m_{\beta}^{A}(f)$, respectively, cf. [7,8,9].

A graph A is called *edge distance-balanced* (briefly EDB), while we have $m_{\alpha}^{A}(f) = m_{\beta}^{A}(f)$. Also we define A as *nicely edge distance-balanced* ($NEDB$), whenever there exists a positive integer $\acute{\gamma}_A$, so that for every edge $f = \alpha\beta$ we have: $m_{\alpha}^{A}(f) = m_{\beta}^{A}(f) = \acute{\gamma}_A$.

It is said A as a graph is *strongly edge distance-balanced* ($SEDB$), whenever for each $i \geq 1$ it holds:

$$\acute{D}_{i-1}^{i}(f) = \acute{D}_{i}^{i-1}(f)$$

According to the stated definition, clearly if graph be $SEDB$, then it is a EDB graph.
In this segment, we would express some examples and results concerning $Gt - EDB$ graphs.

2 Main results

At first, we present an example of $Gt - EDB$ graph.

Example 2.1. The complete bipartite graphs $K_{n,tn}$ are a class of $Gt - EDB$ graphs.

Proof. Let X and Y be two separate parts of $K_{n,tn}$, such that for every edge $f = \alpha\beta$, $\alpha \in X$ and $\beta \in Y$. As we know $K_{n,tn}$ is a bipartite graph with diameter 2. Then α has $(tn - 1)$ adjacent edges and β includes $(n - 1)$ adjacent edges. According to the definition of $m_{\alpha}^{A}(f)$, we obtain $m_{\alpha}^{A}(f) = tn$ and $m_{\beta}^{A}(f) = n$. Thus, $m_{\alpha}^{A}(f) = tm_{\beta}^{A}(f)$. This implies that $K_{n,tn}$ is a $Gt - EDB$ graph. □

Proposition 2.2. *Assume that A is a $Gt - EDB$ bipartite graph, where its diameter is 2. Then for each pair of adjacent vertices α and β, $deg(\alpha) = tdeg(\beta)$.*

Proof. Since A is a $Gt-EDB$ graph, then $m_{\alpha}^{A}(f)=tm_{\beta}^{A}(f)$ and we have

$$|\{f\}\bigcup_{i=1}^{d-1}\acute{D}_{i-1}^{i}(f)|=t|\{f\}\bigcup_{i=1}^{d-1}\acute{D}_{i}^{i-1}(f)|.$$

Therefore,

$$\sum_{i=1}^{d-1}|\acute{D}_{i-1}^{i}(f)|=t\sum_{i=1}^{d-1}|\acute{D}_{i}^{i-1}(f)|+(t-1). \tag{1}$$

If $|\acute{D}_{1}^{2}(f)|=r$, then $|\acute{D}_{2}^{1}(f)|=tr+(t-1)$. Thus, $deg(\beta)=r+1$ and $deg(\alpha)=tr+t=t(r+1)$. Therefore, always $deg(\alpha)=tdeg(\beta)$. □

Lemma 2.3. *Suppose that A is a $Gt-EDB$ bipartite graph with $d=2$. Then A can only be $K_{n,tn}$.*

Proof. Consider that A is a $Gt-EDB$ bipartite graph, in which its diameter is equal to 2. It is asserted that A is a complete bipartite graph. If not, it can not have a diameter of 2. The result is obtained from Proposition 2.2 that, $deg(\alpha)=tdeg(\beta)$. If A be a complete bipartite graph, then A must be $K_{n,tn}$. □

Proposition 2.4. *A bipartite graph A is $Gt-EDB$ if and only if*

$$S_{z_e}(A)=t.\frac{(tn+t+1)^2.tn^2}{(t+1)^2}.$$

Proof. Presume that A is $Gt-EDB$. For every edge $f=\alpha\beta$, we have $m_{\alpha}^{A}(f)=tm_{\beta}^{A}(f)$ and since A is bipartite also $m_{\alpha}^{A}(f)+m_{\beta}^{A}(f)+m_{0}^{A}(f)=|E(A)|-1$ holds. Therefore,

$$m_{\alpha}^{A}(f)+m_{\beta}^{A}(f)=|E(A)|-m_{0}^{A}(f)-1.$$

Then,

$$t^2(m_{\beta}^{A}(f))^2+(m_{\beta}^{A}(f))^2+2t(m_{\beta}^{A}(f))^2=(|E(A)|-m_{0}^{A}(f)-1)^2.$$

Hence,

$$(m_{\beta}^{A}(f))^2=\frac{(|E(A)|-m_{0}^{A}(f)-1)^2}{(t+1)^2},$$

and so,

$$\sum_{f\in E(A)}m_{\alpha}^{A}(f).m_{\beta}^{A}(f)=t\sum_{f\in E(A)}(m_{\beta}^{A}(f))^2=$$

$$t.\frac{(|E(A)|-m_{0}^{A}(f)-1)^2.|E(A)|}{(t+1)^2}=t.\frac{(tn+t+1)^2.tn^2}{(t+1)^2}.$$

For converse, let $S_{z_e}(A)=t.\frac{(tn+t+1)^2.tn^2}{(t+1)^2}$. Since A is a graph, we have $m_{\alpha}^{A}(f)+m_{\beta}^{A}(f)+m_{0}^{A}(f)=|E(A)|-1$ and also

$$m_{0}^{A}(f)+(t+1)m_{\beta}^{A}(f)=|E(A)|-1.$$

Hence,

$$m_{\beta}^{A}(f)=\frac{(|E(A)|-m_{0}^{A}(f)-1)}{(t+1)}.$$

As well as

$$m_{\alpha}^{A}(f).m_{\beta}^{A}(f)=t.\frac{(|E(A)|-m_{0}^{A}(f)-1)^2}{(t+1)^2},$$

and hence

$$m_{\alpha}^{A}(f)=tm_{\beta}^{A}(f)=t.\frac{(|E(A)|-m_{0}^{A}(f)-1)}{(t+1)}.$$

This implies that A is $Gt-EDB$. □

3 $Gt-NEDB$ and $Gt-SEDB$ graphs

For every edge $f=\alpha\beta\in E(A)$ in a $Gt-EDB$ graph, $m^A_\alpha(f)=tm^A_\beta(f)$. Consider that for every arbitrary edge $f\in E(A)$, the constant of $m^A_\beta(f)$ is $\acute{\gamma}_A$. Then A is introduced as *Generalized t-nicely edge distance-balanced* ($Gt-NEDB$). Each $Gt-NEDB$ graph is $Gt-EDB$ and every bipartite $Gt-EDB$ graph is $Gt-NEDB$. At first, we start with the below lemma.

Lemma 3.1. *If A be a connected $Gt-NEDB$ graph with diameter of d, then for each arbitrary edge $f=\alpha\beta\in E(A)$, there will precisely be $|E(A)|-(t+1)\acute{\gamma}_A$ edges of A, such that will be at the equal distance from α and β. On the other hand, $m^A_0(f)=|E(A)|-(t+1)\acute{\gamma}_A-1$.*

Proof. It is directly deduced from $m^A_\alpha(f)+m^A_\beta(f)+m^A_0(f)=|E(A)|-1$. □

Proposition 3.2. *Suppose that A is a connected $Gt-NEDB$ graph with diameter d. Then $d-1\leq t\acute{\gamma}_A$.*

Proof. Let a path $a_0,a_1,a_2,...,a_{d-1},a_d$. Also, we have $h_1,h_2,h_3,...,h_d$ as a series of edges, in which $d_A(h_1,h_d)=d$. Now, let $h_1=a_0a_1$ be an arbitrary edge of A. without loss of generality, we assume that $m^A_{a_1}(h_1)=tm^A_{a_0}(h_1)$. Hence, $|\{h_2,...,h_d\}|=d-1\leq m^A_{a_1}(h_1)=tm^A_{a_0}(h_1)$. This shows that $d-1\leq t\acute{\gamma}_A$. □

While for each arbitrary edge $f=\alpha\beta\in E(A)$ and every $i\in[1,d-1]$ in a graph A with diameter d, we have $|\acute{D}^i_{i-1}(f)|=t|\acute{D}^{i-1}_i(f)|+(t-1)$, then such graphs are called $Gt-SEDB$. Let $t=1$. Then graph A is a $SEDB$ graph.

Example 3.3. A class of $Gt-SEDB$ graphs are complete bipartite graphs $K_{n,tn}$.

Proof. Let $f=\alpha\beta\in E(K_{n,tn})$. Since $K_{n,tn}$ is bipartite with diameter 2, we attain $\acute{D}^2_1(f)=(n-1)$ and $\acute{D}^1_2(f)=t(n-1)$. Therefore, $\acute{D}^1_2(f)=t\acute{D}^2_1(f)+(t-1)$ and it completes the result. □

Proposition 3.4. *Consider that A is a $Gt-SEDB$ graph with diameter 2. Then A is a $Gt-EDB$ graph for $t\in\mathbb{N}$ and $t>1$.*

Proof. According to (1), we know that the graph A is $Gt-EDB$ if and only if for each arbitrary edge $f=\alpha\beta\in E(A)$ and each $i\in[1,d-1]$, we have

$$\sum_{i=1}^{d-1}|\acute{D}^{i-1}_i(f)|=t\sum_{i=1}^{d-1}|\acute{D}^i_{i-1}(f)|+(t-1).$$

Let now A be a $Gt-SEDB$ graph. Then for each $f=\alpha\beta\in E(A)$ and each $i\in[1,d-1]$, it is obtained

$$|\acute{D}^{i-1}_i(f)|=t|\acute{D}^i_{i-1}(f)|+(t-1).$$

Thus,

$$\sum_{i=1}^{d-1}|\acute{D}^{i-1}_i(f)|=t\sum_{i=1}^{d-1}|\acute{D}^i_{i-1}(f)|+(t-1)(d-1).$$

If $d=2$, then we obtain

$$|\acute{D}^1_2(f)|=t|\acute{D}^2_1(f)|+(t-1).$$

The proof is completed. □

Pay attention that If $t=1$, then every $SEDB$ graph is EDB

References

[1] A. Abedi, M. Alaeiyan, A. Hujdurović, K. Kutnar, *Quasi-λ-distance-balanced graphs*, Discrete Appl. Math., 227, (2017), pp. 21–28.

[2] Z. Aliannejadi, A. Gilani, M. Alaeiyan, J. Asadpour, *On some properties of edge quasi-distance-balanced graphs*, Journal of Mathematical Extension, 16 (2022), pp. 1–13.

[3] Z. Aliannejadi, M. Alaeiyan, A. Gilani, *Strongly edge distance-balanced graph products*, 7th International Conference on Combinatorics, Cryptography, Computer Science and Computing, (2022).

[4] K. Balakrishman, M. Changat, I. Peterin, S.P. Špacapan, P. Šparal, A. R. Subhamathi, *Strongly distance-balanced graph and graph product*, European. J. Combin., 30 (2009), pp. 1048–1053.

[5] D.M. Cvetkocić, M. Doob, H. Sachs, *Spectra of Graphs-Theory and Application*, Academic Press, New York, (1980).

[6] M. Faghani, A.R. Ashrafi, *Revised and edge revised Szeged indices of graphs*, Ars Math. Contemp., 7 (2014), pp. 153–160.

[7] A. Graovac, M. Juvan, M. Petkovsek, A. Vesel, J. Zerovnik, *The Szeged index of fasciagraphs*, Match Common. Chem., 49 (2003), pp. 47–66.

[8] I. Gutman, L. Popovic, P.V. Khadikar, S. Karmarkar, S. Joshi, M. Mandloi, *Relations between Wiener and Szeged indices of monocyclic molecules*, Match Common. Math. Comput. Chem., 35 (1997), pp. 91–103.

[9] I. Gutman, A.R. Ashrafi, *The edge version of the Szeged index*, Croat. Chem. Acta., 81 (2008), pp. 263–266.

[10] A. Hujdurović, *On some properties of quasi-distance-balanced graphs*, Bull. Aust. Math. Soc., 97 (2018), pp. 177–184.

[11] A. Ilič, S. Klavžar, M. Milanović, *On distance-balanced graphs*, European. J. Combin., 31 (2010), pp. 733–737.

[12] W. Imrich, S. Klavžar, *Product Graphs: Structure and Recognition*, Wiley, New York, USA, (2000).

[13] J. Jerebic, S. Klavžar, D.F. Rall, *Distance-balanced graphs*, Ann. Comb., 12 (2008), pp. 71–79.

[14] M.H. Khalifeh, H. Yousefi-Azari, A.R. Ashrafi, S.G. Wagner, *Some new results on distance-based graph invariants*, European J. Combin., 30 (2009), pp. 1149–1163.

[15] K. Kutnar, A. Malnič, D. Marušič, Š. Miklavič, *Distance-balanced graphs:symmetry conditions*, Discrete Math., 306 (2006), pp. 1881–1894.

[16] K. Kutnar, A. Malnič, D. Marušič, Š. Miklavič, *The strongley distance-balanced property of generalized petersen graphs*, Ars Math. Contemp., 2 (2009), pp. 41–47.

[17] K. Kutnar, Š. Miklavič, *Nicely distance-balanced graphs*, European. j. Combin., 39 (2014), pp. 57–67.

[18] Š. Miklavič, P. Šparl, *On the connectivity of bipartite distance-balanced graphs*, European. J. Combin., 33 (2012), pp. 237–247.

[19] M. Tavakoli, H. Yousefi-azari, A.R. Ashrafi, *Note on Edge Distance-Balanced Graphs*, Transaction on Combinatorics, University of Isfehan, 1 no. 1 (2012), pp. 1–6.

e-mail: z_alian@azad.ac.ir
e-mail: shafiee.s88@gmail.com

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

On the Temperature Indices of Fuzzy Graphs

Mahsa Sadeghi[1]
Mazandaran University, Babolsar, Iran

Ali Asghar Talebi
Mazandaran University, Babolsar, Iran

Abstract

In graph theory, the temperature index is one of the topological graph indices that is mostly used as a physico-chemical descriptor in mathematical modelling of molecular structures. In this paper, while introducing fuzzy temperature indices, these indices were investigated for some fuzzy graphs (FG). our recent findings consists of calculating the bounds for complete FG, paths, stars and cycles in FGs, as well as the Cartesian product, union, join and combination of two FGs.

Keywords: Temperature indices, Fuzzy graph
Mathematics Subject Classification [2010]: 13D45, 39B42

1 Introduction

Fuzzy graph theory is rapidly expanding in many fields, especially chemical-mathematical, due to its unique properties and closeness to the more realistic model. Many topological indices exist only in the crisp state, but are new in the fuzzy graph environment. Fuzzy topological indices are one of the mathematical approaches performed for many technological, engineering and real-world problems such as telecommunications, social networks, traffic light control, maritime, neural networks, Internet routing and wireless sensor network [11]. Graph theory is an attractive field for study in the field of discrete mathematics, and its findings are widely used in many scientific fields [12, 13, 14, 15, 1, 4, 16, 17].

Fuzzy graph is one of the most versatile tools in the field of mathematics, which allows the user to easily describe the fuzzy relationship between any object. With the approach of fuzzy relation, Kauffman presented fuzzy Graph [7]. Various studies have been done on fuzzy graphs. Also, some topological indices have been investigated on fuzzy graphs and their application in mathematical chemistry has been stated [2, 3, 5]. In this article, the limits of the first fuzzy Temperature index for the fuzzy graphs of path, cycle, star, complete graph, Cartesian multiplication, Join graph and the combination and union of two graphs are calculated and relations are expressed.

1.1 Significance and objective of the article

In this paper the Temperature indices is studied for FGs. After giving some preliminary definitions in section2, we investigated some theoretical developments for this index in section 3, with emphasis on calculation of the bounds for several FGs; complete FG, paths, stars and cycles in FGs, also Cartesian product, union, join and composition of two FGs.

[1] speaker

2 Preliminaries

Here some necessary definitions required to develop our results are given as following which most of them can be found in [10]. For any universal set X, with a membership function $\mu : X \to [0,1]$, the pair $S = (X, \mu)$ is named a fuzzy set S.

Definition 2.1. The triple $G = (V, \sigma, \mu)$ consists of a nonempty set V, and two mappings $\mu : V \times V \longrightarrow [0,1]$ and $\sigma : V \longrightarrow [0,1]$ is called a fuzzy graph if

$$\mu(x,y) \leq \sigma(x) \wedge \sigma(y) \text{ for all } x, y \in V.$$

Here μ is symmetry and so, we use symbole xy instead (x,y). Also, $\mu^* = \{uv \in V \times V : \mu(uv) > 0\}$ and $\sigma^* = \{u \in V : \sigma(u) > 0\}$, are deputing the supports of μ and σ respectively, signed by $Supp(\mu)$ and $Supp(\sigma)$.

Definition 2.2. For any fuzzy graph $G = (V, \sigma, \mu)$, a fuzzy graph $H = (P, \tau, \nu)$ is a partial fuzzy subgraph (PFSG) of G if we have:

$$\tau(u) \leq \sigma(u), \text{ for all } u, v \in V,$$
$$\nu(uv) \leq \mu(uv), \text{ for all } u, v \in V.$$

A fuzzy graph $H = (V, \tau, \nu)$ is named a fuzzy subgraph (FSG) of G induced by P, if $P \subseteq V$ and we have:
$\tau(u) = \sigma(u)$ for all $u \in P$ and $\nu(uv) = \mu(uv)$ for all $u, v \in P$.

Definition 2.3. In a fuzzy graph $G = (V, \sigma, \mu)$, Let $\mu^t = \{uv \in E(G) : \mu(uv) \geq t\}$ and $\sigma^t = \{u \in V : \sigma(u) \geq t\}$ for all $0 \leq t \leq 1$. Then $\mu^t \subseteq \{uv : \sigma(u) \geq t, \sigma(v) \geq t\}$. Also $G^t = (V, \sigma^t, \mu^t)$ is a graph, which is named the threshold graph of G, depending on t.

Definition 2.4. A sequence of different vertices $v_1, v_2, \cdots, v_n$ that $\mu(v_i v_{i+1}) > 0; i = 1, ..., n$ is named a path P of the lenth n in a fuzzy graph $G = (V, \sigma, \mu)$ and the successive pairs $(v_i v_{i+1})$ are considered as edges of the path.

Definition 2.5. Let $G = (V, \sigma, \mu)$ be a fuzzy graph, then:

(i) if $(Supp(\sigma), Supp(\mu))$ is a cycle, then G is named a cycle.

(ii) if $\nexists$ unique $uv \in Supp(\mu)$ such that $\mu(uv) = \wedge\{\mu(xy) | xy \in Supp(\mu)\}$,
and $(Supp(\sigma), Supp(\mu))$ is a cycle, then G is named a fuzzy cycle.

Definition 2.6. A fuzzy graph $G = (V, \sigma, \mu)$ is named a complete fuzzy graph (CFG) if $\mu(uv) = \sigma(u) \wedge \sigma(v)$, for all $u, v \in V$.

Definition 2.7. Let G is a graph and v is a vertex of G, The set of vertices adjacent to v is called the neighborhood of v, denoted $N(v)$.

Definition 2.8. For all edges incident at a vertex v in a fuzzy graph G, the sum of their membership values represented by $\sum_{u \in N(v)} \mu(uv)$ is called the degree of v.

Here, δ and Δ represents the minimum and maximum degree of G and $\sigma_{max} = max\{\sigma(u) : u \in V\}$, $\sigma_{min} = min\{\sigma(u) : u \in V\}$ and $\mu_{max} = max\{\mu(uv) : uv \in E(G)\}$, $\mu_{min} = min\{\mu(uv) : uv \in E(G)\}$. Throughout this article, the FG, $G_1 = (V_1, \sigma_1, \mu_1)$ has n_1-vertices, m_1-edges, edge set $E(G_1)$, $\sigma_{max_1} = max\{\sigma_1(u) : u \in V_1\}$, $\sigma_{min_1} = min\{\sigma_1(u) : u \in V\}$ and $G_2 = (V_2, \sigma_2, \mu_2)$ has n_2-vertices, m_2-edges, edge set $E(G_2)$, $\sigma_{max_2} = max\{\sigma_2(u) : u \in V_2\}$, $\sigma_{min_2} = min\{\sigma_2(u) : u \in V_2\}$ and $\Delta_1 = \Delta(G_1), \Delta_2 = \Delta(G_2), \delta_1 = \delta(G_1), \delta_2 = \delta(G_2)$.

Definition 2.9. A regular graph is a graph with all vertices of the same degree.

Definition 2.10. If $G_1 = (V_1, \sigma_1, \mu_1)$, $G_2 = (V_2, \sigma_2, \mu_2)$ are 2 FGs, then $G_1 \times G_2 = (V, \sigma, \mu)$ named the Cartesian product of G_1 and G_2, is an FG too, in which $V = V_1 \times V_2$, $\sigma(u, v) = \wedge\{\sigma_1(u), \sigma_2(v)\}$ for all $(u, v) \in V$ and for every $(u_1, v_1), (u_2, v_2) \in V$ we have

$$\mu((u_1, v_1)(u_2, v_2)) = \begin{cases} \wedge\{\sigma_1(u_1), \mu_2(v_1v_2)\} & if \quad u_1 = u_2, v_1v_2 \in E(G_2) \\ \wedge\{\sigma_2(v_1), \mu_1(u_1u_2)\} & if \quad v_1 = v_2, u_1u_2 \in E(G_1) \\ 0 & otherwise \end{cases}$$

Definition 2.11. If $G_1 = (V_1, \sigma_1, \mu_1)$, $G_2 = (V_2, \sigma_2, \mu_2)$ are 2 FGs, then $G_1[G_2] = (V, \sigma, \mu)$ named the composition of G_1 and G_2, is an FG too, in which $V = V_1 \times V_2$, $\sigma(u, v) = \wedge\{\sigma_1(u), \sigma_2(v)\}$ for all $(u, v) \in V$ and for every $(u_1, v_1), (u_2, v_2) \in V$ we have

$$\mu((u_1, v_1)(u_2, v_2)) = \begin{cases} \wedge\{\sigma_1(u_1), \mu_2(v_1v_2)\} & if \quad u_1 = u_2, v_1v_2 \in E(G_2) \\ \wedge\{\sigma_2(v_1), \sigma_2(v_2), \mu_1(u_1u_2)\} & if \quad u_1u_2 \in E(G_1) \\ 0 & otherwise \end{cases}$$

Definition 2.12. If $G_1 = (V_1, \sigma_1, \mu_1), G_2 = (V_2, \sigma_2, \mu_2)$ are 2 FGs such that $V_1 \cap V_2 = \emptyset$, then $G_1 + G_2 = (V, \sigma, \mu)$ named the join of G_1 and G_2 is a FG too, in which $V = V_1 \cup V_2$, and σ, μ are defined as follow

$$\sigma(u) = \begin{cases} \sigma_1(u) & if \quad u \in V_1 \\ \sigma_2(u) & if \quad u \in V_2 \end{cases} \qquad \forall u \in V.$$

and

$$\mu(u, v) = \begin{cases} \wedge\{\sigma_1(u), \sigma_2(v)\} & if \quad u \in V_1 and\ v \in V_2 \\ \mu_1(uv) & if \quad uv \in E(G_1) \\ \mu_2(uv) & if \quad uv \in E(G_2) \\ 0 & otherwise \end{cases} \qquad \forall u, v \in V.$$

Definition 2.13. Suppose $G_1 = (V_1, \sigma_1, \mu_1)$, $G_2 = (V_2, \sigma_2, \mu_2)$ are 2 FGs, then $G_1 \cup G_2 = (V, \sigma, \mu)$ named the union of G_1 and G_2, is a FG too, in which $V = V_1 \cup V_2$, such that σ, μ are defined as follow

$$\sigma(u) = \begin{cases} \sigma_1(u) & if \quad u \in V_1 \setminus V_2 \\ \sigma_2(u) & if \quad u \in V_2 \setminus V_1 \\ \vee\{\sigma_1(u), \sigma_2(u)\} & if \quad u \in V_1 \cap V_2 \end{cases} \qquad \forall u \in V$$

and

$$\mu(u, v) = \begin{cases} \mu_1(uv) & if \quad uv \in E(G_1) \setminus E(G_2) \\ \mu_2(uv) & if \quad uv \in E(G_2) \setminus E(G_1) \\ \vee\{\mu_1(u, v), \mu_2(u, v)\} & if \quad uv \in E(G_1) \cap E(G_2) \\ 0 & otherwise \end{cases} \qquad \forall u, v \in V.$$

3 The fuzzified Temperature indices

Recently, Temperature indices have been used for studying the crisp graph modelling for molecular structure of Covid19 drugs [6]. In this section we introduce a new definition of Temperature indices for fuzzy graphs, and then we calculate the bounds for first Temperature index; T_1, through proving some theorems, with explicit examples. Other Temperature indices for fuzzy graphs can be obtained simply from the fuzzified form of T_1. But the first we should have a review on the previous definition of Temperature indices for crisp graphs.

Definition 3.1. Let $G = (V, E)$ be a graph. For a vertex $u \in V(G)$, the Temperature degree of u is defined as follows [8]:

$$T_u = \frac{d(u)}{n - d(u)}$$

where n is the number of vertices, $d(u)$ is the degree of u. Using this Temperature degree, the Temperature indices were introduced (see Table 1) [8, 9].

Table 1: Temperature topological indices of G.

Temperature Index name	**Definition**
First Temperature index	$T_1 = \sum_{uv \in E(G)} (T_u + T_v)$
Second Temperature index	$T_2 = \sum_{uv \in E(G)} (T_u.T_v)$
The modified second Temperature index	$MT_2 = \sum_{uv \in E(G)} \frac{1}{T_u.T_v}$
The modified third Temperature index	$MT_3(G) = \sum_{uv \in E(G)} \frac{1}{T_u + T_v}$
First hyper Temperature indices	$HT_1(G) = \sum_{uv \in E(G)} (T_u + T_v)^2$
Second hyper Temperature indices	$HT_2(G) = \sum_{uv \in E(G)} (T_u.T_v)^2$
F-Temperature index	$FT(G) = \sum_{uv \in E(G)} (T_u)^2 + (T_v)^2$
Sum connectivity Temperature index	$ST = \sum_{uv \in E(G)} \frac{1}{\sqrt{T_u + T_v}}$
The Reciprocal product connectivity Temperature index	$RPT = \sum_{uv \in E(G)} \sqrt{T_u.T_v}$
Product connectivity Temperature index	$PT = \sum_{uv \in E(G)} \frac{1}{\sqrt{T_u.T_v}}$

Now we define Temperature indices for a fuzzy graph as follows:

Definition 3.2. For a fuzzy graph $G = (V, \sigma, \mu)$, the Temperature degree of a vertex $u \in V(G)$ is defined as follows:

$$T_u = \frac{d(u)}{n - d(u)} \tag{1}$$

where n is the number of vertices of G.

According to definition 3.2 we can define the Temperature indices for a fuzzy graph as Table 2.

Theorem 3.3. *Let $G = (V, \sigma, \mu)$ be a fuzzy graph with m edges and n vertices. Then we have:*

$$2m\sigma_{min}\frac{\delta}{n - \delta} \leq T_1(G) \leq 2m\sigma_{max}\frac{\Delta}{n - \Delta}.$$

Table 2: Temperature topological indices of FG.

Temperature Index name	**Definition**
First Temperature index	$T_1 = \sum_{uv \in E(G)} (\sigma_u T_u + \sigma_v T_v)$
Second Temperature index	$T_2 = \sum_{uv \in E(G)} (\sigma_u T_u . \sigma_v T_v)$
The modified second Temperature index	$MT_2 = \sum_{uv \in E(G)} \frac{1}{\sigma_u T_u . \sigma_v T_v}$
The modified third Temperature index	$MT_3(G) = \sum_{uv \in E(G)} \frac{1}{\sigma_u T_u + \sigma_v T_v}$
First hyper Temperature indices	$HT_1(G) = \sum_{uv \in E(G)} (\sigma_u T_u + \sigma_v T_v)^2$
Second hyper Temperature indices	$HT_2(G) = \sum_{uv \in E(G)} (\sigma_u T_u . \sigma_v T_v)^2$
F-Temperature index	$FT(G) = \sum_{uv \in E(G)} (\sigma_u T_u)^2 + (\sigma_v T_v)^2$
Sum connectivity Temperature index	$ST = \sum_{uv \in E(G)} \frac{1}{\sqrt{\sigma_u T_u + \sigma_v T_v}}$
The Reciprocal product connectivity Temperature index	$RPT = \sum_{uv \in E(G)} \sqrt{\sigma_u T_u . \sigma_v T_v}$
Product connectivity Temperature index	$PT = \sum_{uv \in E(G)} \frac{1}{\sqrt{\sigma_u T_u . \sigma_v T_v}}$

Proof. According to relation (1), we have

$$T_u = \frac{d(u)}{n - d(u)} \leq \frac{\Delta}{n - \Delta}. \tag{2}$$

Therefore

$$T_1 = \sum_{uv \in E(G)} (\sigma(u) T_u + \sigma(v) T_v) \leq 2m\sigma_{max} \frac{\Delta}{n - \Delta}.$$

Similarly $T_1 \geq 2m\sigma_{min} \frac{\delta}{n - \delta}$ □

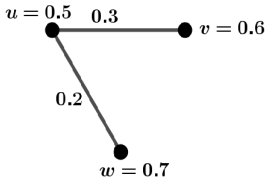


Figure 1: A fuzzy graph

Example 3.4. Suppose G is the FG shown in Figure 1. Then we have the Temperature degree of vertices as Table 3.

Therefore for $T_1(G)$, we have:

1. $T_1(G) = \sum_{uv \in E(G)} (\sigma(u) T_u + \sigma(v) T_v) = (0.5 \times 0.2 + 0.6 \times 0.11) + (0.7 \times 0.07 + 0.5 \times 0.2) = 0.315$

2. $2m\sigma_{max} \frac{\Delta}{n - \Delta} = 2 \times 2 \times 0.7 \times \frac{0.5}{3 - 0.5} \simeq 0.56$

Table 3: Temperature degree of vertices.

vertex	Temperature degree
u	$T_u = \frac{0.5}{3-0.5} = 0.2$
v	$T_v = \frac{0.3}{3-0.3} = 0.11$
w	$T_w = \frac{0.2}{3-0.2} = 0.07$

3. $2m\sigma_{min}\frac{\delta}{n-\delta} = 2 \times 2 \times 0.5 \times \frac{0.2}{3-0.2} \simeq 0.14.$

Clearly $0.14 \leq T_1(G) \leq 0.56$.

Theorem 3.5. *For a fuzzy path $P = (\sigma, \mu) : (v_1, v_2, \cdots, v_n)$, we have:*

$$T_1(P) \leq \sigma_{max}(\frac{2\mu_{max}}{n-\mu_{max}} + \frac{(4n-8)\mu_{max}}{n-2\mu_{max}}).$$

Proof. As P is a path, $d(v_1) = \mu_1$, $d(v_n) = \mu_{n-1}$ and $d(v_i) = \mu_{i-1} + \mu_i$ for $i = 2, 3, ..., n-1$, where $\sigma(v_i) = \sigma_i$ and $\mu(v_i v_{i+1}) = \mu_i$ for $i = 1, 2, 3, ..., n$. Therefore

$$\begin{aligned}
T_1(P) =& (\sigma_1\frac{\mu_1}{n-\mu_1} + \sigma_2\frac{\mu_1+\mu_2}{n-(\mu_1+\mu_2)}) + \sum_{i=2}^{n-2}(\sigma_i\frac{\mu_{i-1}+\mu_i}{n-(\mu_{i-1}+\mu_i)}) + (\sigma_{i+1}\frac{\mu_i+\mu_{i+1}}{n-(\mu_i+\mu_{i+1})}) \\
&+(\sigma_{n-1}\frac{\mu_{n-2}+\mu_{n-1}}{n-(\mu_{n-2}+\mu_{n-1})} + \sigma_n\frac{\mu_{n-1}}{n-\mu_{n-1}}) \\
\leq& 2\sigma_{max}\frac{\mu_{max}}{n-\mu_{max}} + 2\sigma_{max}\frac{2\mu_{max}}{n-2\mu_{max}} + 2(n-3)(\sigma_{max}\frac{2\mu_{max}}{n-2\mu_{max}}) \\
=& \sigma_{max}(\frac{2\mu_{max}}{n-\mu_{max}} + \frac{(4n-8)\mu_{max}}{n-2\mu_{max}}).
\end{aligned}$$

□

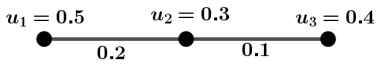


Figure 2: A fuzzy path

Example 3.6. Suppose G is the fuzzy path shown in Figure 2. Then we have Temperature degree of vertices as Table 4.

Table 4: Temperature degree of vertices.

vertex	Temperature degree
u_1	$T_{u_1} = \frac{0.2}{3-0.2} = 0.071$
u_2	$T_{u_2} = \frac{0.3}{3-0.3} = 0.11$
u_3	$T_{u_3} = \frac{0.1}{3-0.1} = 0.034$

Therefore for $T_1(G)$, we have:

1. $T_1(G) = \sum_{uv \in E(G)} (\sigma(u)T_u + \sigma(v)T_v) = (0.5 \times 0.071 + 0.3 \times 0.11) + (0.3 \times 0.11 + 0.4 \times 0.034) = 0.1151$

2. $\sigma_{max}(\frac{2\mu_{max}}{n - \mu_{max}} + \frac{(4n-8)\mu_{max}}{n - 2\mu_{max}}) = 0.5 \times (\frac{2\times 0.2}{3-0.2} + \frac{4\times 0.2}{3-0.4}) = 0.225.$

Clearly $T_1(G) \leq 0.225$.

Theorem 3.7. *For a fuzzy cycle $C = (\sigma, \mu) : (v_1, v_2, \cdots, v_n)$, we have $T_1(C) \leq \frac{4n\sigma_{max}\mu_{max}}{n - 2\mu_{max}}$.*

Proof. As $C(v_1, v_2, \cdots, v_n)$ is a cycle, then $d(v_1) = \mu_1 + \mu_n$ and $d(v_i) = \mu_{i-1} + \mu_i$ for $i = 2, 3, ..., n$, where $\sigma(v_i) = \sigma_i$ and $\mu(v_i v_{i+1}) = \mu_i$ for $i = 1, 2, 3, ..., n$. Therefore

$$\begin{aligned}
T_1(C) =& (\sigma_1 \frac{\mu_1 + \mu_n}{n - (\mu_1 + \mu_n)} + \sigma_2 \frac{\mu_1 + \mu_2}{n - (\mu_1 + \mu_2)}) + \sum_{i=2}^{n-1} (\sigma_i \frac{\mu_{i-1} + \mu_{i+1}}{n - (\mu_{i-1} + \mu_i)} + \sigma_{i+1} \frac{\mu_i + \mu_{i+1}}{n - (\mu_i + \mu_{i+1})}) \\
&+ (\sigma_n \frac{\mu_{n-1} + \mu_n}{n - (\mu_{n-1} + \mu_n)} + \sigma_1 \frac{\mu_1 + \mu_n}{n - (\mu_1 + \mu_n)}) \\
\leq& 4\sigma_{max} \frac{2\mu_{max}}{n - 2\mu_{max}} + 2(n-2)\sigma_{max} \frac{2\mu_{max}}{n - 2\mu_{max}} \\
=& \frac{4n\sigma_{max}\mu_{max}}{n - 2\mu_{max}}.
\end{aligned}$$

□

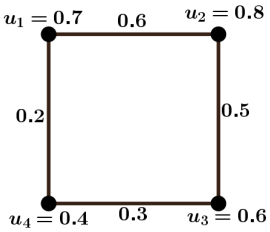


Figure 3: A fuzzy cycle

Example 3.8. Suppose G is the fuzzy cycle shown in Figure 3. Then we have the Temperature degree of vertices as Table 5.

Table 5: Temperature degree of vertices.

vertex	**Temperature degree**
u_1	$T_{u_1} = \frac{0.8}{4 - 0.8} = 0.25$
u_2	$T_{u_2} = \frac{1.1}{4 - 1.1} = 0.38$
u_3	$T_{u_3} = \frac{0.8}{4 - 0.8} = 0.25$
u_4	$T_{u_4} = \frac{0.5}{4 - 0.5} = 0.14$

Therefore for $T_1(G)$, we have:

1. $T_1(G) = (0.7\times 0.25 + 0.8\times 0.38) + (0.8\times 0.38 + 0.6\times 0.14) + (0.6\times 0.14 + 0.4\times 0.25) + (0.4\times 0.25 + 0.7\times 0.25) = 1.326$

2. $\frac{4n\sigma_{max}\mu_{max}}{n-2\mu_{max}} = 4 \times 4 \times 0.8 \times \frac{0.6}{4-1.2} \simeq 2.743.$

Clearly $T_1(G) \leq 2.743$.

Theorem 3.9. *Let $S = (\sigma, \mu)$ be a fuzzy star with vertex set $V = \{v_0, v_1, ..., v_n\}$ where v_0 is the center of S. Then $T_1(S) \leq n\sigma_{max}\mu_{max}(\frac{1}{1-\mu_{max}} + \frac{1}{n-\mu_{max}})$.*

Proof. Since $S(\sigma, \mu)$ is a star, then $d(v_0) = \mu_1 + \cdots + \mu_n$, and $d(v_i) = \mu_i$ for $i = 1, 2, ..., n$, where $\sigma(v_i) = \sigma_i, i = 0, \cdots, n$ and $\mu(v_0, v_i) = \mu_i$ for $i = 1, 2, 3, ..., n$. Therefore

$$\begin{aligned} T_1(S) =& \sum_{i=1}^{n}(\sigma_0 \frac{\sum\limits_{j=1}^{n}\mu_j}{n - \sum\limits_{j=1}^{n}\mu_j} + \sigma_i \frac{\mu_i}{n-\mu_i}) \\ \leq& n(\sigma_{max}\frac{(n)\mu_{max}}{n-n\mu_{max})} + \sigma_{max}\frac{\mu_{max}}{n-\mu_{max}}) \\ =& n\sigma_{max}\mu_{max}(\frac{1}{1-\mu_{max}} + \frac{1}{n-\mu_{max}}) \end{aligned}$$

□

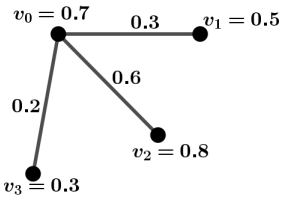


Figure 4: A fuzzy star

Example 3.10. Suppose G is the fuzzy star shown in Figure 4. Then we have the Temperature degree of vertices as Table 6.

Table 6: Temperature degree of vertices.

vertex	**Temperature degree**
v_0	$T_{v_0} = \frac{1.1}{4-1.1} = 0.38$
v_1	$T_{v_1} = \frac{0.3}{4-0.3} = 0.08$
v_2	$T_{v_2} = \frac{0.6}{4-0.6} = 0.18$
v_3	$T_{v_3} = \frac{0.2}{4-0.2} = 0.05$

Therefore for $T_1(G)$, we have:

1. $T_1(G) = (0.7 \times 0.38 + 0.5 \times 0.08) + (0.7 \times 0.38 + 0.8 \times 0.18) + (0.7 \times 0.38 + 0.3 \times 0.05) = 1.021$
2. $n\sigma_{max}\mu_{max}(\frac{1}{1-\mu_{max}} + \frac{1}{n-\mu_{max}}) = 4 \times 0.8 \times 0.6 \times (\frac{1}{1-0.6} + \frac{1}{4-0.6}) \simeq 5.376.$

Clearly $T_1(G) \leq 5.376$.

Theorem 3.11. *Let $G = (V, \sigma, \mu)$ be a complete fuzzy graph with vertex set $V = \{v_1, \cdots, v_n\}$ such that $\sigma_1 \leq \sigma_2 \leq \cdots \leq \sigma_n$, in which $\sigma(v_i) = \sigma_i$ for $i = 1, 2, 3, ..., n$. Then $T_1(G) = n(n-1)\sum_{i=1}^{n} \sigma_i \frac{(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t}{n - [(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t]}$.*

Proof. As G is a CFG, then $d(v_i) = (n-i)\sigma_i + \sum_{j=1}^{i-1} \sigma_j$. Therefore

$$\begin{aligned} T_1(G) = &\sum_{1 \leq i \leq j \leq n} (\sigma_i \frac{(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t}{n - [(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t]} + \sigma_j \frac{(n-j)\sigma_j + \sum_{t=1}^{j-1} \sigma_t}{n - [(n-j)\sigma_j + \sum_{t=1}^{j-1} \sigma_t]}) \\ =&n(n-1)\sum_{i=1}^{n} \sigma_i \frac{(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t}{n - [(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t]}. \end{aligned}$$

□

Corollary 3.12. *Let $G = (V, \sigma, \mu)$ be a complete fuzzy graph with vertex set $V = \{v_1, \cdots, v_n\}$ such that $\sigma_1 \leq \sigma_2 \leq \cdots \leq \sigma_n$, in which $\sigma(v_i) = \sigma_i$ for $i = 1, 2, 3, ..., n$. Then $T_1(G) \leq n(n-1)^2(\frac{\sigma_n^2}{n - (n-1)\sigma_n})$.*

Proof. As G is a CFG, then $d(v_i) = (n-i)\sigma_i + \sum_{j=1}^{i-1} \sigma_j$. Therefore

$$\begin{aligned} T_1(G) = &\sum_{1 \leq i \leq j \leq n} (\sigma_i \frac{(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t}{n - [(n-i)\sigma_i + \sum_{t=1}^{i-1} \sigma_t]} + \sigma_j \frac{(n-j)\sigma_j + \sum_{t=1}^{j-1} \sigma_t}{n - [(n-j)\sigma_j + \sum_{t=1}^{j-1} \sigma_t]}) \\ \leq &\frac{n(n-1)}{2}[\sigma_n \frac{(n-i)\sigma_n + (i-1)\sigma_n}{n - [(n-i)\sigma_n + (i-1)\sigma_n]} + \sigma_n \frac{(n-j)\sigma_n + (j-1)\sigma_n}{n - (n-1)\sigma_n}] \\ = &\frac{n(n-1)}{2}(2\sigma_n^2 \frac{n-1}{n - (n-1)\sigma_n}) = n(n-1)^2 \frac{\sigma_n^2}{n - (n-1)\sigma_n}. \end{aligned}$$

□

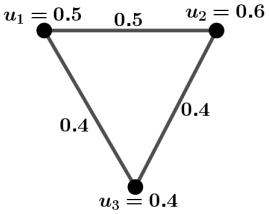


Figure 5: A complete fuzzy graph

Table 7: Temperature degree of vertices.

vertex	Temperature degree
u_1	$T_{u_1} = \frac{0.9}{3-0.9} = 0.43$
u_2	$T_{u_2} = \frac{0.9}{3-0.9} = 0.43$
u_3	$T_{u_3} = \frac{0.8}{3-0.8} = 0.36$

Example 3.13. Suppose G is the complete fuzzy graph shown in Figure 5. Then we have the Temperature degree of vertices as Table 7.

Therefore for $T_1(G)$, we have:

1. $T_1(G) = (0.5 \times 0.43 + 0.6 \times 0.43) + (0.6 \times 0.43 + 0.4 \times 0.36) + (0.4 \times 0.36 + 0.5 \times 0.43) = 1.234$,
2. $n(n - 1^2(\frac{\sigma_n^2}{n-(n-1)\sigma_n}) = 3 \times 4 \times (\frac{(0.6)^2}{3-2\times 0.6}) = 2.4$.

Clearly $T_1(G) \leq 2.4$.

Theorem 3.14. *For two fuzzy graphs $G_1 = (V_1, \sigma_1, \mu_1)$, $G_2 = (V_2, \sigma_2, \mu_2)$ and their Cartesian product $G = G_1 \times G_2 = (V, \sigma, \mu)$, such that G_i have n_i vertices and m_i edges for $i = 1, 2$, we have*

$$T_1(G_1 \times G_2) \leq (2m_1n_2 + 2m_2n_1)[\frac{\Delta}{n-\Delta}(\wedge\{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\})].$$

Proof. Using the definition of the Cartesian product of G_1 and G_2 we have:

$\sigma(u, v) = \wedge\{\sigma_1(u), \sigma_2(v)\}, \forall (u, v) \in V$,

$\mu((u_1, v_1)(u_2, v_2)) = \begin{cases} \wedge\{\sigma_1(u_1), \mu_2(v_1v_2)\} & if \quad u_1 = u_2, v_1v_2 \in E(G_2) \\ \wedge\{\sigma_2(v_1), \mu_1(u_1u_2)\} & if \quad v_1 = v_2, u_1u_2 \in E(G_1) \\ 0 & otherwise \end{cases}$, $\forall (u_1, v_1), (u_2, v_2) \in V$. Then

$$\begin{aligned} d_{G_1\times G_2}(u, v) &= \sum_{vv_i \in E(G_2)} \mu((u, v)(u, v_i)) + \sum_{uu_i \in E(G_1)} \mu((u, v)(u_i, v)) \\ &= \sum_{vv_i \in E(G_2)} \wedge\{\sigma_1(u), \mu_2(vv_i)\} + \sum_{uu_i \in E(G_1)} \wedge\{\sigma_2(v), \mu_1(uu_i)\} \\ &\leq \sum_{vv_i \in E(G_2)} \mu_2(vv_i) + \sum_{uu_i \in E(G_1)} \mu_1(uu_i) = d_{G_1}(u) + d_{G_2}(v) \end{aligned}$$

Now first Temperature index of $G_1 \times G_2$ is:

$$\begin{aligned} T_1(G_1 \times G_2) = &\sum_{u_1u_2 \in E_1, v_1 \in V_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_2, v_1)T_{(u_2,v_1)}) \\ &+ \sum_{u_1 \in V_1, v_1v_2 \in E_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_1, v_2)T_{(u_1,v_2)}) \\ &= K_1 + K_2 \end{aligned}$$

where $K_1 = \sum_{u_1u_2 \in E_1, v_1 \in V_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_2, v_1)T_{(u_2,v_1)})$ and

$K_2 = \sum_{u_1 \in V_1, v_1 v_2 \in E_2} (\sigma(u_1, v_1) T_{(u_1,v_1)} + \sigma(u_1, v_2) T_{(u_1,v_2)})$. Now

$$\begin{aligned} K_1 &\leq \sum_{u_1 u_2 \in E_1, v \in V_2} (\wedge\{\sigma_1(u_1), \sigma_2(v_1)\} T_{(u_1,v_1)} + \wedge\{\sigma_1(u_2), \sigma_2(v_1)\} T_{(u_2,v_1)} \\ &\leq \sum_{u_1 u_2 \in E_1, v \in V_2} (\wedge\{\sigma_{1max}(u_1), \sigma_{2max}(v_1)\} T_{(u_1,v_1)} + \wedge\{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\} T_{(u_2,v_1)} \\ &= \wedge \{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\} \sum_{u_1 u_2 \in E_1, v \in V_2} (T_{(u_1,v_1)} + T_{(u_2,v_1)}) \\ &\leq 2 m_1 n_2 \frac{\Delta}{n - \Delta} (\wedge\{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\}) \end{aligned}$$

Similarly we can get $K_2 \leq 2 m_2 n_1 (\wedge\{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\})(\frac{\Delta}{n - \Delta})$. Therefore

$T_1(G_1 \times G_2) \leq (2 m_1 n_2 + 2 m_2 n_1)[\frac{\Delta}{n - \Delta} (\wedge\{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\})]$. □

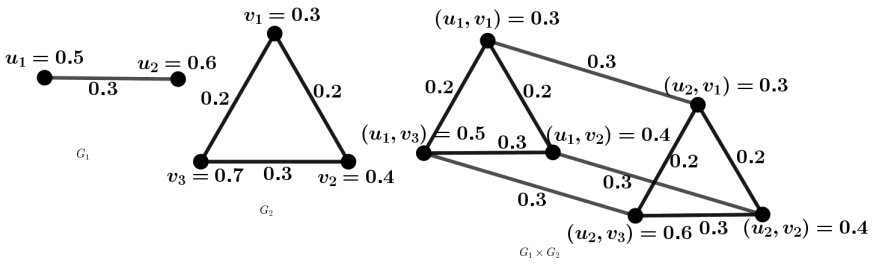


Figure 6: The cartesian product of fuzzy graph's G_1 and G_2

Example 3.15. Suppose $G_1 \times G_2$ is the fuzzy graph shown in Figure 6. Then we have the Temperature degree of vertices as Table 8.

Table 8: Temperature degree of vertices.

vertex	Temperature degree
(u_1, v_1)	$T_{(u_1,v_1)} = \frac{0.7}{6 - 0.7} = 0.13$
(u_1, v_2)	$T_{(u_1,v_2)} = \frac{0.8}{6 - 0.8} = 0.15$
(u_1, v_3)	$T_{(u_1,v_3)} = \frac{0.8}{6 - 0.8} = 0.15$
(u_2, v_1)	$T_{(u_2,v_1)} = \frac{0.7}{6 - 0.7} = 0.13$
(u_2, v_2)	$T_{(u_2,v_2)} = \frac{0.7}{6 - 0.7} = 0.13$
(u_2, v_3)	$T_{(u_2,v_3)} = \frac{0.8}{6 - 0.8} = 0.15$

Therefore for $T_1(G_1 \times G_2)$, we have:

1. $T_1(G_1 \times G_2) = (0.3 \times 0.13 + 0.3 \times 0.13) + (0.3 \times 0.13 + 0.4 \times 0.15) + (0.4 times 0.15 + 0.5 \times 0.15) + (0.5 \times 0.15 + 0.3 \times 0.13) + (0.5 \times 0.15 \times 0.6 \times 0.15) + (0.4 \times 0.15 + 0.4 \times 0.13) + (0.3 \times 0.13 + 0.4 \times 0.13) + (0.4 \times 0.13 + 0.6 \times 0.15) + (0.6 \times 0.15 + 0.3 \times 0.13) = 1.065$
2. $(2 m_1 n_1 + 2 m_2 n_1)[\frac{\Delta}{n - \Delta} (\wedge\{\sigma_{1max}(u_2), \sigma_{2max}(v_1)\})] = 1.6.$

Clearly $T_1(G_1 \times G_2) \leq 1.6$.

Theorem 3.16. *Let $G_1[G_2] = (V, \sigma, \mu)$ be the composition of G_1 and G_2. Then*

$$T_1(G_1[G_2]) \leq 2(m_2n_1 + m_1n_2)(\sigma_{1max} + \sigma_{2max})(\frac{\Delta}{n - \Delta}).$$

Proof. As $G_1[G_2] = (V, \sigma, \mu)$ is the composition of $G_1 = (V_1, \sigma_1, \mu_1)$ and $G_2 = (V_2, \sigma_2, \mu_2)$ where $V = V_1 \times V_2$ and $\sigma(u, v) = \wedge\{\sigma_1(u), \sigma_2(v)\}, \forall (u, v) \in V$,

$$\mu((u_1, v_1)(u_2, v_2)) = \begin{cases} \wedge\{\sigma_1(u_1), \mu_2(v_1v_2)\} & if \quad u_1 = u_2, v_1v_2 \in E(G_2) \\ \wedge\{\sigma_2(v_1), \sigma_2(v_2), \mu_1(u_1u_2)\} & if \quad u_1u_2 \in E(G_1) \\ 0 & otherwise \end{cases} \qquad \forall (u_1, v_1), (u_2, v_2) \in V,$$

we have

$$\begin{aligned} d_{G_1[G_2]}(u, v) &= \sum_{v_iv \in E(G_2)} \mu((u, v)(u_1, v_1)) + \sum_{u_iu \in E(G_1), v_j \in V_2} \mu((u, v)(u_i, v_j) \\ &= \sum_{v_iv \in E(G_2)} \wedge\{\sigma_1(u), \mu_2(vv_i)\} + \sum_{u_iu \in E(G_1), v_j \in V_2} \wedge\{\sigma_2(v), \sigma_2(v_j), \mu_1(uu_i)\} \\ &\leq \sum_{v_iv \in E(G_2)} \mu_2(vv_i) + \sum_{u_iu \in E(G_1), v_j \in V_2} \mu_1(uu_i) \\ &= n_2 d_{G_1}(u) + d_{G_2}(v). \end{aligned}$$

Hence

$$\begin{aligned} T_1(G_1[G_2]) &= \sum_{u_1 \in V_1, v_1v_2 \in E_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_1, v_2)T_{(u_1,v_2)}) \\ &\quad + \sum_{u_1u_2 \in E_1, v_1, v_2 \in V_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_2, v_2)T_{(u_2,v_2)}) \\ &= K_1 + K_2, \end{aligned}$$

where $K_1 = \sum_{u_1 \in V_1, v_1v_2 \in E_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_1, v_2)T_{(u_1,v_2)})$ and

$K_2 = \sum_{u_1u_2 \in E_1, v_1, v_2 \in V_2} (\sigma(u_1, v_1)T_{(u_1,v_1)} + \sigma(u_2, v_2)T_{(u_2,v_2)})$.

Now we get

$$\begin{aligned} K_1 &\leq \sum_{u_1 \in V_1, v_1v_2 \in E_2} (\wedge\{\sigma_1(u_1), \sigma_2(v_1)\}T_{(u_1,v_1)} + \wedge\{\sigma_1(u_1), \sigma_2(v_2)\}T_{(u_1,v_2)}) \\ &\leq \sum_{u_1 \in V_1, v_1v_2 \in E_2} (2\sigma_{1max} \times \frac{\Delta}{n - \Delta} + 2\sigma_{2max} \times \frac{\Delta}{n - \Delta}) \\ &= 2m_1n_2(\sigma_{1max} + \sigma_{2max}) \times \frac{\Delta}{n - \Delta}. \end{aligned}$$

Similarly we can get $K_2 \leq 2m_2n_1(\sigma_{1max} + \sigma_{2max}) \times \frac{\Delta}{n - \Delta}$. Therefore,

$$T_1(G_1[G_2]) \leq 2(m_2n_1 + m_1n_2)(\sigma_{1max} + \sigma_{2max})(\frac{\Delta}{n - \Delta}).$$

□

Example 3.17. Suppose $G_1[G_2]$ is the fuzzy graph shown in Figure 7.Then we have the Temperature degree of vertices as Table 9.

Therefore for $T_1(G_1[G_2])$, we have:

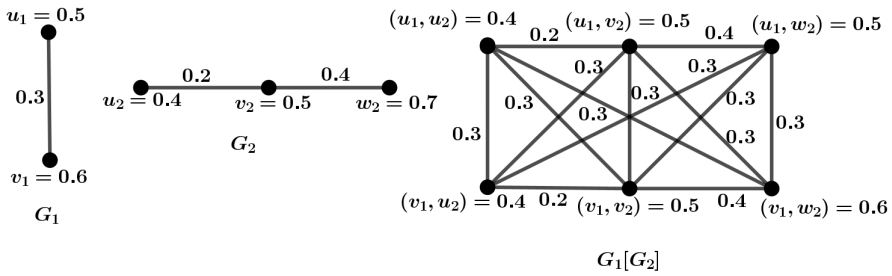


Figure 7: The composition of fuzzy graph's G_1 and G_2

Table 9: Temperature degree of vertices.

vertex	**Temperature degree**
(u_1, u_2)	$T_{(u_1,u_2)} = \frac{1.1}{6-1.1} = 0.22$
(u_1, v_2)	$T_{(u_1,v_2)} = \frac{1.5}{6-1.5} = 0.33$
(v_1, v_2)	$T_{(u_1,v_2)} = \frac{1.5}{6-1.5} = 0.33$
(u_1, w_2)	$T_{(u_1,w_2)} = \frac{1.3}{6-1.3} = 0.28$
(v_1, u_2)	$T_{(v_1,u_2)} = \frac{1.1}{6-1.1} = 0.22$
(v_1, w_2)	$T_{(v_1,w_2)} = \frac{1.3}{6-1.3} = 0.28$

1. $T_1(G_1[G_2]) = (0.4 \times 0.22 + 0.5 \times 0.28) + (0.4 \times 0.22 + 0.6 \times 0.28) + (0.4 \times 0.22 + 0.5 \times 0.33) + (0.4 \times 0.22 + 0.4 \times 0.22) + (0.5 \times 0.33 + 0.5 \times 0.28) + (0.5 \times 0.33 + 0.6 \times 0.28) + (0.5 \times 0.33 + 0.5 \times 0.33) + (0.5 \times 0.33 + 0.4 \times 0.22) + (0.5 \times 0.28 + 0.6 \times 0.28) + (0.5 \times 0.28 + 0.5 \times 0.33) + (0.5 \times 0.28 + 0.4 \times 0.22) + (0.6 \times 0.28 + 0.5 \times 0.33) + (0.5 \times 0.33 + 0.4 \times 0.22) = 3.561$

2. $2(m_2n_1 + m_1n_2)(\sigma_{1max} + \sigma_{2max})(\frac{\Delta}{n-\Delta}) = 6.006.$

Clearly $T_1(G_1[G_2]) \leq 6.006$.

Theorem 3.18. *If $G_1 + G_2 = (V, \sigma, \mu)$ is the join of $G_1 = (V_1, \sigma_1, \mu_1)$ and $G_2 = (V_2, \sigma_2, \mu_2)$, we have*

$$T_1(G_1 + G_2) \leq 2(m_1 + m_2 + n_1n_2)\sigma_{max}\frac{\Delta}{n-\Delta}$$

Proof. As $G_1 + G_2 = (V, \sigma, \mu)$ is the join of G_1 and G_2 then for $u, v \in V$

$$\sigma(u) = \begin{cases} \sigma_1(u) & if \quad u \in V_1 \\ \sigma_2(u) & if \quad u \in V_2 \end{cases}$$

and

$$\mu(uv) = \begin{cases} \wedge\{\sigma_1(u), \sigma_2(v)\} & if \quad u \in V_1 and\ v \in V_2 \\ \mu_1(uv) & if \quad uv \in E(G_1) \\ \mu_2(uv) & if \quad uv \in E(G_2) \\ 0 & otherwise \end{cases}.$$

Hence

$$d_{G_1+G_2}(u) = \begin{cases} d_{G_1}(u) + \sum\limits_{v\in V_2} \wedge\{\sigma_1(u), \sigma_2(v)\} & u \in V_1 \\ d_{G_2}(u) + \sum\limits_{v\in V_1} \wedge\{\sigma_1(u), \sigma_2(v)\} & u \in V_2 \end{cases}$$
$$\leq \begin{cases} d_{G_1}(u) + \sum\limits_{v\in V_2} \sigma_1(u) & u \in V_1 \\ d_{G_2}(u) + \sum\limits_{v\in V_1} \sigma_2(u) & u \in V_2 \end{cases}$$
$$\leq \begin{cases} d_{G_1}(u) + n_2\sigma_1(u) & u \in V_1 \\ d_{G_2}(u) + n_1\sigma_2(u) & u \in V_2 \\ . \end{cases}$$

Then

$$T_1(G_1 + G_2) = \sum_{uv\in E_1} (\sigma_1(u_1)T_{u_1v_1} + \sigma_2(v_1)T_{u_1v_1}) + \sum_{uv\in E_2} (\sigma_1(u_2)T_{u_2v_2} + \sigma_2(v_2)T_{u_2v_2})$$
$$+ \sum_{u\in V_1, v\in V_2} (\sigma_1(u)T_{uv} + \sigma_2(v)T_{uv}) = K_1 + K_2 + K_3,$$

where $K_1 = \sum\limits_{uv\in E_1} (\sigma_1(u_1)T_{u_1v_1} + \sigma_2(v_1)T_{u_1v_1})$, $K_2 = \sum\limits_{uv\in E_2} (\sigma_1(u_2)T_{u_2v_2} + \sigma_2(v_2)T_{u_2v_2})$ and $K_3 = \sum\limits_{u\in V_1, v\in V_2} (\sigma_1(u)T_{uv} + \sigma_2(v)T_{uv})$. Now

$$K_1 \leq m_1(2\sigma_{max} \times \frac{\Delta}{n-\Delta}) = 2m_1\sigma_{max}\frac{\Delta}{n-\Delta}$$

Similarly $K_2 \leq 2m_2\sigma_{max}\frac{\Delta}{n-\Delta}$ and $K_3 \leq 2n_1n_2(\sigma_{max}\frac{\Delta}{n-\Delta})$. Therefore

$$T_1(G_1 + G_2) \leq 2(m_1 + m_2 + n_1n_2)\sigma_{max}(\frac{\Delta}{n-\Delta})$$

□

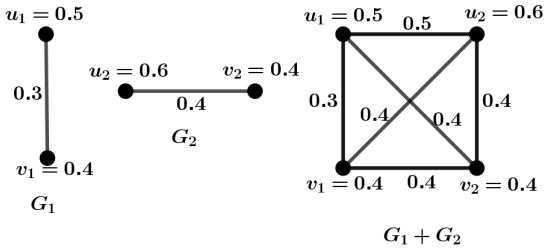


Figure 8: The join of fuzzy graph's G_1 and G_2

Example 3.19. Suppose $G_1 + G_2$ is the fuzzy graph shown in Figure 8. Then we have the Temperature degree of vertices as Table 10.

Therefore for $T_1(G_1 + G_2)$, we have:

1. $T_1(G_1 + G_2) = (0.5 \times 0.43 + 0.6 \times 0.48) + (0.5 \times 0.43 + 0.4 \times 0.43) + (0.5 \times 0.43 + 0.4 \times 0.38) + (0.6 \times 0.48 + 0.4 \times 0.43) + (0.6 \times 0.48 + 0.4 \times 0.38) + (0.4 \times 0.43 + 0.4 \times 0.38) = 2.481$

2. $2(m_1 + m_2 + n_1n_2)\sigma_{max}(\frac{\Delta}{n-\Delta}) = 3.456.$

Table 10: Temperature degree of vertices.

vertex	Temperature degree
u_1	$T_{u_1} = \frac{1.2}{4-1.2} = 0.43$
u_2	$T_{u_2} = \frac{1.3}{4-1.3} = 0.48$
v_1	$T_{v_1} = \frac{1.1}{4-1.1} = 0.38$
v_2	$T_{v_2} = \frac{1.2}{4-1.2} = 0.43$

Clearly $T_1(G_1 + G_2) \leq 3.456$.

Theorem 3.20. *Let $G_1 \cup G_2 = (V, \sigma, \mu)$ be the union of $G_1 = (V_1, \sigma_1, \mu_1)$ and $G_2 = (V_2, \sigma_2, \mu_2)$. Then $T_1(G_1 \cup G_2) \leq 2(m_1 + m_2 - k)(\sigma_{max}\frac{\Delta}{n-\Delta})$ where $k = \mid E(G_1) \cap E(G_2) \mid$ and $\Delta = max\{\Delta_1, \Delta_2\}$.*

Proof. As $G_1 \cup G_2 = (V, \sigma, \mu)$ is the union of G_1 and G_2

$$\sigma(u) = \begin{cases} \sigma_1(u) & if \quad u \in V_1 \setminus V_2 \\ \sigma_2(u) & if \quad u \in V_2 \setminus V_1 \\ \vee\{\sigma_1(u), \sigma_2(u)\} & if \quad u \in V_1 \cap V_2 \end{cases}$$

and

$$\mu(u,v) = \begin{cases} \mu_1(uv) & if \quad uv \in E(G_1) \setminus E(G_2) \\ \mu_2(uv) & if \quad uv \in E(G_2) \setminus E(G_1) \\ \vee\{\mu_1(u,v), \mu_2(u,v)\} & if \quad uv \in E(G_1) \cap E(G_2) \\ 0 & otherwise \end{cases}.$$

Then

$$\begin{aligned} T_1(G_1 \cup G_2) &= \sum_{uv \in E(G_1 \cup G_2)} (\sigma(u)T_u + \sigma(v)T_v) \\ &\leq \sum_{uv \in E(G_1) \setminus E(G_2)} (2\sigma_{max}\frac{\Delta}{n-\Delta}) + \sum_{uv \in E(G_2) \setminus E(G_1)} (2\sigma_{max}\frac{\Delta}{n-\Delta}) \\ &- \sum_{uv \in E(G_1) \cap E(G_2)} (2\sigma_{max}\frac{\Delta}{n-\Delta}) = 2(m_1 + m_2 - k)(\sigma_{max}\frac{\Delta}{n-\Delta}). \end{aligned}$$

□

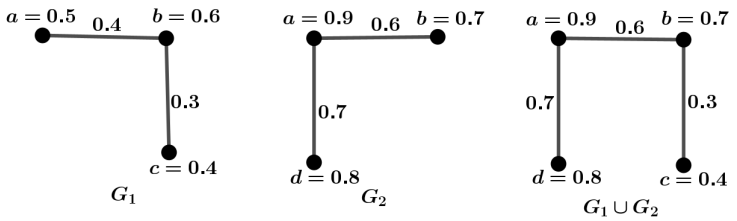


Figure 9: The union of fuzzy graph's G_1 and G_2

Table 11: Temperature degree of vertices.

vertex	Temperature degree
a	$T_a = \frac{1.3}{4-1.3} = 0.48$
b	$T_b = \frac{0.9}{4-0.9} = 0.29$
c	$T_c = \frac{0.3}{4-0.3} = 0.08$
d	$T_d = \frac{0.7}{4-0.7} = 0.21$

Example 3.21. Suppose $G_1 \cup G_2$ is the fuzzy graph shown in Figure 9. Then we have the Temperature degree of vertices as Table 11.

Therefore for $T_1(G_1 \cup G_2)$, we have:

1. $T_1(G_1 \cup G_2) = (0.9 \times 0.48 + 0.7 \times 0.29) + (0.7 \times 0.29 + 0.4 \times 0.08) + (0.9 \times 0.48 + 0.8 \times 0.21) = 1.47$
2. $2(m_1 + m_2 - k)(\sigma_{max}\frac{\Delta}{n-\Delta}) = 2.592.$

Clearly $T_1(G_1 \cup G_2) \leq 2.592$.

Acknowledgment

The authors would like to thank the esteemed conference secretary and the reviewers of the article.

References

[1] M. Binu, S. Mathew, J.N Mordeson, *Connectivity index of a fuzzy graph and its application to human trafficking*, Fuzzy sets and systems, 360 (2019), pp. 117–136.

[2] S.R. Islam, M. Pal,*Second Zagreb index for fuzzy graphs and its application in mathematical chemistry*, Iranian Journal of Fuzzy Systems, 20 (2023), pp. 119–136.

[3] U. Jana, G. Ghorai,*First entire Zagreb index of fuzzy graph and its application*, Axioms, 12 (2023), pp. 415.

[4] A. Josy, S. Mathew, J.N. Mordeson, *Neighborhood connectivity index of a fuzzy graph and its application to human trafficking*, Iranian Journal of Fuzzy Systems, 19 (2022), pp. 139–154.

[5] S. Kalathian, S. Ramalingam, S. Raman and N. Srinivasan,*Some topological indices in fuzzy graphs*, Journal of Intelligent and Fuzzy Systems, 39 (2020), pp. 6033–6046.

[6] N. Kansal, P. Garg, O. Singh, *Temperature-Based Topological Indices and QSPR Analysis of COVID-19 Drugs*, Polycyclic aromatic compounds, (2022).

[7] A. Kauffman, *Introduction a la Theorie des Sous-Emsembles Flous*, Masson et Cie, Paris, French, 1973.

[8] V.R Kulli, *Computation of Some Temperature Indices of HC5C5 [p, q] Nanotubes*, Annals of Pure and Applied Mathematics, 20 (2019), pp. 69–74.

[9] V.R Kulli, *Inverse sum temperature index and multiplicative inverse sum temperature index of certain nanotubes*, International Journal of Recent Scientific Research, 12 (2021), pp. 40635–40639.

[10] S. Mathew, J.N. Mordeson, D.S. Malik, *Fuzzy Graph Theory*, Studies in Fuzziness and Soft Computing, Switzerland, 2018.

[11] A. Muneera, T.N. Rao, R.V.N.S Rao and J.V. Rao,*Applications of Fuzzy Graph Theory Portrayed In Various Fields*, Research Square, Durham, NC, USA, (2021).

[12] J. Ramezani Tousi, M. Ghods,*Computing K Banhatti and K Hyper Banhatti indices of Titania Nanotubes TiO2[m, n]*, Journal of Information and Optimization Sciences, 44 (2023), pp. 207–216.

[13] J. Ramezani Tousi, M. Ghods,*Investigating Banhatti indices on the molecular graph and the line graph of Glass with M-polynomial approach*, Proyecciones Journal of Mathematics, 43 (2024), pp. 199–219.

[14] J. Ramezani Tousi, M. Ghods,*Some polynomials and degree-based topological indices of molecular graph and line graph of Titanium dioxide nanotubes*, Journal of Information and Optimization Sciences, 45 (2023), pp. 0252–2667.

[15] J. Ramezani Tousi, M. Ghods,*Computational Analysis of the molecular graph and the line graph of Glass by studying their M-Polynomial and topological indices*, Discontinuity, Nonlinearity, and Complexity, 13 (2024), pp. 361–371.

[16] X. Shi, R. Cai, J. Ramezani Tousi and A.A Talebi,*Quantitative Structure–Property Relationship Analysis in Molecular Graphs of Some Anticancer Drugs with Temperature Indices Approach*, Mathematics, 12 (2024), pp. 1953.

[17] H. Wiener, *Structural determination of Paraffin Boiling Points*, Iranian Journal of Fuzzy Systems, (1974).

Email: m.sadeghi002@umail.umz.ac.ir
Email: a.talebi@umz.ac.ir

Degree-based topological indices and QSPR analysis of Novel Drugs used for the Treatment of Diabetes

Arezo Esmaeili, Masoud Ghods

Semnan University, Department of Applied Mathematics,

Semnan 35131-19111, Iran

Arezo.esmaeili@semnan.ac.ir; mghods@semnan.ac.ir

ABSTRACT

Topological indices (TIs) are quantitative descriptors obtained from the molecular graph that represents. The chemical structure of a compound is analyzed through the calculation of physicochemical properties and drug characteristics, which is conducted using TI derived from degree and adjacency. This study aims to investigate TI based on the degree of ten diabetes medications employing multivariate, specifically the *M*-polynomial approach. Our Quantitative Structure-Property Relationship (QSPR) models revealed a robust correlation between these indices and pertinent drug properties. The analyses suggest that the identification of optimal regression models based on these indices demonstrates a significant ability to predict the physical features of pharmaceutical agents, including Boiling Point (BP), Enthalpy of Vaporization (EV), Flash Point (FP), Molar Refractivity (MR), Polar Surface Area (PSA), Polarizability (PO), Molar Volume (MV) and Index of Refraction (IR) for diabetes medications.

KEYWORDS: *M*-polynomial, QSPR, Topological Indices, Physicochemical properties.

1 INTRODUCTION

Diabetes is one of the oldest known diseases in human history. The term "diabetes" is derived from the Greek word "siphon," which means "to pass through," as patients with diabetes often produce large amounts of urine. The initial recorded medical accounts of diabetes can be traced back to approximately 1500 BC in ancient Egyptian manuscripts, where the symptoms of the disease were clearly outlined.

During the 2nd century AD, the Greek doctor "Aretaeus" and in the third century "Galen" described this condition [1,2]. The history of diabetes medications dates back to the early twentieth century with the discovery of insulin. In 1921, "Frederick Banting" and "Charles Best" extracted insulin from the pancreas of dogs and demonstrated that this hormone could lower blood sugar levels. This revolutionary discovery transformed the treatment of type 1 diabetes and saved millions of lives.

Following the discovery of insulin, oral medications for type 2 diabetes were developed. The first oral medication, "sulfonylureas," was introduced in 1955. These drugs help stimulate the pancreas to produce more insulin. In subsequent decades, novel medications, including metformin (1957) and DPP-4 Antagonist, were introduced to aid in blood sugar control.

In recent years, New categories of therapeutic agents, including GLP-1 receptor agonists and SGLT2 inhibitors, have recently emerged, offering not only blood sugar control but also additional benefits like weight loss and cardiovascular protection [3,4].

Diabetes is a metabolic disorder characterized by the pancreas's inability to produce adequate insulin or by the body's ineffective utilization of insulin. This chronic condition results in increased blood glucose concentrations, commonly referred to as " Blood Glucose". Glucose is obtained from the nutrients we

consume and functions as a crucial energy substrate for our bodies. The pancreas produces a substance known as insulin, which facilitates the uptake of sugar into cells for utilization as energy. Another hormone, referred to as glucagon, also contributes to the maintenance of blood sugar levels [5-7]. Diabetes is a long-term disorder for which there is currently no definitive cure; however, successful management approaches can substantially improve the quality of life for those affected by the disease. Pharmacological treatments are employed to control this serious condition, and numerous clinical trials are being conducted to combat its complications. Timely diagnosis, screening, and appropriate medication are essential for helping patients manage this potentially life-threatening disease in the long term. Among the essential medications for diabetes management are Gliclazide, Sitagliptin, Vildagliptin, Empagliflozin, Nateglinide, Tolazamide, Bromocriptine, Metformin, Alogliptin and Miglitol [8]. Illustration 1 depicts the molecular structure of the pharmaceuticals.

The diverse characteristics and behaviors of a substance are intricately connected to its molecular representation, which is a central focus in the field of graph theory in chemistry. QSPR are mathematical frameworks that correlate the physicochemical characteristics and biological functions of substances with their chemical architectures. These models have become essential tools in the pharmaceutical development process, assisting in the prediction of the physicochemical attributes and biological functions of compounds.

The properties of a molecule can be expressed via topological descriptors, which provide insights without requiring experimental laboratory work. A topological descriptor is a representation from the set of graphs to the set of real numbers, describing the topology of the graph, and is utilized in QSPR analyses. Importantly, these descriptors remain invariant for structurally equivalent graphs. While topological descriptors can be calculated using conventional designations, the process can be labor-intensive, particularly when deriving multiple descriptors within a specific category [9-11].

Topological indices are quantitative measures that characterize the topology of a molecular graph within the realm of mathematical chemistry. They encapsulate molecular attributes such as complexity, symmetry, and connectivity. These indices play a crucial role in the assessment of physicochemical, biological, and pharmaceutical characteristics of chemical compounds. Various polynomials and topological indices are extensively calculated, as these polynomials encode diverse properties of the molecular graph.

Chemical graph theory represents a crucial domain within computational chemistry and drug design, where degree-based topological descriptors hold substantial significance and are integral to this field. The application of TI in QSPR studies has attracted much attention in recent years [12-14]. Although topological descriptors are utilized across various disciplines, including mathematics, bioinformatics, informatics, and biology, their most prominent application thus far remains in nonempirical QSPR.

In this study, we construct the molecular graph of diabetes medications based on the molecular structure sourced from ChemSpider, ensuring that it is free from loops and multiple edges. Let V(H) and W(H) represent the collections of vertices and edges of a graph H, correspondingly. The degree of a vertex r∈ V(H), represented as δ(r), refers to the number of edges associated with r. After edge counting, the corresponding polynomial is calculated from the following formula:

$$M(H;x,y)=\sum_{\alpha\le\beta} m_{\alpha\beta}(H)\,x^{\alpha}y^{\beta} \tag{1}$$

That $m_{\alpha\beta}$ indicates the quantity of edges between vertices of degree α and β.

We have subsequently computed degree-based topological indices associated with diabetes medications. The characteristics estimated through this approach demonstrate a robust relationship with the properties of diabetes therapeutics, as established through linear regression analysis. It has been observed that a significant association exists between the properties of these compounds and their corresponding topological indices.

2 MATERIAL AND METHOD

In the molecular configurations of medications, atoms are modeled as vertices, while the bonds that connect these atoms are represented as edges. The graph H = (V, W) is defined as a simple, finite, and connected graph, where V and W denote the collections of nodes and edges, correspondingly, within the chemical graph. The degree of a node s in graph H is defined as the count of nodes that are neighboring it, represented as δ(s). In the context of chemistry, the valence of an atom is closely related to its connectivity within the molecular structure [15,16]. The formula for calculating the TIs is given in Table 1. Due to its extensive applicability, the derivation of the formulas for degree-based TI is given in various articles. For further reading, refer to references [17-20].

Table 1 Exploration of TIs and Their Formulation via *M*-polynomial.

TI	Formula H(Ⅱ(x), Ⅱ(y))	g (x, y) = M (H; x, y)
First Zagreb Index: M_1	$\sum_{rs\in W(H)}(\eta(r)+\eta(s))$	$(D_x+D_y)(g(x,y))\big\|_{x=y=1}$
Second Zagreb Index: M_2	$\sum_{rs\in W(H)}\eta(r)\eta(s)$	$(D_xD_y)(g(x,y))\big\|_{x=y=1}$
Redefined Third Zagreb Index: $RezM_3$	$\sum_{rs\in W(H)}\eta(r)\eta(s)(\eta(r)+\eta(s))$	$(D_xD_y)(D_x+D_y)(g(x,y))\big\|_{x=y=1}$
Modified Second Zagreb Index: mM_2	$\sum_{rs\in W(H)}\frac{1}{\eta(r)\eta(s)}$	$S_xS_y(g(x,y))\big\|_{x=y=1}$
Forgotten Topological Index: F	$\sum_{rs\in W(H)}(\eta^2(r)+\eta^2(s))$	$(D_x^2+D_y^2)(g(x,y))\big\|_{x=y=1}$
Symmetric Division Index: SDD	$\sum_{rs\in W(H)}\frac{(\eta^2(r)+\eta^2(s))}{\eta(r)\eta(s)}$	$(D_xS_y+S_xD_y)(g(x,y))\big\|_{x=y=1}$
Harmonic Index: H	$\sum_{rs\in W(H)}\frac{2}{\eta(r)+\eta(s)}$	$2S_xJ(g(x,y))\big\|_{x=1}$
Inverse Sum Index: ISI	$\sum_{rs\in W(H)}\frac{\eta(r)\eta(s)}{\eta(r)+\eta(s)}$	$S_xJD_xD_y(g(x,y))\big\|_{x=1}$
Augmented Zagreb Index: *AZI*	$\sum_{rs\in W(H)}\left(\frac{\eta(r)\eta(s)}{\eta(r)+\eta(s)-2}\right)^3$	$S_x^3Q_{-2}JD_x^3D_y^3(g(x,y))\big\|_{x=1}$
Sum Connectivity Index: SCI(G)	$\sum_{rs\in W(H)}\frac{1}{\sqrt{\eta(r)+\eta(s)}}$	$S_x^{\frac{1}{2}}J(g(x,y))\big\|_{x=1}$
Inverse Randić Index: IR	$\sum_{rs\in W(H)}\frac{1}{\sqrt{\eta(r)\eta(s)}}$	$S_x^{\frac{1}{2}}S_y^{\frac{1}{2}}(g(x,y))\big\|_{x=y=1}$
Ordinary Geometric Arithmetic Index: OGA	$\sum_{rs\in W(H)}\frac{2\sqrt{\eta(r)\eta(s)}}{(\eta(r)+\eta(s))}$	$2S_xJD_x^{\frac{1}{2}}D_y^{\frac{1}{2}}(g(x,y))\big\|_{x=1}$
Atomic Bond Connectivity Index: ABC	$\sum_{rs\in W(H)}\sqrt{\frac{\eta(r)+\eta(s)-2}{\eta(r)\eta(s)}}$	$S_x^{\frac{1}{2}}Q_{-2}J\left(D_x^{\frac{1}{2}}+D_y^{\frac{1}{2}}\right)(g(x,y))\big\|_{x=1}$

Where,

$D_x=x\left(\frac{\partial g(x,y)}{\partial x}\right)$, $D_y=y\left(\frac{\partial g(x,y)}{\partial y}\right)$, $S_x=\int_0^x\frac{g(t,y)}{t}dt$, $S_y=\int_0^y\frac{g(x,t)}{t}dt$, $Jg(x,y)=g(x,x)$, $Q_kg(x)=x^kg(x)$.

For degree-based TI: $\eta(r)=\delta(r),\eta(s)=\delta(s),g(x,y)=M(H;x,y)$.

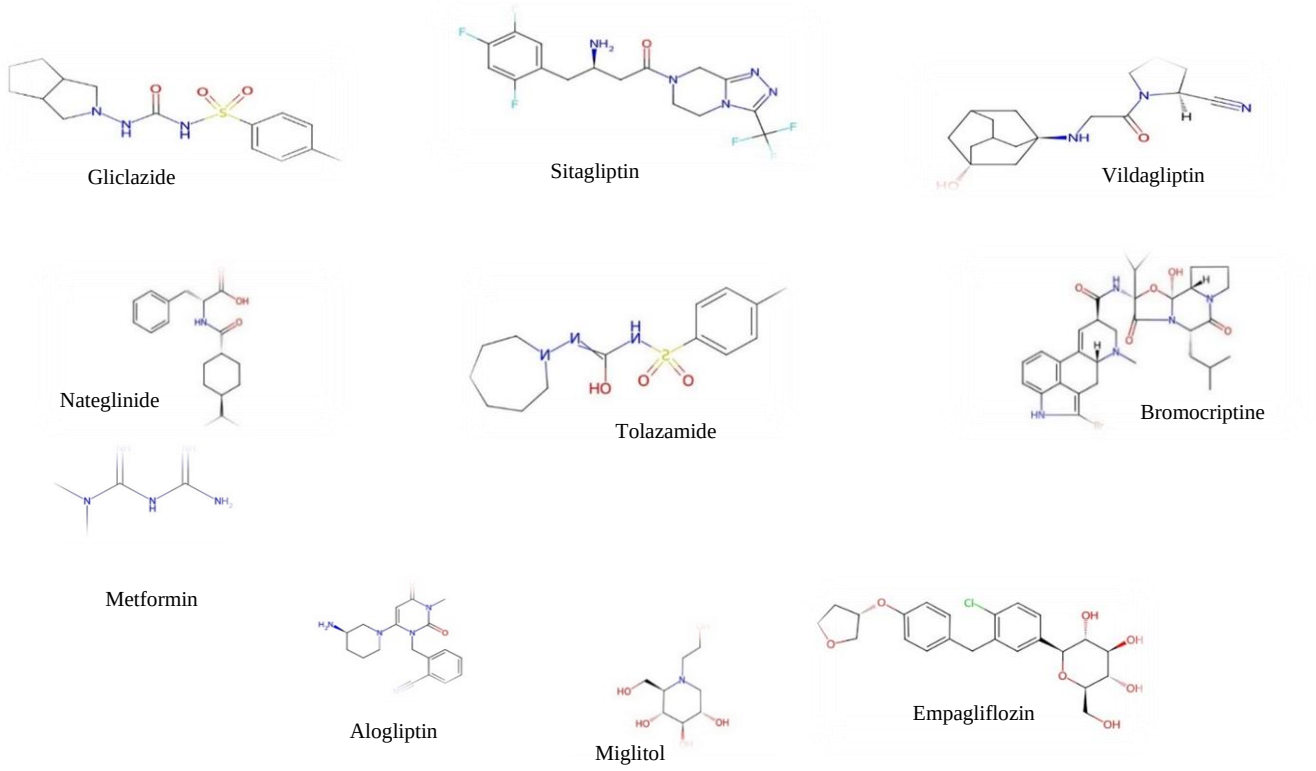


Figure 1: Molecular structure of Gliclazide, Sitagliptin, Vildagliptin, Nateglinide, Tolazamide, Bromocriptine, Metformin, Alogliptin, Miglitol, Empagliflozin.

Theorem 1. Assuming that GL represents Gliclazide, the following relationship is established:

$$M\ (GL;x,y) = 2xy^{3} + 2xy^{4} + 4x^{2}y^{2} + 13x^{2}y^{3} + x^{2}y^{4} + x^{3}y^{3} + x^{3}y^{4}.$$

Proof: Figure 2 illustrates the Gliclazide graph. Observing that, we can conclude that $|V(GL)| = 22$ and $|W(GL)| = 24$.

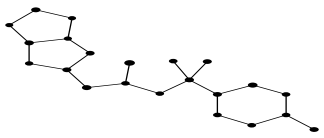


Figure 2: Molecular graph of Gliclazide (GL).

In the framework of structural examination, the edge collection of Gliclazide (GL) can be categorized into seven distinct groups, as delineated below, according to the degrees of the vertices:

$$W_{13} = \{rs \in W\ (GL) \mid \delta(r) = 1,\ \ \delta(s) = 3\},\ W_{14} = \{rs \in W\ (GL) \mid \delta(r) = 1,\ \delta(s) = 4\},$$
$$W_{22} = \{rs \in W\ (GL) \mid \delta(r) = 2,\ \delta(s) = 2\},\ W_{23} = \{rs \in W\ (GL) \mid \delta(r) = 2,\ \delta(s) = 3\},$$
$$W_{24} = \{rs \in W\ (GL) \mid \delta(r) = 2,\ \delta(s) = 4\},\ W_{33} = \{rs \in W\ (GL) \mid \delta(r) = 3,\ \delta(s) = 3\},$$
$$W_{34} = \{rs \in W\ (GL) \mid \delta(r) = 3,\ \delta(s) = 4\}.$$

By a designation of *M*-polynomial

$$M(H;x,y)=\sum_{\alpha\le\beta} m_{\alpha\beta}(H)x^{\alpha}y^{\beta}.$$

$$M(GL;x,y)=\sum_{1\le 3} m_{13}x\ \ y^{3}+\sum_{1\le 4} m_{14}xy^{4}+\sum_{2\le 2} m_{22}x^{2}y^{2}+\sum_{2\le 3} m_{23}x^{2}y^{3}+\sum_{2\le 4} m_{24}x^{2}y^{4}$$

$$+\sum_{3\le 3} m_{33}x^{3}y^{3}+\sum_{3\le 4} m_{34}x^{3}y^{4}=|w_{13}|xy^{3}+|w_{14}|xy^{4}+|w_{22}|x^{2}y^{2}+|w_{23}|x^{2}y^{3}$$

$$+|w_{24}|x^{2}y^{4}+|w_{33}|x^{3}y^{3}+|w_{34}|x^{3}y^{4}.$$

$$M\left(GL;x,y\right)=2xy^{3}+2xy^{4}+4x^{2}y^{2}+13x^{2}y^{3}+x^{2}y^{4}+x^{3}y^{3}+x^{3}y^{4}.$$

The spatial depiction of *M*-polynomials for Gliclazide is depicted in Figure 3 below.

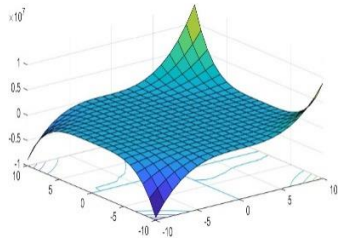


Figure 3: Scheme of *M*-Polynomial for Gliclazide.

In the following proposition, we derive several TIs of Gliclazide.

Proposition 1. Let GL represent the graph of Gliclazide. The following relationships are defined:

1. $M_1(GL)=118.$
2. $M_2(GL)=137.$
3. $mM_2(GL)=4.6527.$
4. $\mathrm{Re}zM_3(GL)=704.$
5. $F(GL)=318.$
6. $SDD(GL)=57.9166.$
7. $IR(GL)=10.4374.$
8. $H(GL)=9.9523.$
9. $ISI(GL)=27.2476.$
10. $AZI(GL)=180.7053.$
11. $SCI(GL)=10.9027.$
12. $OGA(GL)=113.1993.$
13. $ABC(GL)=44.0504.$

Proof:

$$M\ (GL;x,y)=g\ (x,y)=2xy^{4}+2xy^{3}+13x^{2}y^{3}+4x^{2}y^{2}+x^{2}y^{4}+x^{3}y^{4}+x^{3}y^{3}.$$
$$D_{X}\ g\ (x,y)=2xy^{3}+2xy^{4}+8x^{2}y^{2}+26x^{2}y^{3}+3x^{3}y^{4}+3x^{3}y^{3}+2x^{2}y^{4}.$$
$$D_{y}\ g\ (x,y)=6xy^{3}+8xy^{4}+8x^{2}y^{2}+39x^{2}y^{3}+4x^{2}y^{4}+3x^{3}y^{3}+4x^{3}y^{4}.$$
$$\left(D_{x}+D_{y}\right)\left(g\ (x,y)\right)=8xy^{3}+10xy^{4}+16x^{2}y^{2}+65x^{2}y^{3}+6x^{2}y^{4}+6x^{3}y^{3}+7x^{3}y^{4}.$$
$$D_{x}D_{y}\ \left(g\ (x,y)\right)=6xy^{3}+8xy^{4}+16x^{2}y^{2}+78x^{2}y^{3}+8x^{2}y^{4}+9x^{3}y^{3}+12x^{3}y^{4}.$$
$$D_{x}^{k}D_{y}^{k}\ \left(g\ (x,y)\right)=3^{K}2xy^{3}+4^{K}2xy^{4}+2^{2K}4x^{2}y^{2}+6^{K}13x^{2}y^{3}+8^{K}x^{2}y^{4}+9^{K}x^{3}y^{3}+12^{K}x^{3}y^{4}.$$
$$S_{x}S_{y}\ \left(g\ (x,y)\right)=\frac{2}{3}xy^{3}+\frac{2}{4}xy^{4}+x^{2}y^{2}+\frac{13}{6}x^{2}y^{3}+\frac{1}{8}x^{2}y^{4}+\frac{1}{9}x^{3}y^{3}+\frac{1}{12}x^{3}y^{4}.$$
$$S_{x}^{k}S_{y}^{k}\ \left(g\ (x,y)\right)=\frac{2}{3^{K}}xy^{3}+\frac{2}{4^{K}}xy^{4}+\frac{4}{2^{2K}}x^{2}y^{2}+\frac{13}{6^{K}}x^{2}y^{3}+\frac{1}{8^{K}}x^{2}y^{4}+\frac{1}{9^{K}}x^{3}y^{3}+\frac{1}{12^{K}}x^{3}y^{4}.$$
$$\left(D_{x}^{2}+D_{y}^{2}\right)\left(g\ (x,y)\right)=20xy^{3}+34xy^{4}+32x^{2}y^{2}+169x^{2}y^{3}+20x^{2}y^{4}+18x^{3}y^{3}+25x^{3}y^{4}.$$
$$D_{x}D_{y}\ \left(D_{x}+D_{y}\right)\left(g\ (x,y)\right)=24xy^{3}+40xy^{4}+64x^{2}y^{2}+390x^{2}y^{3}+48x^{2}y^{4}+54x^{3}y^{3}+84x^{3}y^{4}.$$
$$S_{x}J\ \left(g\ (x,y)\right)=\frac{3}{2}x^{4}+3x^{5}+\frac{1}{3}x^{6}+\frac{1}{7}x^{7}.$$
$$S_{x}JD_{x}D_{y}\ \left(g\ (x,y)\right)=\frac{22}{4}x^{4}+\frac{86}{5}x^{5}+\frac{17}{6}x^{6}+\frac{12}{7}x^{7}.$$
$$S_{x}^{3}Q_{-2}JD_{x}^{3}D_{y}^{3}\ \left(g\ (x,y)\right)=\frac{310}{8}x^{2}+\frac{2936}{27}x^{3}+\frac{1241}{64}x^{4}+\frac{1728}{125}x^{5}.$$
$$S_{x}^{\frac{1}{2}}J\ \left(g\ (x,y)\right)=3x^{4}+3\sqrt{5}x^{5}+\frac{\sqrt{6}}{3}x^{6}+\frac{\sqrt{7}}{7}x^{7}.$$
$$S_{x}^{\frac{1}{2}}S_{y}^{\frac{1}{2}}\left(g\ (x,y)\right)=\frac{2\sqrt{3}}{3}xy^{3}+xy^{4}+2x^{2}y^{2}+\frac{13}{\sqrt{6}}x^{2}y^{3}+\frac{\sqrt{2}}{4}x^{2}y^{4}+\frac{1}{3}x^{3}y^{3}+\frac{\sqrt{3}}{6}x^{3}y^{4}.$$
$$S_{x}^{\frac{1}{2}}Q_{-2}J\left(D_{x}^{\frac{1}{2}}+D_{y}^{\frac{1}{2}}\right)\left(g\ (x,y)\right)=\frac{2+2\sqrt{3}+8\sqrt{2}}{\sqrt{2}}x^{2}+\frac{6+13\sqrt{2}+13\sqrt{3}}{\sqrt{3}}x^{3}+\frac{2\left(1+\sqrt{3}\right)+\sqrt{2}}{2}x^{4}+\frac{2\sqrt{5}+\sqrt{15}}{5}x^{5}.$$

We now have the following:

1. $M_{1}(GL)=\left(D_{x}+D_{y}\right)\left(g\ (x,y)\right)\big|_{x=y=1}=118.$
2. $M_{2}(GL)=D_{x}D_{y}\,g\ (x,y)\big|_{x=y=1}=137.$
3. $mM_{2}(GL)=S_{x}S_{y}\,g\ (x,y)\big|_{x=y=1}=4.6527.$
4. $\mathrm{Re}\,zM_{3}(GL)=D_{x}D_{y}\left(D_{x}+D_{y}\right)g\ (x,y)\big|_{x=y=1}=704.$
5. $F\ (GL)=\left(D_{x}^{2}+D_{y}^{2}\right)g\ (x,y)\big|_{x=y=1}=318.$
6. $SDD\ (GL)=\left(S_{y}D_{x}+S_{x}D_{y}\right)g\ (x,y)\big|_{x=y=1}=57.9166.$
7. $IR\ (GL)=S_{x}^{\frac{1}{2}}S_{y}^{\frac{1}{2}}\left(g\ (x,y)\right)\big|_{x=y=1}=10.4374.$
8. $H\ (GL)=2S_{x}J\ \left(g\ (x,y)\right)\big|_{x=y=1}=9.9523.$
9. $ISI\ (GL)=S_{x}JD_{x}D_{y}\ \left(g\ (x,y)\right)\big|_{x=y=1}=27.2476.$
10. $AZI\ (GL)=S_{x}^{3}Q_{-2}JD_{x}^{3}D_{y}^{3}\ \left(g\ (x,y)\right)\big|_{x=y=1}=180.7053.$
11. $SCI\ (GL)=S_{x}^{\frac{1}{2}}J\ \left(g\ (x,y)\right)\big|_{x=y=1}=10.9027.$
12. $OGA\ (GL)=2S_{x}JD_{x}^{\frac{1}{2}}D_{y}^{\frac{1}{2}}\left(g\ (x,y)\right)\big|_{x=y=1}=113.1993.$
13. $ABC\ (GL)=S_{x}^{\frac{1}{2}}Q_{-2}J\left(D_{x}^{\frac{1}{2}}+D_{y}^{\frac{1}{2}}\right)\left(g\ (x,y)\right)\big|_{x=y=1}=44.0504.$

Theorem 2. Assuming that **SI** represents Sitagliptin, the following relationship is established:

$$M\left(SI;x,y\right)=5xy^{3}+3xy^{4}+2x^{2}y^{2}+14x^{2}y^{3}+5x^{3}y^{3}+x^{3}y^{4}.$$

Proof: Figure 4 illustrates the Sitagliptin graph. Observing that, we can conclude that $\left|\mathrm{V(SI)}\right|$ = 28 and $\left|\mathrm{W(SI)}\right|$ = 30.

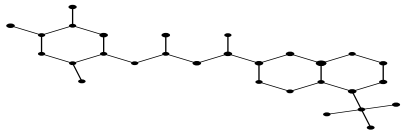


Figure 4: Molecular graph of Sitagliptin (SI).

In the framework of structural examination, the edge collection of Sitagliptin (SI) can be categorized into six distinct groups, as delineated below, according to the degrees of the vertices:

$$W_{13}=\left\{rs\in W\left(SI\right)|\,\delta\left(r\right)=1,\ \ \delta\left(s\right)=3\right\},W_{14}=\left\{rs\in W\left(SI\right)|\,\delta\left(r\right)=1,\ \delta\left(s\right)=4\right\},$$
$$W_{22}=\left\{rs\in W\left(SI\right)|\,\delta\left(r\right)=2,\ \delta\left(s\right)=2\right\},W_{23}=\left\{rs\in W\left(SI\right)|\,\delta\left(r\right)=2,\ \delta\left(s\right)=3\right\},$$
$$W_{33}=\left\{rs\in W\left(SI\right)|\,\delta\left(r\right)=3,\ \delta\left(s\right)=3\right\},W_{34}=\left\{rs\in W\left(SI\right)|\,\delta\left(r\right)=3,\ \delta\left(s\right)=4\right\}.$$

By a designation of *M*-polynomial

$$M\left(H;x,y\right)=\sum_{i\le j}m_{ij}\left(H\right)x^{i}y^{j}.$$

$$M\left(SI;x,y\right)=\sum_{1\le3}m_{13}x\ \ y^{3}+\sum_{1\le4}m_{14}xy^{4}+\sum_{2\le2}m_{22}x^{2}y^{2}+\sum_{2\le3}m_{23}x^{2}y^{3}+\sum_{3\le3}m_{33}x^{3}y^{3}+\sum_{3\le4}m_{34}x^{3}y^{4}$$
$$=\left|E_{13}\right|xy^{3}+\left|E_{14}\right|xy^{4}+\left|E_{22}\right|x^{2}y^{2}+\left|E_{23}\right|x^{2}y^{3}+\left|E_{33}\right|x^{3}y^{3}+\left|E_{34}\right|x^{3}y^{4}.$$
$$M\left(SI;x,y\right)=5xy^{3}+3xy^{4}+2x^{2}y^{2}+14x^{2}y^{3}+5x^{3}y^{3}+x^{3}y^{4}.$$

The spatial depiction of *M*-polynomials for Sitagliptin is depicted in Figure 5 below.

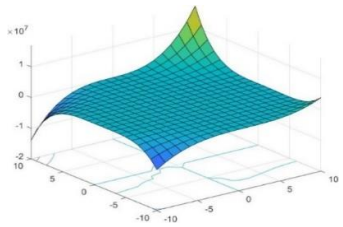


Figure 5: Scheme of *M*-polynomial for Sitagliptin.

In the following proposition, we derive several TIs of Sitagliptin.

Proposition 2. Let **SI** represent the graph of Sitagliptin. The following relationships are defined:

1. $M_1(SI) = 150.$
2. $M_2(SI) = 176.$
3. $mM_2(SI) = 5.8888.$
4. $\mathrm{Re}zM_3(SI) = 911.$
5. $F(SI) = 414.$
6. $SDD(SI) = 75.8333.$
7. $IR(SI) = 13.0576.$
8. $H(SI) = 12.2523.$
9. $ISI(SI) = 34.1642.$
10. $AZI(SI) = 222.7632.$
11. $SCI(SI) = 13.5217.$
12. $OGA(SI) = 63.5646.$
13. $ABC(SI) = 52.9457.$

Theorem 3. Assuming that **VI** represents Vildagliptin, the following relationship is established:

$$M(VI; x, y) = xy^2 + xy^3 + xy^4 + 3x^2y^2 + 10x^2y^3 + 7x^2y^4 + 2x^3y^3.$$

Proof: Figure 6 illustrates the Vildagliptin graph. Observing that, we can conclude that $|V(VI)| = 22$ and $|W(VI)| = 25$.

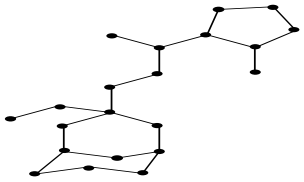


Figure 6: Molecular graph of Vildagliptin (VI).

In the framework of structural examination, the edge collection of Vildagliptin (VI) can be categorized into seven distinct groups, as delineated below, according to the degrees of the vertices:

$$W_{12} = \{rs \in W(VI) \mid \delta(r) = 1,\ \delta(s) = 2\},\ W_{23} = \{rs \in W(VI) \mid \delta(r) = 2,\ \delta(s) = 3\},$$
$$W_{13} = \{rs \in W(VI) \mid \delta(r) = 1,\ \delta(s) = 3\}, W_{22} = \{rs \in W(VI) \mid \delta(r) = 2,\ \delta(s) = 2\},$$
$$W_{14} = \{rs \in W(VI) \mid \delta(r) = 1,\ \delta(s) = 4\}, W_{24} = \{rs \in W(VI) \mid \delta(r) = 2,\ \delta(s) = 4\},$$
$$W_{33} = \{rs \in W(VI) \mid \delta(r) = 3,\ \delta(s) = 3\}.$$

By a designation of *M*-polynomial

$$M(H; x, y) = \sum_{\alpha \le \beta} m_{\alpha\beta}(H) x^{\alpha} y^{\beta}.$$

$$M(VI; x, y) = \sum_{1\le 2} m_{12} x\ y^2 + \sum_{1\le 3} m_{13} xy^3 + \sum_{1\le 4} m_{14} x\ y^4 + \sum_{2\le 2} m_{22} x^2y^2 + \sum_{2\le 3} m_{23} x^2y^3 + \sum_{2\le 4} m_{24} x^2y^4$$
$$+ \sum_{3\le 3} m_{33} x^3y^3 = |W_{12}| xy^2 + |W_{13}| xy^3 + |W_{14}| xy^4 + |W_{22}| x^2y^2 + |W_{23}| x^2y^3 + |W_{24}| x^2y^4 + |W_{33}| x^3y^3.$$
$$M(VI; x, y) = xy^2 + xy^3 + xy^4 + 3x^2y^2 + 10x^2y^3 + 7x^2y^4 + 2x^3y^3.$$

The spatial depiction of *M*-polynomials for Vildagliptin is depicted in Figure 7 below.

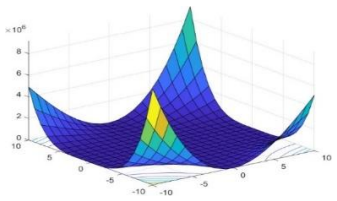


Figure 7: Scheme of *M*-polynomial for Vildagliptin.

In the following proposition, we derive several TIs of Vildagliptin.

Proposition 3. Let **VI** represent the graph of Vildagliptin. The following relationships are defined:

1. $M_1(VI) = 128.$
2. $M_2(VI) = 155.$
3. $mM_2(VI) = 4.5972.$
4. $\mathrm{Re}zM_3(VI) = 830.$
5. $F(VI) = 362.$
6. $SDD(VI) = 59.25.$
7. $IR(VI) = 10.5085.$
8. $H(VI) = 10.0666.$
9. $ISI(VI) = 29.55.$
10. $AZI(VI) = 196.5266.$
11. $SCI(VI) = 11.1708.$
12. $OGA(VI) = 23.2015.$
13. $ABC(VI) = 45.6562.$

Theorem 4. Assuming that **EM** represents Empagliflozin, the following relationship is established:

$$M(EM; x, y) = xy^2 + 4xy^3 + 6x^2y^2 + 17x^2y^3 + 6x^3y^3.$$

Proof: Figure 8 illustrates the Empagliflozin graph. Observing that, we can conclude that $|V(EM)| = 31$ and $|E(EM)| = 34$.

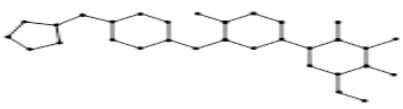


Figure 8: Molecular graph of Empagliflozin (EM).

In the framework of structural examination, the edge collection of Empagliflozin (EM) can be categorized into five distinct groups, as delineated below, according to the degrees of the vertices:

$$W_{12} = \{rs \in W(EM) \mid \delta(r) = 1,\ \delta(s) = 2\}, W_{13} = \{rs \in W(EM) \mid \delta(r) = 1,\ \delta(s) = 3\},$$
$$W_{22} = \{rs \in W(EM) \mid \delta(r) = 2,\ \delta(s) = 2\}, W_{23} = \{rs \in W(EM) \mid \delta(r) = 2,\ \delta(s) = 3\},$$
$$W_{33} = \{rs \in W(EM) \mid \delta(r) = 3,\ \delta(s) = 3\}.$$

By a designation of *M*-polynomial

$$M(H;x,y)=\sum_{\alpha\le\beta} m_{\alpha\beta}(H)x^{\alpha}y^{\beta}.$$

$$M(EM;x,y)=\sum_{1\le 2} m_{12}x\ \ y^{2}+\sum_{1\le 3} m_{13}xy^{3}+\sum_{2\le 2} m_{22}x^{2}y^{2}+\sum_{2\le 3} m_{23}x^{2}y^{3}+\sum_{3\le 3} m_{33}x^{3}y^{3}$$
$$=|W_{12}|xy^{2}+|W_{13}|xy^{3}+|W_{22}|x^{2}y^{2}+|W_{23}|x^{2}y^{3}+|W_{33}|x^{3}y^{3}.$$
$$M(EM;x,y)=xy^{2}+4xy^{3}+6x^{2}y^{2}+17x^{2}y^{3}+6x^{3}y^{3}.$$

The spatial depiction of *M*-polynomials for Empagliflozin is depicted in Figure 9 below.

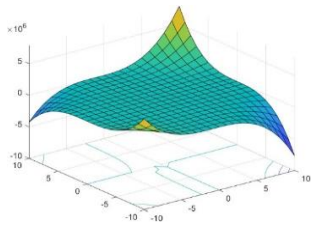


Figure 9: Scheme of *M*-polynomial for Empagliflozin.

In the following proposition, we derive several TIs of Empagliflozin.

Proposition 4. Let **EM** represent the graph of Empagliflozin. The following relationships are defined:

1. $M_1(EM)=164.$
2. $M_2(EM)=194.$
3. $mM_2(EM)=6.8333.$
4. $\mathrm{Re}zM_3(EM)=984.$
5. $F(EM)=422.$
6. $SDD(EM)=76.6666.$
7. $IR(EM)=14.9568.$
8. $H(EM)=7.2333.$
9. $ISI(EM)=39.0666.$
10. $AZI(EM)=273.8437.$
11. $SCI(EM)=15.6293.$
12. $OGA(EM)=62.5027.$
13. $ABC(EM)=104.582.$

Similarly, the TIs were calculated for six additional diabetes medications., and the results of these calculations are presented in Tables 3 and 4.

3 TOPOLOGICAL INDICES AND QSPR

Based on the aforementioned information, thirteen TIs were analyzed for ten diabetic drugs, with the results presented in Tables 3 and 4. The modeling of eight physical features, including BP, EV, FP, MR, PSA, PO, MV, and IR, was conducted for the drugs Sitagliptin, Vildagliptin, Empagliflozin, Gliclazide, Nataglinide, Tolazamide, Bromocriptine, Metformin, Alogliptin, and Miglitol, extracted from the ChemSpider database and presented in Table 2. Furthermore, the normality of these data was evaluated, and the correlations among them are detailed in Table 5.

Subsequently, a linear regression model was employed to evaluate and analyze the data.

The physical characteristics of pharmaceutical agents employed in the treatment of diabetes are detailed

in Table 2.

***Table* 2** Physical features of diabetes drugs.

Name	***BP***	***EV***	***FP***	***MR***	***PSA***	***PO***	***MV***	***IR***
Sitagliptin	529.9	80.5	274.3	85.2	77	33.8	252.4	1.59
Vildagliptin	531.3	92.8	275.1	81.7	76	32.4	238.3	1.601
Empagliflozin	664.5	102.7	355.7	114.4	109	45.4	322.4	1.628
Gliclazide	-	-	-	84.4	87	33.5	239.2	1.624
Nateglinide	527.6	84.4	272.9	89.6	66	35.5	287.3	1.536
Tolazamide	484.5	79	246.8	82.5	90	32.7	237.9	1.61
Bromocriptine	891.3	135.7	492.8	165.4	118	65.6	429.4	1.697
Metformin	172.5	40.9	58.1	33.4	89	13.2	100.8	1.576
Alogliptin	519.2	79.2	267.8	93.3	94	37	252.9	1.66
Miglitol	453.7	82.3	284.3	48.5	104	19.2	142.1	1.598

The calculation results of section 2 are shown in Table 3,4.

***Table* 3** The computed values of TIs for the pharmaceutical agents.

Name	**M_1**	**M_2**	**$RezM_3$**	**mM_2**	**F**	**SDD**	**H**
Sitagliptin	150.00	176	911	5.8888	414	75.83333	12.25238
Vildagliptin	128.00	155	830	4.59722	362	59.25	10.0666
Empagliflozin	164.00	194	984	6.83333	422	76.6666	7.23333
Gliclazide	118.00	137	704	4.6527	318	57.9166	9.9523
Nateglinide	112.00	126	618	5.17	282	56.33	10.5
Tolazamide	104.00	116	578	4.63	272	53.25	9.52
Bromocriptine	250.00	488	1672	8.79	710	114.58	19.04
Metformin	36.00	36	174	2.1	94	23	3.63
Alogliptin	126.00	149	704	5.25	328	60.3	11
Miglitol	66.00	77	400	3.36	172	33.67	6.26

***Table* 4** The computed values of TIs for the pharmaceutical agents.

Name	ISI	AZI	SCI	IR	OGA	ABC
Sitagliptin	34.16428	222.7632	13.52172	13.05763	63.5646	52.9457
Vildagliptin	29.55	196.52662	11.17086	10.5085	23.2015	45.6562
Empagliflozin	39.0666	273.84375	15.6293	14.9568	62.5027	104.582
Gliclazide	27.2476	180.7053	10.9027	10.4374	113.1993	44.05046
Nateglinide	26.25	178.98	11.2	10.97	23.12	45.02
Tolazamide	23.95	161.31	10.2	9.97	21.08	41.05
Bromocriptine	42.07	400.73	21.29	20.04	46.08	86.96
Metformin	7.65	44.27	3.8	4.04	15.49	15.02
Alogliptin	31	205.22	11.92	11.47	25.13	48.21
Miglitol	15.38	77.51	6.58	6.61	13.4	26.8

3.1 *Regression models*

In this section, the analysis is performed utilizing the TIs calculated in Section 2. The linear regression model is articulated as follows:

$$P=B+A(TI) \quad (2)$$

Where P represents the features of the diabetes medication, B is a constant, A is the regression coefficient. This analysis was conducted using SPSS software, incorporating eight specific characteristics and thirteen TIs for a total of ten diabetes medications.

Utilizing equation (2), various linear regression models for TIs are presented as follows:

1. M_1

BP=158.783+2.945 [M_1], EV=39.190+.374 [M_1], FP=70.387+1.668 [M_1], MR=12.486+.601 [M_1], PO=4.908+.239 [M_1], MV=62.151+1.500 [M_1], IR=1.546+.001 [M_1].

2. M_2

BP=308.978+1.314 [M_2], EV=57.355+.172 [M_2], FP=153.375+.756 [M_2], MR=42.983+.271[M_2], PO=17.024+.108 [M_2], MV=141.845+.656 [M_2], IR=1.568+.000264 [M_2].

3. $RezM_3$

BP=209.041+2.081 [$RezM_3$], EV=44.823+0.274 [$RezM_3$], FP=97.282+1.258 [$RezM_3$], MR=23.479+0.327 [$RezM_3$], PO=9.275+0.130[$RezM_3$], MV=91.111+1.898[$RezM_3$], IR=1.554+0.130[$RezM_3$].

4. mM_2

BP=44.112+93.899 [mM2], EV=25.689+11.718 [mM2], FP=4.510+53.352 [mM2], MR=-9.694+19.023 [mM2], PO=-3.897+7.553 [mM_2], MV=3.169+48.194 [mM2], IR=1.533+.015 [mM2].

5. F

BP=187.631+1.010 [F], EV=42.481+.129 [F], FP=86.467+.573 [F], MR=18.388+.206 [F], PO=7.253+.082 [F], MV=78.155+.510 [F], IR=1.549+.000186 [F].

6. SDD
BP=119.918+6.684 [SDD], EV=34.811+.840 [SDD], FP=49.613+3.764 [SDD], MR=3.890+1.374 [SDD], PO=1.495+.546 [SDD], MV=39.811+3.446 [SDD], IR=1.541+.001 [SDD].
7. H(G)
BP=169.209+36.330 [H], EV=40.904+4.574 [H], FP=76.043+20.596 [H], MR=13.530+7.472 [H], PO=5.334+2.966 [H], MV=64.670+18.662 [H], IR=1.548+.006 [H].
8. ISI
BP=99.745+15.564 [ISI], EV=33.524+1.910 [ISI], FP=40.198+8.696 [ISI], MR=1.623+3.120 [ISI], PO=.582+1.239 [ISI], MV=28.453+8.027 [ISI], IR=1.543+.003 [ISI].
9. AZI
BP=196.086+1.709 [AZI], EV=44.215+.216 [AZI], FP=93.482+.958 [AZI], MR=18.951+.355 [AZI], PO=7.476+.141 [AZI], MV=77.612+.889 [AZI], IR=1.553+.000306 [AZI].
10. SCI
BP=109.483+35.980 [SCI], EN=33.510+4.519 [SCI], FP=42.877+20.339 [SCI], MR=2.483+7.345 [SCI], PO=.936+2.916 [SCI], MV=35.007+18.523 [SCI].
11. IR
BP=88.283+39.164 [IR], EV=31.030+4.903 [IR], FP=30.862+22.141 [IR], MR=-1.772+7.997 [IR], PO=-.753+3.175 [IR], MV=23.889+20.202 [IR], IR=1.538+.007 [IR].
12.ABC
BP=235.392+5.697 [ABC], EV=49.348+.715 [ABC], FP=114.082+3.219 [ABC], MR=29.203+1.149 [ABC], PO=11.539+.456 [ABC], MV=100.937+2.926 [ABC].

Table 5 The computed values of correlation coefficients of physical features for the pharmaceutical agents.

TI	***BP***	***EN***	***FP***	***MR***	***PSA***	***PO***	***MV***	***IR***
M_1	0.953	0.915	0.903	0.974	0.419	0.974	0.958	0.681
M_2	0.902	0.894	0.868	0.934	0.537	0.934	0.89	**0.727**
$RezM_3$	0.947	**0.926**	0.905	0.958	0.448	0.958	0.933	0.692
mM_2	0.960	0.906	**0.912**	0.977	0.426	0.978	**0.976**	0.629
F	0.940	0.911	0.892	0.96	0.419	0.96	0.937	0.691
SDD	0.939	0.892	0.885	0.967	0.390	0.967	0.955	0.654
H	0.836	0.796	0.793	0.86	0.199	0.86	0.846	0.59
ISI	0.905	0.840	0.846	0.908	0.273	0.909	0.921	0.581
AZI	**0.947**	0.903	0.888	**0.985**	0.413	**0.985**	0.973	0.679
SCI	0.959	0.911	0.907	0.982	0.409	0.982	0.975	0.654

IR	0.958	0.907	0.906	0.981	0.409	0.981	**0.976**	0.645
OGA	0.579	0.493	0.525	0.321	0.066	0.322	0.324	0.261

Bold numbers indicate the strongest correlations.

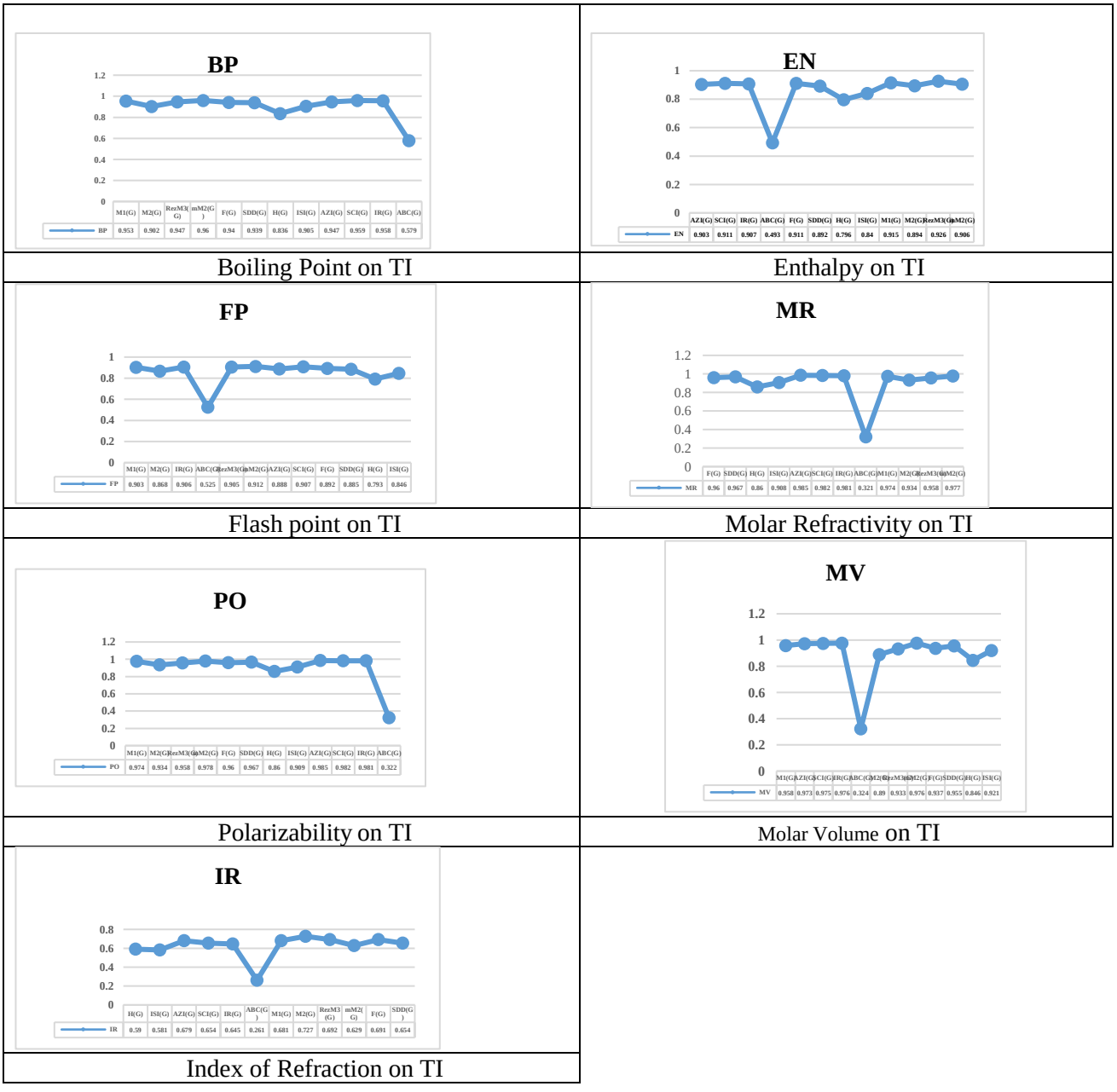


Figure 10: Correlation coefficients on Physical feature.

Table 6 Calculation of statistical metrics for the linear QSPR about M1.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	2.945	158.783	.953	.908	49.157	69.056	.000	significant
EV	10	.374	39.190	.915	.838	8.623	36.181	.003	significant
FP	10	1.668	70.387	.903	.815	41.675	30.804	.001	significant
MR	10	.601	12.486	**.974**	.949	6.713	149.902	.000	significant
PO	10	.239	4.908	**.974**	**.950**	2.658	150.742	.000	significant
MV	10	1.500	62.151	.958	.918	21.648	89.843	.000	significant
IR	10	.001	1.546	.681	.463	.027	6.906	.030	significant
Bold numbers indicate the strongest correlations.									

Table 7 Calculation of statistical metrics for the linear QSPR about M_2.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	1.314	308.978	.902	.813	49.611	30.374	.000	significant
EV	10	.172	57.355	.894	.799	6.792	27.840	.000	significant
FP	10	.756	153.375	.868	.753	34.020	21.395	.003	significant
MR	10	.271	42.983	.934	.873	7.386	55.051	.000	significant
PO	10	.108	17.024	**.934**	**.873**	2.936	54.875	.000	significant
MV	10	.656	141.845	.890	.792	24.022	30.405	.000	significant
IR	10	.000264	1.568	.727	.529	.018	8.981	.000	significant
Bold numbers indicate the strongest correlations.									

Table 8 Calculation of statistical metrics for the linear QSPR about $RezM_3$.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	.421	209.041	.947	.897	46.507	60.882	.003	significant
EV	10	.054	44.823	.926	.858	7.206	42.401	.000	significant
FP	10	.240	97.282	.905	.819	36.851	31.626	.033	significant
MR	10	.085	23.479	.958	.917	7.647	88.635	.015	significant
PO	10	.034	9.275	**.958**	**.917**	3.033	88.861	.016	significant
MV	10	.210	91.111	.933	.871	24.277	53.785	.006	significant
IR	10	7.693E-5	1.554	.692	.479	.024	7.365	.000	significant
Bold numbers indicate the strongest correlations.									

Table 9 Calculation of statistical metrics for the linear QSPR about mM_2.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	93.899	44.112	.960	.921	57.045	81.646	.000	significant
EV	10	11.718	25.689	.906	.821	11.351	32.118	.001	significant
FP	10	53.352	4.510	.912	.832	49.695	34.731	.001	significant
MR	10	19.023	-9.694	.977	.955	7.872	171.003	.000	significant
PO	10	7.553	-3.897	**.978**	**.956**	3.118	171.811	.000	significant
MV	10	48.194	3.169	.976	.952	20.788	157.402	.000	significant
IR	10	.015	1.533	.629	.396	.036	5.234	.000	significant
Bold numbers indicate the strongest correlations.									

Table 10 Calculation of statistical metrics for the linear QSPR about F.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	1.010	187.631	.940	.883	52.369	53.046	.009	significant
EV	10	.129	42.481	.911	.829	8.378	33.994	.001	significant
FP	10	.573	86.467	.892	.795	41.519	27.129	.001	significant
MR	10	.206	18.388	.960	.922	7.900	94.044	.000	significant
PO	10	.082	7.253	**.960**	**.922**	3.132	94.333	.000	significant
MV	10	.510	78.155	.937	.878	24.974	57.797	.014	significant
IR	10	.000186	1.549	.691	.477	.026	7.304	.000	significant
Bold numbers indicate the strongest correlations.									

Table 11 Calculation of statistical metrics for the linear QSPR about SDD.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	6.684	119.918	.939	.881	61.516	51.907	.000	significant
EV	10	.840	34.811	.892	.796	10.656	27.298	.014	significant
FP	10	3.764	49.613	.885	.782	49.753	25.173	.002	significant
MR	10	1.374	3.890	.967	.936	8.346	116.430	.000	significant
PO	10	.546	1.495	**.967**	**.936**	3.307	116.942	.000	significant
MV	10	3.446	39.811	.955	.913	24.688	83.623	.000	significant
IR	10	.001	1.541	.654	.428	.031	5.995	.000	significant
Bold numbers indicate the strongest correlations.									

Table 12 Calculation of statistical metrics for the linear QSPR about H.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	36.330	169.209	.836	.698	97.072	16.194	.005	significant
EV	10	4.574	40.904	.796	.633	14.141	12.095	.010	significant
FP	10	20.596	76.043	.793	.628	64.408	11.823	.011	significant
MR	10	7.472	13.530	.860	.740	16.711	22.782	.001	significant
PO	10	2.966	5.334	**.860**	**.740**	6.639	22.742	.001	significant
MV	10	18.662	64.670	.846	.717	44.300	20.223	.002	significant
IR	10	.006	1.548	.590	.348	.033	4.274	.000	significant
Bold numbers indicate the strongest correlations.									

Table 13 Calculation of statistical metrics for the linear QSPR about ISI.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	15.564	99.745	.905	.819	81.684	31.688	.001	significant
EV	10	1.910	33.524	.840	.706	13.760	16.820	.005	significant
FP	10	8.696	40.198	.846	.716	61.207	17.618	.004	significant
MR	10	3.120	1.623	.908	.825	14.896	37.720	.000	significant
PO	10	1.239	.582	**.909**	**.826**	5.900	37.944	.000	significant
MV	10	8.027	28.453	.921	.848	35.297	44.468	.000	significant
IR	10	.003	1.543	.581	.338	.036	4.083	.000	significant
Bold numbers indicate the strongest correlations.									

Table 14 Calculation of statistical metrics for the linear QSPR about AZI.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	1.709	196.086	.947	.897	48.044	60.726	.005	significant

EV	10	.216	44.215	.903	.816	8.468	31.093	.001	significant
FP	10	.958	93.482	.888	.788	41.128	26.019	.001	significant
MR	10	.355	18.951	.985	.971	4.709	263.641	.004	significant
PO	10	.141	7.476	**.985**	**.971**	1.861	266.291	.004	significant
MV	10	.889	77.612	.973	.946	16.157	140.696	.001	significant
IR	10	.000306	1.553	.679	.461	.025	6.834	.000	significant
Bold numbers indicate the strongest correlations.									

Table 15 Calculation of statistical metrics for the linear QSPR about SCI.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	35.980	109.483	.959	.920	50.573	80.674	.000	significant
EV	10	4.519	33.510	.911	.831	9.731	34.377	.011	significant
FP	10	20.339	42.877	.907	.823	45.011	32.543	.001	significant
MR	10	7.345	2.483	.982	.964	6.286	212.053	.000	significant
PO	10	2.916	.936	**.982**	**.964**	2.485	213.896	.000	significant
MV	10	18.523	35.007	.975	.951	18.489	155.908	.000	significant
IR	10	.006	1.541	.654	.427	.031	5.966	.000	significant
Bold numbers indicate the strongest correlations.									

Table 16 Calculation of statistical metrics for the linear QSPR about IR.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	39.164	88.283	.958	.917	53.834	77.480	.000	significant
EV	10	4.903	31.030	.907	.823	10.410	32.475	.001	significant
FP	10	22.141	30.862	.906	.820	47.362	31.993	.001	significant
MR	10	7.997	-1.772	.981	.962	6.715	202.318	.000	significant
PO	10	3.175	-.753	**.981**	**.962**	2.656	203.860	.000	significant
MV	10	20.202	23.889	.976	.953	18.988	161.463	.000	significant

IR	10	.007	1.538	.645	.416	.033	5.688	.000	significant
Bold numbers indicate the strongest correlations.									

Table 17 Calculation of statistical metrics for the linear QSPR about ABC.

Physical features	***Number***	***A***	***B***	***R***	***R square***	***Std. E***	***F***	***Sig***	Indicant
Bp	10	5.697	235.392	.842	.709	80.156	17.042	.004	significant
EV	10	.715	49.348	.799	.639	11.794	12.400	.004	significant
FP	10	3.219	114.082	.796	.634	53.735	12.112	.010	significant
MR	10	1.149	29.203	.854	.729	14.075	21.533	.002	significant
PO	10	.456	11.539	**.854**	**.730**	5.581	21.610	.002	significant
MV	10	2.926	100.937	.857	.734	35.410	22.066	.002	significant
Bold numbers indicate the strongest correlations.									

4 CONCLUSION

Table 5 and Figure 10 illustrate the correlation between the physical-chemical features of diabetes medications and the defined topological indices in this study, the majority of the indicators showed a strong and positive correlation. The mM_2 showed a positive and excellent correlation with BP, FP, MV with "r=0.960", "r=0.912", "r=0.976" values. In addition, EV and MR are positive and significant predictors with the $RezM_3$ with the value of "r=0.926", "r=0.958". The AZI showed a high positive correlation with the PO value of (0.985). MV is a high and positive predictor with IR having a value of" r=0.976". The IR property provided a relatively good correlation with the M_2. The PSA property did not have a significant correlation with any of the indices, and the OGA did not have a significant correlation with any of the properties. A positive correlation is observed between the physical and chemical features of diabetes drugs and the TI. Tables 6 through 17 present the regression models for various physical and chemical features. The results show that the regression values (r) exceed 0.5, while the p-values are less than 0.05, indicating reliable predictors for linear regression. Equations are derived based on criteria such as minimum standard error (Std. E), maximum coefficient of determination (R square), and maximum F-statistic (F). Therefore, it can be concluded that all physical and chemical features are highly significant. This underscores the potential significance of these TI in the analysis of QSPR for diabetes drugs, as evidenced by the plotted regression lines (eighty-two lines). The findings of this study may be leveraged to inform the production, development, and enhancement of more effective diabetes therapeutics. Furthermore, the methodology employed in this study can be extended to explore the structural characteristics of other pharmaceutical compounds.

REFERENCES

1. American Diabetes Association. (2014). Diagnosis and classification of diabetes mellitus. Diabetes Care, 37(Supplement 1), S81-S90.

2. M. Hasani, M. Ghods, " Topological indices and QSPR analysis of some chemical structures applied for the treatment of heart patients" International Journal of Quantum Chemistry, Chem. Methodol. 2023, 7, 288.2024.
3. American Diabetes Association. (2015). Standards of medical care in diabetes—2015. Diabetes Care, 38(Supplement 1), S1-S94.
4. JR. Tousi, M. Ghods, " Some polynomials and degree-based topological indices of molecular graph and line graph of Titanium dioxide nanotubes" Journal of Information and Optimization Sciences, Publication date2024.
5. American Diabetes Association. (2021). "Standards of Medical Care in Diabetes—2021." *Diabetes Care*, 44(Supplement 1), S1-S232. doi:10.2337/dc21-Sintroduction.
6. McCulloch, D. K., & Haffner, S. M. (2019). "Diabetes: A Comprehensive Guide." *The Journal of Clinical Endocrinology & Metabolism*, 104(5), 1436-1445. doi:10.1210/jc.2018-01858.
7. World Health Organization. (2021). "Diabetes." Retrieved from.
8. American Diabetes Association. (2021). "Standards of Medical Care in Diabetes—2021." *Diabetes Care*, 44(Supplement 1), S1-S232. doi:10.2337/dc21-Sintroduction.
9. Randić, M. (2001). "Chemical Graph Theory." *Journal of Mathematical Chemistry*, 29(3), 237-249. doi:10.1023/A:1010159521288.
10. JR. Tousi, M. Ghods," Computational Analysis of the Molecular Graph and the Line Graph of Glass by Studying Their M-Polynomial and Topological Indices" Journal Discontinuity, Nonlinearity, and Complexity, Publication date 2024/6/1.
11. Wang, R., & Liu, S. (2018). "Graph Theory and Its Applications in Chemistry." Molecular Diversity, 22(4), 657-672. doi:10.1007/s11030-018-9868-3.
12. Y. C. Kwun, A. Farooq, W. Nazeer, Z. Zahid, S. Noreen, S. M. Kang, Int. J. Anal. Chem. 2018, 2018, 1709073.
13. A. Ali, W. Nazeer, M. Munir, S. M. Kang, Open Chem. 2018, 16, 73.
14. B. Basavanagoud, A. P. Barangi, Open J. Dis. Appl. Math. 2019, 2, 59.
15. A.A. Talebi, Xiaolong Shi, Ruiqi Cai, J. R. Tousi," Quantitative Structure–Property Relationship Analysis in Molecular Graphs of Some Anticancer Drugs with Temperature Indices Approach",[1] Institute of Computing Science and Technology, Guangzhou University, Guangzhou 510006, China, [2] Department of Mathematics, University of Mazandaran, Babolsar 4741613534, Iran.
16. Y. C. Kwun, A. Ali, W. Nazeer, M. Ahmad Chaudhary, S. M. Kang, J. Chem. 2018, 2018.
17. A. A. Talebi, M.Mojahedfar, Siran Lei, Yongsheng Rao," A Novel Concept of Level Graph in Interval-Valued Fuzzy Graphs with Application" [1] Institute of Computing Science and Technology, Guangzhou University, Guangzhou 510006, China, [2] Department of Mathematics, University of Mazandaran, Babolsar 4741613534, Iran.
18. H. Yang, A. Q. Baig, W. Khalid, M. R. Farahani, X. Zhang, J. Chem. 2019, 2019.
19. Wang, Y., & Zhang, J. (2011). "Degree-based topological indices." Journal of Mathematical Chemistry, 49(3), 823-834.
20. McCulloch, D. K., & Haffner, S. M. (2019). "Diabetes: A Comprehensive Guide." The Journal of Clinical Endocrinology & Metabolism, 104(5), 1436-1445. doi:10.1210/jc.2018-01858.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Computational Approaches to Thalassemia Drug Design Using Topological Indices and Python Programming

Negar Kheirkhahan
Department of Applied Mathematics, Semnan University
Semnan 35131-19111, Iran
Negar.kheirkhahan@semnan.ac.ir

Masoud Ghods
Department of Applied Mathematics, Semnan University
Semnan 35131-19111, Iran
mghods@semnan.ac.ir

ABSTRACT

Thalassemia is an inherited blood disorder caused by mutations in the gene responsible for producing haemoglobin. Haemoglobin, a protein found in red blood cells, carries oxygen throughout the body. These mutations significantly reduce the production of red blood cells, leading to anemia. Currently, the available treatments for thalassemia are limited, with only a few therapeutic options that are effective for managing the condition. In recent years, there has been increasing interest in the use of topological indices in various fields, including medicine. This article examines the potential of temperature-based topological indices in analysing drugs used to treat thalassemia. This approach, known as quantitative structure-property relationship (QSPR) modelling, allows us to analyse the relationship between a molecule's structure and its physicochemical properties. These drugs include Decitabine, Etavopivat, Hydroxyurea, Mitapivat, Sirolimus, and Thalidomide. The analyses suggest that identifying optimal regression models using temperature indices effectively predicts critical physical and chemical properties of thalassemia drugs. These properties include Density, Boiling Point, Enthalpy of Vaporization, Flash Point, Molar Refraction, Polar Surface Area, Polarizability, Surface Tension, Molar Volume, and Complexity. This research demonstrates that temperature-based topological indices have the potential to become a valuable tool for developing and optimizing thalassemia drugs. The results show that the p-value is less than 0.05, indicating that the samples are statistically significant. To analyse the graph structure and compute molecular indices, we used the Python programming language along with the math library for mathematical computations.

KEYWORDS: Temperature indices, Topological indices, Thalassemia drugs, (QSPR) modelling.

1 INTRODUCTION

Thalassemia is a genetic blood disorder that occurs when the body produces fewer healthy red blood cells and haemoglobin than normal. Haemoglobin is a protein in red blood cells that carries oxygen to all body tissues. Thalassemia is the most common monogenic disorder worldwide and indicates a major public health issue. This condition leads to fatigue and reduced work capacity in adults and can also cause gastrointestinal, neurological, and immune system disorders. Additionally, it can exacerbate chronic kidney disease and congestive heart failure. One of the most common types of anemia is thalassemia minor [13, 17, 23]. Diagnosis of thalassemia can be performed through routine tests such as complete blood count (CBC) or measurement of serum iron and ferritin [11]. Sometimes, bone marrow biopsy analysis is necessary for definitive diagnosis. However, implementing these tests is associated with high costs and time requirements [13]. Graph theory in chemistry is an interdisciplinary field that leverages the power of

graph theory to analyse the structures of molecules and establish connections between various chemical properties, activities (e.g., biological activity, reactivity), and events. In this approach, a molecular graph serves as a symbolic representation of a molecule's structural formula. Vertices within the graph denote atoms, and edges represent the chemical bonds that connect them. This visual framework allows researchers to explore how a molecule's structure influences its various properties and behaviors. Chemical graph theory offers innovative tools for studying chemical structures, including topological indices expressed as real numbers [8, 20]. These indices serve as descriptors for exploring the structure and certain properties of molecular graphs. Many studies have explored molecular graphs and drug structures using topological indices [3, 4, 7, 12, 14, 15, 21].

Investigating the relationships between a molecule's structure, as described by topological indices, and its physicochemical properties is a cornerstone of Quantitative Structure-Property Relationship (QSPR) modelling. These models leverage regression analysis techniques to establish correlations between the physical and chemical properties of molecules and their corresponding topological indices. This approach offers valuable insights into how a molecule's structure influences its behavior. Building upon this foundation, the field of Quantitative Structure-Activity Relationship (QSAR) has extensively employed topological indices to analyse the activity of drug structures. [2, 6, 10]. In this article, various topological indices are examined on several thalassemia drugs to enable researchers to identify relevant physical properties and chemical reactions.

2 PAPER FORMAT

In the molecular graph G, the degree of any vertex u is represented as du. The number of vertices in G is n, and the connection between vertices u and v is denoted by uv.

Definition 1 Fajtlowicz defined the concept of the vertex temperature u for a connected graph G as follows [16]:

$$T_u = \frac{d_u}{n - d_u}.$$

Definition 2 Temperature indices have been calculated based on vertex temperature, as is shown in Table 2 [16, 18, 19].

Table 1 lists the abbreviations used in this article.

Recent studies have focused on temperature indices. [1, 5, 9, 22].

Table 1 Abbreviations list.

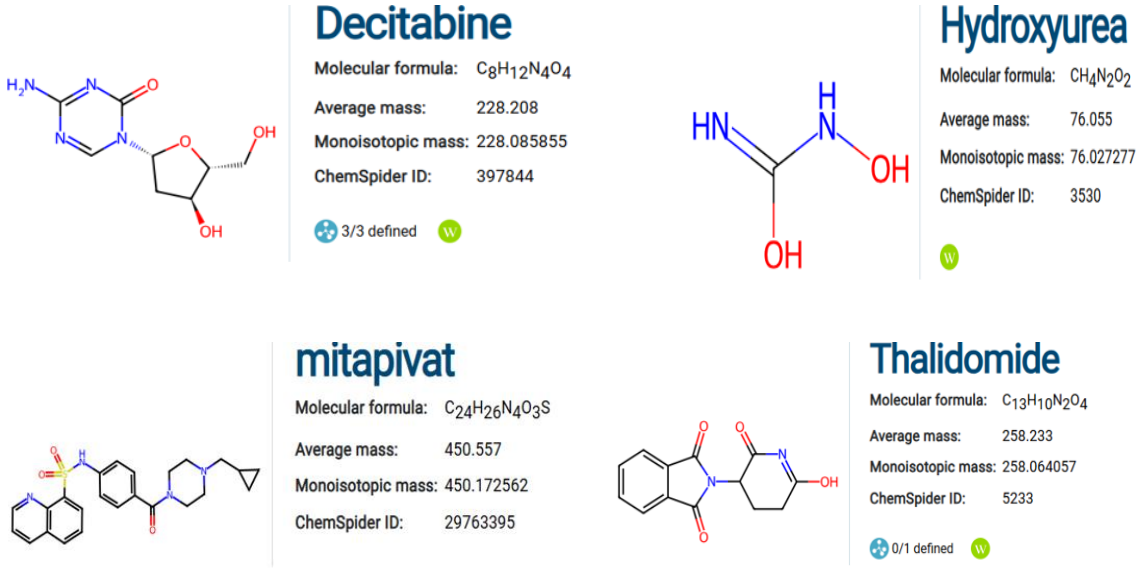
MEANING	ABBREVIATION
Density	DE
Boiling point	BP
Enthalpy of Vaporization	EN
Flash Point	FP
Molar Refractivity	MR
Polar Surface Area	PSA
Polarizability	PO
Surface Tension	ST
Molar Volume	MV
Complexity	COM
number of samples used for building the regression equation	N
correlation coefficient	R
Standard Error of regression coefficient	SE
Fisher's statistic	F
Topological Indices	TI
Quantitative structure-property relationship	QSPR

Table 2. Topological indices related to temperature for graph G.

TEMPERATURE INDEX	DEFINITION
Product connectivity temperature index [18]	$PT(G)=\sum_{uv\in E(G)}\frac{1}{\sqrt{T_u\times T_v}}$
Harmonic temperature index [16]	$HT(G)=\sum_{uv\in E(G)}\frac{2}{T_u+T_v}$
first temperature index [18]	$T_1(G)=\sum_{uv\in E(G)}(T_u+T_v)$
Symmetric division temperature index [18]	$SDT(G)=\sum_{uv\in E(G)}(\frac{T_u}{T_v}+\frac{T_v}{T_u})$
The modified third temperature index [19]	${}^{m}T_3(G)=\sum_{uv\in E(G)}\frac{1}{(T_u+T_v)}$
The modified second temperature index [19]	${}^{m}T_2(G)=\sum_{uv\in E(G)}\frac{1}{(T_u.T_v)}$

3 PRINCIPAL FINDINGS

In this section, following the introduction of the chemical structures of Thalassemia drugs (Figure 1) such as Decitabine, Etavopivat, Hydroxyurea, Mitapivat, Sirolimus, and Thalidomide, the vertex temperatures are obtained, and temperature indices are then calculated.



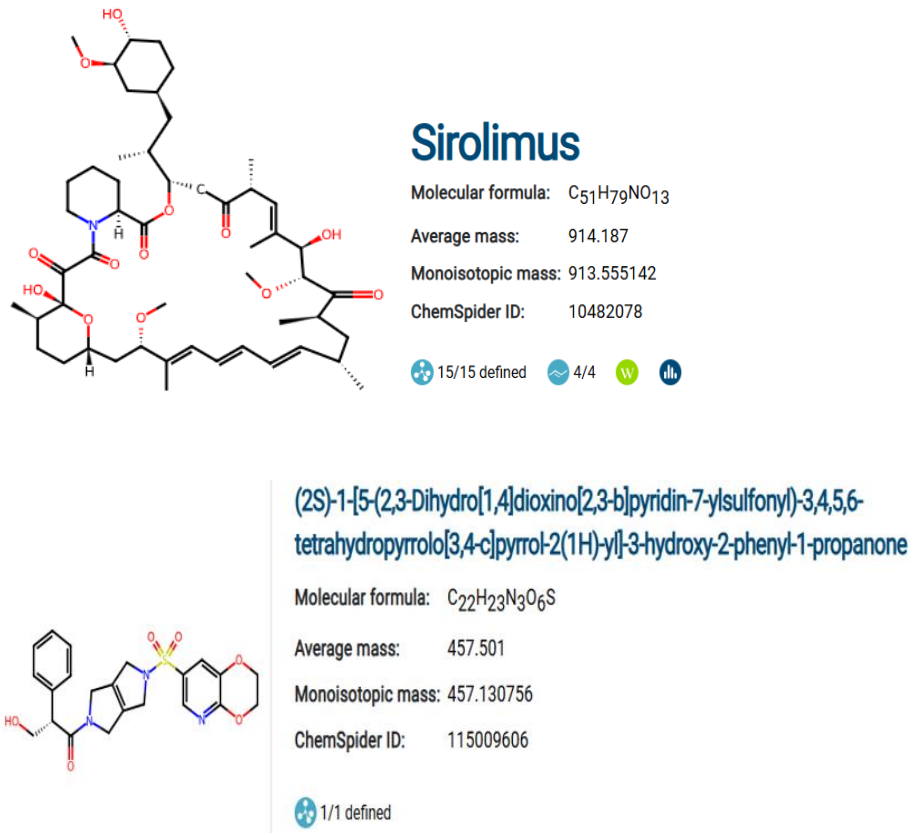


Figure 1: Chemical structure of Thalassemia drugs.

As an example, temperature indices have been calculated for the drug Sirolimus.
Figure 2 shows the Chemical structure and molecular graph of Sirolimus.

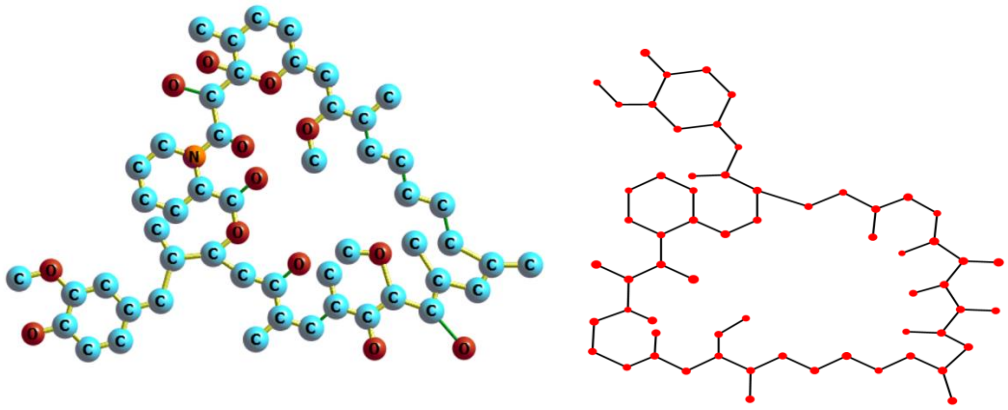


Figure 2: The Chemical structure and Molecular graph of Sirolimus.

The molecular graph of Sirolimus, denoted by S, incorporates eight distinct edge types. These edge types will be further categorized and explained in detail in the following section.

$$E_1=\left\{uv\in E(S)|T_u=\frac{2}{62},T_v=\frac{3}{61}\right\},\ E_2=\left\{uv\in E(S)|T_u=\frac{2}{62},T_v=\frac{2}{62}\right\},E_3=\left\{uv\in E(S)|T_u=\frac{1}{63},T_v=\frac{2}{62}\right\},E_4=\left\{uv\in E(S)|T_u=\frac{1}{63},T_v=\frac{3}{61}\right\},$$
$$E_5=\left\{uv\in E(S)|T_u=\frac{3}{61},T_v=\frac{3}{61}\right\},\ E_6=\left\{uv\in E(S)|T_u=\frac{3}{61},T_v=\frac{4}{60}\right\},E_7=\left\{uv\in E(S)|T_u=\frac{1}{63},T_v=\frac{4}{60}\right\},E_8=\left\{uv\in E(S)|T_u=\frac{2}{62},T_v=\frac{4}{60}\right\}.$$

The analysis of the edges in S is presented in Table 3.

Table 3 Edge partitioning of S.

(T_U,T_V) / UV ∈ $E(S)$	$(\frac{2}{62},\frac{3}{61})$	$(\frac{2}{62},\frac{2}{62})$	$(\frac{1}{63},\frac{2}{62})$	$(\frac{1}{63},\frac{3}{61})$	$(\frac{3}{61},\frac{3}{61})$	$(\frac{3}{61},\frac{4}{60})$	$(\frac{1}{63},\frac{4}{60})$	$(\frac{2}{62},\frac{24}{60})$
Number of edges	25	9	2	15	12	2	1	1

Using the definition 2 and Table 2, the following topological indices for S can be calculated:

- PT(S) index
- HT(S) index
- T_1(S) index
- SDT(S) index
- ${}^mT_3$(S) index
- ${}^mT_2$(S) index

Theorem 1 Following the definition of vertex temperature and the calculation methods outlined in Table 2, the temperature indices of S were computed as follows:

1. PT(S) index=1863.1456
2. HT(S) index=1760.2038
3. T_1(S) index=5.18322
4. SDT(S) index=164.0530
5. ${}^mT_3$(S) index=880.1019
6. ${}^mT_2$(S) index=54509.6666

Proof

Utilizing the relationships in Table 3 and applying them to Table 2, we obtain:

$$1.PT(S)=\sum_{uv\in E(A)}\frac{1}{\sqrt{T_u.T_v}}=25(\frac{1}{\sqrt{\frac{2}{62}.\frac{3}{61}}})+9(\frac{1}{\sqrt{\frac{2}{62}.\frac{2}{62}}})+2(\frac{1}{\sqrt{\frac{1}{63}.\frac{2}{62}}})+15(\frac{1}{\sqrt{\frac{1}{63}.\frac{3}{61}}})+12(\frac{1}{\sqrt{\frac{3}{61}.\frac{3}{61}}})+2(\frac{1}{\sqrt{\frac{3}{61}.\frac{4}{60}}})$$
$$+(\frac{1}{\sqrt{\frac{1}{63}.\frac{4}{60}}})+(\frac{1}{\sqrt{\frac{2}{62}.\frac{4}{60}}})=1863.1456$$

$$2.HT(S)=\sum_{uv\in E(A)}\frac{2}{T_u+T_v}=25(\frac{2}{\frac{2}{62}+\frac{3}{61}})+9(\frac{2}{\frac{2}{62}+\frac{2}{62}})+2(\frac{2}{\frac{1}{63}+\frac{2}{62}})+15(\frac{2}{\frac{1}{63}+\frac{3}{61}})+12(\frac{2}{\frac{3}{61}+\frac{3}{61}})+2(\frac{2}{\frac{3}{61}+\frac{4}{60}})$$
$$+(\frac{2}{\frac{1}{63}+\frac{4}{60}})+(\frac{2}{\frac{2}{62}+\frac{4}{60}})=1760.2038$$

$$3.T_1(S)=\sum_{uv\in E(A)}(T_u+T_v)=25(\frac{2}{62}+\frac{3}{61})+9(\frac{2}{62}+\frac{2}{62})+2(\frac{1}{63}+\frac{2}{62})+15(\frac{1}{63}+\frac{3}{61})+12(\frac{3}{61}+\frac{3}{61})+2(\frac{3}{61}+\frac{4}{60})$$
$$+(\frac{1}{63}+\frac{4}{60})+(\frac{2}{62}+\frac{4}{60})=5.18322$$

$$4.SDT(S)=\sum_{uv\in E(A)}(\frac{T_u}{T_v}+\frac{T_v}{T_u})=25(\frac{\frac{2}{62}}{\frac{3}{61}}+\frac{\frac{3}{61}}{\frac{2}{62}})+9(\frac{\frac{2}{62}}{\frac{2}{62}}+\frac{\frac{2}{62}}{\frac{2}{62}})+2(\frac{\frac{1}{63}}{\frac{2}{62}}+\frac{\frac{2}{62}}{\frac{1}{63}})+15(\frac{\frac{1}{63}}{\frac{3}{61}}+\frac{\frac{3}{61}}{\frac{1}{63}})+12(\frac{\frac{3}{61}}{\frac{3}{61}}+\frac{\frac{3}{61}}{\frac{3}{61}})+2(\frac{\frac{3}{61}}{\frac{4}{60}}+\frac{\frac{4}{60}}{\frac{3}{61}})$$
$$+(\frac{\frac{1}{63}}{\frac{4}{60}}+\frac{\frac{4}{60}}{\frac{1}{63}})+(\frac{\frac{2}{62}}{\frac{4}{60}}+\frac{\frac{4}{60}}{\frac{2}{62}})=164.0530$$

$$5.{}^{m}T_3(S)=\sum_{uv\in E(G)}\frac{1}{(T_u+T_v)}=25(\frac{1}{\frac{2}{62}+\frac{3}{61}})+9(\frac{1}{\frac{2}{62}+\frac{2}{62}})+2(\frac{1}{\frac{1}{63}+\frac{2}{62}})+15(\frac{1}{\frac{1}{63}+\frac{3}{61}})+12(\frac{1}{\frac{3}{61}+\frac{3}{61}})+2(\frac{1}{\frac{3}{61}+\frac{4}{60}})$$
$$+(\frac{1}{\frac{1}{63}+\frac{4}{60}})+(\frac{1}{\frac{2}{62}+\frac{4}{60}})=880.1019$$
$$=128.455$$

$$6.{}^{m}T_2(S)=\sum_{uv\in E(G)}\frac{1}{(T_u.T_v)}=25(\frac{1}{\frac{2}{62}.\frac{3}{61}})+9(\frac{1}{\frac{2}{62}.\frac{2}{62}})+2(\frac{1}{\frac{1}{63}.\frac{2}{62}})+15(\frac{1}{\frac{1}{63}.\frac{3}{61}})+12(\frac{1}{\frac{3}{61}.\frac{3}{61}})+2(\frac{1}{\frac{3}{61}.\frac{4}{60}})$$
$$+(\frac{1}{\frac{1}{63}.\frac{4}{60}})+(\frac{1}{\frac{2}{62}.\frac{4}{60}})=54509.6666$$

4 TEMPERATURE INDICES AND QSPR MODELS

This study investigates the relationship between six topological indices derived from temperature indices PT(G), HT(G), T1(G), SDT(G), ${}^{m}T_3(G)$, and ${}^{m}T_2(G)$ and ten representative physical features (DE), (BP), (EN), (FP), (MR), (PSA), (PO), (ST), (MV), and (COM) for six Thalassemia drugs Decitabine, Etavopivat, Hydroxyurea, Mitapivat, Sirolimus, and Thalidomide. The physical and chemical property data for the analysed drugs were retrieved from Table 4 of the ChemSpider database. Following the calculation of topological indices based on molecular structure, as described previously, the obtained values are presented in Table 5 alongside the corresponding experimental property values from the aforementioned source. Normality tests performed on the data in Table 6 confirmed a normal distribution, justifying the use of regression modelling for data analysis.

4.1 Regression analyses

Building upon the temperature indices calculated in Section 3, this section focuses on the development of a linear regression model. This model will be used to analyze the relationships between the calculated temperature indices and the drugs' physical and chemical properties.

$$P=B+A\ (TI) \quad (1)$$

Where:

P: Represents the Thalassemia drug property (dependent variable)

B: Constant term (y-intercept)

A: Regression coefficient

TI: Topological index (independent variable)

This equation (Equation 1) represents the formulated linear regression model. Here, "P" signifies a specific Thalassemia drug property we aim to predict or analyze. "B" is the constant term, representing the expected value of "P" when the topological index (TI) is zero. "A" represents the regression coefficient, indicating the change in "P" associated with a unit increase in the topological index. This analysis was performed using SPSS software to establish linear models for ten specific characteristics (Thalassemia drug properties) of six Thalassemia drugs. These models were built upon the six topological indices calculated earlier. Utilizing Equation (1) as the general framework, the following section will present the various linear models tailored to each of the ten drug properties.

1. Product connectivity temperature index [PT (G)]

DE=1.699+ 0.000293 [PT (G)], BP=429.564+ 0.324 [PT (G)],

EN=73.143+ 0.049 [PT (G)], FP=213.585+ 0.196 [PT (G)]

MR=44.694+ 0.114 [PT (G)], PSA=85.630+ 0.057 [PT (G)]

PO=17.738+ 0.045 [PT (G)], ST=82.536 - 0.017 [PT (G)]

MV=97.955+ 0.374 [PT (G)], COM=276.305+ 0.833 [PT (G)].

2. Harmonic temperature index [HT (G)]

DE=1.700+.00031 [HT (G)], BP=427.650+0.344 [HT (G)]

EN=72.901+0.052 [HT (G)], FP=212.427+0.208 [HT (G)]

MR=44.112+0.121 [HT (G)], PSA=85.448+0.061 [HT (G)]

PO=17.507+0.048 [HT (G)], ST=82.610-0.018 [HT (G)]

MV=96.218+0.396 [HT (G)], COM=272.274+0.883 [HT (G)].

3. First temperature index [T_1 (G)]

DE=-.708+0.049 [T_1 (G)], BP=3344.498+14.101 [T_1 (G)]

EN=488.170+1.831 [T_1 (G)], FP=1976.805+8.527 [T_1 (G)]

PSA=521.875+2688.43 [T_1 (G)], PO=400.825+2688.43 [T_1 (G)]

ST=-48.321+0.846[T_1 (G)], MV=3152.582+13.750[T_1 (G)]

COM=7124.814+13.750[T_1 (G)].

4. Symmetric division temperature index [SDT (G)]

DE=1.850-.004 [SDT (G)], BP=243.290+4.830 [SDT (G)]

EN=47.272+.702 [SDT (G)], FP=100.911+2.921 [SDT (G)]

MR=-13.657+1.604 [SDT (G)], PSA=59.721+0.758 [SDT (G)]

PO=-5.387+0.636 [SDT (G)], ST=89.933-0.219 [SDT (G)]

MV=-83.304+5.111 [SDT (G)], COM=-146.928+11.655 [SDT (G)]

5. The modified third temperature index [$^mT_3$ (G)]

DE=1.700-.001 [$^mT_3$ (G)], BP=427.650+0.688 [$^mT_3$ (G)]

EN=72.901+0.105 [$^mT_3$ (G)], FP=212.427+0.416 [$^mT_3$ (G)]

MR=44.112+0.243 [$^mT_3$ (G)], PSA=85.448+0.121 [$^mT_3$ (G)]

PO=17.507+0.096 [$^mT_3$ (G)], ST=82.610-0.036 [$^mT_3$ (G)]

MV=96.218+0.793 [$^mT_3$ (G)], COM=272.274+1.767 [$^mT_3$ (G)].

6. The modified second temperature index [$^mT_2$ (G)]

DE=1.651+-8.834E-6 [$^mT_2$ (G)], BP=483.872+0.010 [$^mT_2$ (G)]

EN=80.791+0.002 [$^mT_2$ (G)], FP=246.434+0.006 [$^mT_2$ (G)]

MR=62.349+0.004 [$^mT_2$ (G)], PSA=93.346+0.002 [$^mT_2$ (G)]

PO=24.734+0.001 [$^mT_2$ (G)], ST=80.169-0.001 [$^mT_2$ (G)]

MV=153.417+0.012 [$^mT_2$ (G)], COM=403.320+0.026 [$^mT_2$ (G)].

The physical properties of drugs used for Thalassemia drugs are shown in Table 4.

Table 4 Physicochemical properties of drugs used for treating Thalassemia.

DRUGS	DE	BP	EN	FP	MR	PSA	PO	ST	MV	COM
Decitabine	1.9	485.8	86.6	247.6	50.2	121	19.9	91.7	228.21	356
Etavopivat	1.5	725.2	111.2	392.4	115.2	118	45.7	82.4	457.5	832
Hydroxyurea	1.7	222.1	53.3	88.1	13.8	76	5.5	80	76.055	42.9
Mitapivat	1.4	667.3	98.1	357.4	124.7	91	49.4	67.1	450.6	750
Sirolimus	1.2	973	160.7	542.3	246.7	195	97.8	51.4	914.2	1760
Thalidomide	1.6	487.8	79.4	248.8	65.2	87	25.9	71.6	258.23	449

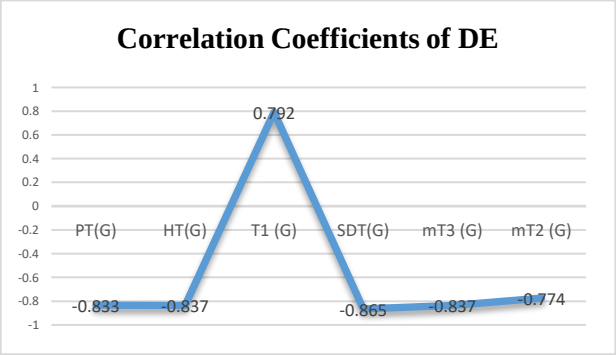
The results of Theorems 1 are shown in Table 5.

Table 5. The values of the temperature indices of the drugs.

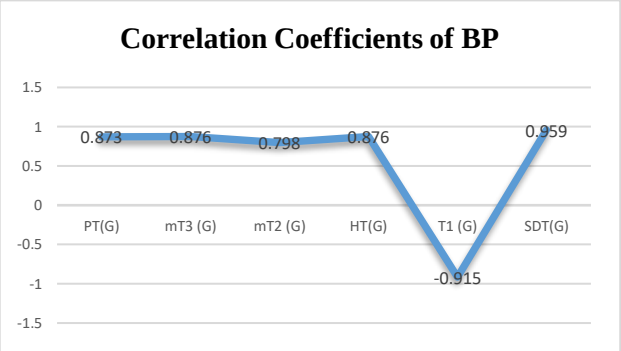
DRUGS	PT(G)	HT(G)	T_1 (G)	SDT(G)	${}^{M}T_3$ (G)	${}^{M}T_2$ (G)
Decitabine	104.0018	97.8943	6.13479	41.97069	48.94716	678.3333
Etavopivat	457.8289	442.2353	6.07057	82.92306	221.1176	6066.2222
Hydroxyurea	6.715476	5.39060	6.58333	18.06944	2.6953	12.33333
Mitapivat	457.3480	444.5014	5.63010	78.08720	222.2507	6132.7777
Sirolimus	1863.1456	1760.2038	5.18322	164.0530	880.1019	54509.6666
Thalidomide	150.9231	143.5729	6.36928	50.01239	71.78646	1144.1111

Table 6. The analysis of correlation coefficients between physical properties of drugs

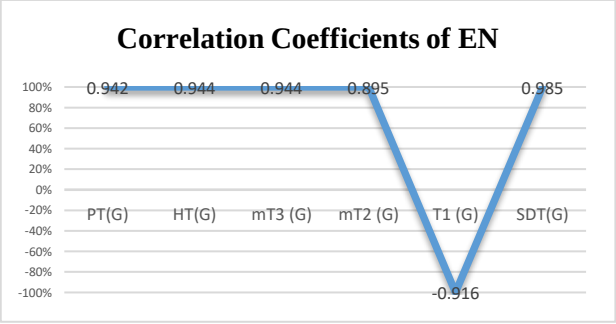
TI	DE	BP	EN	FP	MR	PSA	PO	ST	MV	COM
PT(G)	-0.833	0.873	0.942	0.873	0.965	0.916	0.965	-0.826	0.988	0.970
HT(G)	-0.837	0.876	0.944	0.876	0.967	0.915	**0.968**	**-0.827**	0.989	0.972
T_1 (G)	0.792	-0.915	-0.916	-0.915	-0.947	-0.803	-0.946	0.743	-0.934	-0.923
SDT(G)	-0.865	**0.959**	**0.985**	**0.959**	**0.997**	0.892	0.997	-0.795	**0.994**	**1.000**
${}^{m}T_3$ (G)	**-0.837**	0.876	0.944	0.876	0.967	0.915	**0.968**	**-0.827**	0.989	0.972
${}^{m}T_2$ (G)	-0.774	0.798	0.895	0.798	0.918	**0.920**	0.918	-0.815	0.955	0.927



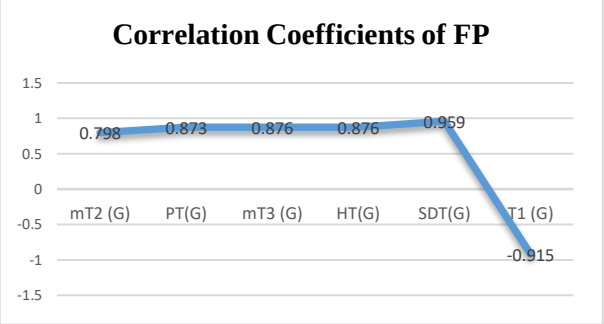
(a) DE on TI



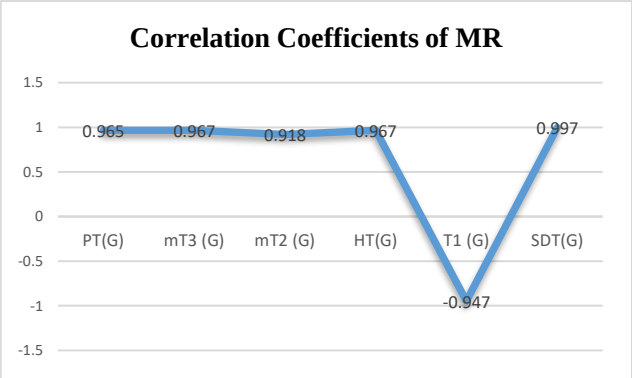
(b) BP on TI



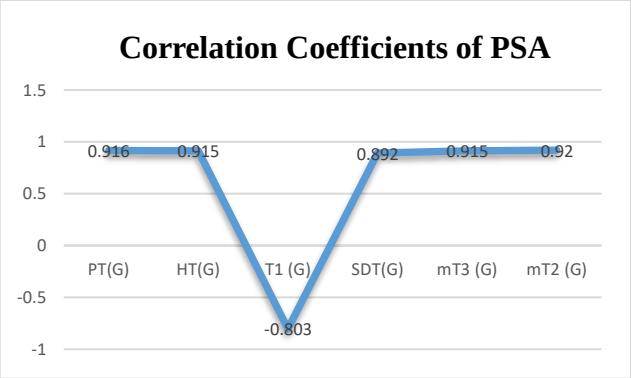
(c) EN on TI



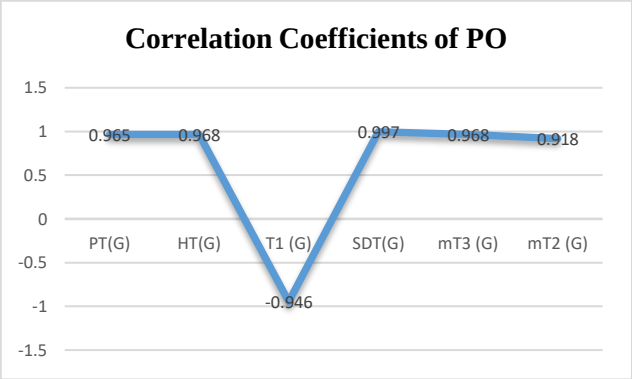
(d) FP on TI



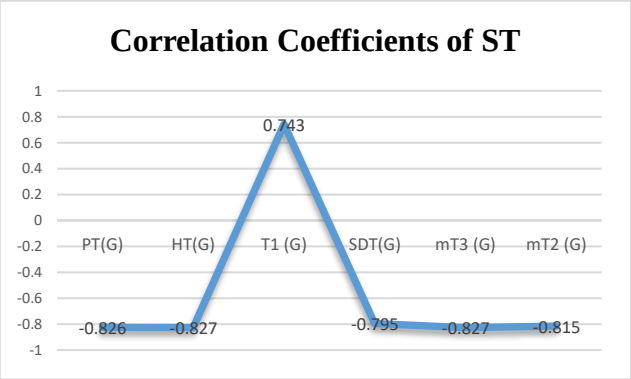
(e) MR on TI



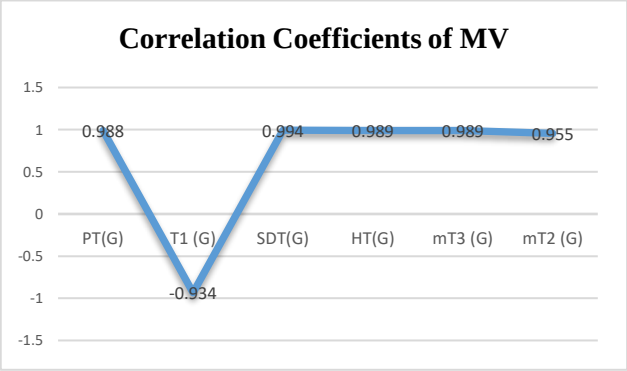
(f) PSA on TI



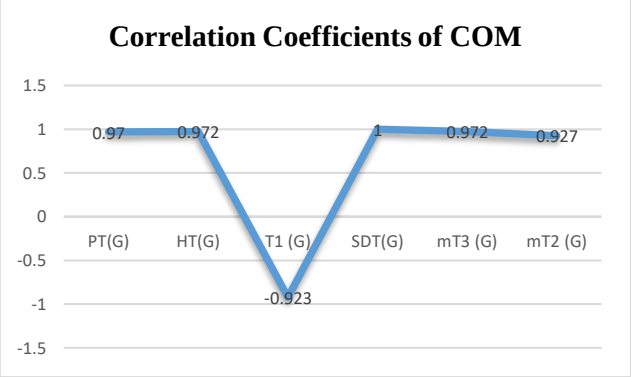
(g) PO on TI



(h) ST on TI



(i) MV on TI



(j) COM on TI

Figure 3: Physicochemical properties with TI.

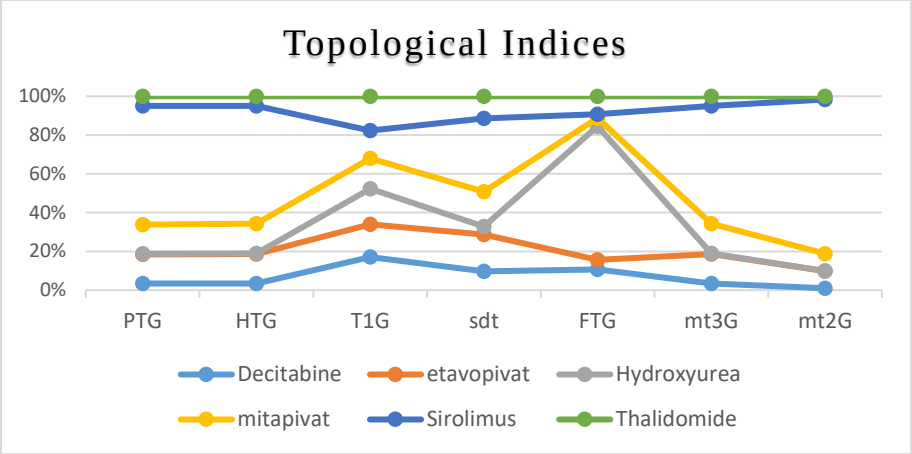


Figure 4: Two-dimensional (2D) graph illustrating the relationship between drugs and their topological indices.

Table 7 Linear Regression-Based QSPR Analysis for Predicting PT (G).

PHYSICAL PROPERTIES	N	A	B	R	R^2	SE	F	P	INDICATOR
DE	6	.000293	1.699	.833	.694	.079	9.080	.000	Significant
BP	6	.324	429.564	.873	.762	73.092	12.820	.004	Significant
EN	6	.049	73.143	.942	.887	7.133	31.481	.001	Significant
FP	6	.196	213.585	.873	.762	44.210	12.821	.008	Significant
MR	6	.114	44.694	.965	.932	12.487	54.848	.002	Significant
PSA	6	.057	85.630	.916	.839	10.133	20.920	.001	Significant
PO	6	.045	17.738	.965	.932	4.944	54.956	.002	Significant
ST	6	-.017	82.536	.826	.682	4.631	8.586	.000	Significant
MV	6	.374	97.955	**.988**	**.976**	23.937	159.510	.000	Significant
COM	6	.833	276.305	.970	.941	84.065	64.200	.001	Significant
The significance of bold numbers denotes highest correlation value									

Table 8 Linear Regression-Based QSPR Analysis for Predicting HT (G).

PHYSICAL PROPERTIES	N	A	B	R	R^2	SE	F	P	INDICATOR
DE	6	.00031	1.700	.837	.700	.078	9.335	.000	Significant
BP	6	.344	427.650	.876	.768	72.436	13.233	.004	Significant
EN	6	.052	72.901	.944	.890	7.059	32.455	.000	Significant
FP	6	.208	212.427	.876	.768	43.814	13.234	.008	Significant
MR	6	.121	44.112	.967	.936	12.156	58.485	.002	Significant
PSA	6	.061	85.448	.915	.837	10.252	20.497	.001	Significant
PO	6	.048	17.507	.968	.936	4.813	58.601	.002	Significant
ST	6	-.018	82.610	.827	.683	4.637	8.632	.000	Significant
MV	6	.396	96.218	**.989**	**.978**	22.786	177.578	.000	Significant
COM	6	.883	272.274	.972	.944	82.097	67.955	.001	Significant
The significance of bold numbers denotes highest correlation value									

Table 9 Linear Regression-Based QSPR Analysis for Predicting T_1 (G).

PHYSICAL PROPERTIES	N	A	B	R	R^2	SE	F	P	INDICATOR
DE	6	.377	-.708	.792	.627	.874	6.719	.061	Significant
BP	6	-458.860	3344.498	.915	.838	606.513	20.697	.005	Significant
EN	6	-65.044	488.170	.916	.838	85.903	20.731	.005	Significant
FP	6	-277.561	1976.805	.915	.838	366.821	20.703	.006	Significant
PSA	6	-67.922	521.875	.803	.645	151.534	7.265	.026	Significant
PO	6	-60.069	400.825	**.946**	**.896**	61.653	34.326	.003	Significant
ST	6	20.409	-48.321	.743	.552	55.301	4.925	.091	Significant
MV	6	-477.917	3152.582	.934	.872	550.630	27.240	.005	Significant
COM	6	-1071.937	7124.814	.923	.853	1339.476	23.158	.006	Significant
The significance of bold numbers denotes highest correlation value									

Table 10 Linear Regression-Based QSPR Analysis for Predicting SDT (G).

PHYSICAL PROPERTIES	N	A	B	R	R^2	SE	F	P	INDICATOR
DE	6	-.004	1.850	.865	.747	.103	11.835	.000	Significant
BP	6	4.830	243.290	.959	.920	61.184	46.189	.002	Significant
EN	6	.702	47.272	.985	.969	5.384	126.218	.001	Significant
FP	6	2.921	100.911	.959	.920	37.007	46.194	.002	Significant
MR	6	1.604	-13.657	.997	.994	5.526	624.283	.000	Significant
PSA	6	.758	59.721	.892	.795	16.538	15.558	.017	Significant
PO	6	.636	-5.387	.997	.994	2.172	634.345	.000	Significant
ST	6	-.219	89.933	.795	.631	7.214	6.847	.000	Significant
MV	6	5.111	-83.304	.994	.989	23.544	349.384	.000	Significant
COM	6	11.655	-146.928	**1.000**	**.999**	12.818	6129.072	.000	Significant
The significance of bold numbers denotes highest correlation value									

Table 11 Linear Regression-Based QSPR Analysis for Predicting ${}^{m}T_3$ (G).

PHYSICAL PROPERTIES	N	A	B	R	R^2	SE	F	P	INDICATOR
DE	6	-.001	1.700	.837	.700	.078	9.335	.000	significant
BP	6	.688	427.650	.876	.768	72.436	13.233	.004	significant
EN	6	.105	72.901	.944	.890	7.059	32.455	.000	significant
FP	6	.416	212.427	.876	.768	43.814	13.234	.008	significant
MR	6	.243	44.112	.967	.936	12.156	58.485	.002	significant
PSA	6	.121	85.448	.915	.837	10.252	20.497	.001	significant
PO	6	.096	17.507	.968	.936	4.813	58.601	.002	significant
ST	6	-.036	82.610	.827	.683	4.637	8.632	.000	significant
MV	6	.793	96.218	.989	**.978**	22.786	177.578	.000	significant
COM	6	1.767	272.274	.972	.944	82.097	67.955	.001	significant
The significance of bold numbers denotes highest correlation value									

Table 12 Linear Regression-Based QSPR Analysis for Predicting ${}^{m}T_2$ (G).

PHYSICAL PROPERTIES	N	A	B	R	R^2	SE	F	P	INDICATOR
DE	6	-8.834E-6	1.651	.774	.599	.081	5.978	.000	significant
BP	6	.010	483.872	.798	.637	81.640	7.022	.004	significant
EN	6	.002	80.791	.895	.801	8.573	16.078	.001	significant
FP	6	.006	246.434	.798	.637	49.381	7.022	.008	significant
MR	6	.004	62.349	.918	.842	17.214	21.315	.010	significant
PSA	6	.002	93.346	.920	.846	8.979	21.941	.000	significant
PO	6	.001	24.734	.918	.842	6.818	21.343	.010	significant
ST	6	-.001	80.169	.815	.664	4.307	7.900	.000	significant
MV	6	.012	153.417	**.955**	**.912**	41.113	41.313	.003	significant
COM	6	.026	403.320	.927	.860	117.605	24.487	.008	significant
The significance of bold numbers denotes highest correlation value									

5 CONCLUSION

Table 6 and Figure 3 visualize the correlations between the physical and chemical properties of Thalassemia drugs and the corresponding temperature indices. Figure 4 presents a graphical representation of the correlations between topological indices (TI) and drugs.

The Sum connectivity temperature index exhibits a positive correlation with BP (r =0.952), EN (r =0.985), FP (r =0.959), MR (r =0.997), MV (r =0.994), and demonstrates the highest correlation with COM (r =1.000). Furthermore, the modified third temperature index exhibits a positive correlation with PO (r =0.968) and the highest inverse correlation coefficient with DE and ST. Moreover, the Harmonic temperature index demonstrates a positive correlation with the PO (r =0.968) and inverse correlation coefficient for ST. Lastly, the modified second temperature index exhibits a highly significant positive correlation with PSA (r =0.920).

We observe a positive correlation between the physicochemical properties of Thalassemia drugs and temperature indices. Tables 7-12 present regression models for various physicochemical properties. The results demonstrate correlation coefficients (r) exceeding 0.6, with p-values below 0.05, indicating robust predictors for linear regression. Equations are derived based on criteria such as minimizing standard error (SE), maximizing R^2, and maximizing the F-statistic. Therefore, it can be inferred that all physicochemical properties hold significant importance. This underscores the potential relevance of these topological indices in QSPR analysis for Thalassemia drugs, and the plotted regression line can be observed. The findings of this study can aid in the production, development, and enhancement of more effective Thalassemia drugs. Additionally, the methodology employed in this study can be applied to explore other drug structures. In addition, in this study, the math library in Python was used for mathematical computations. For example, the PT(G) index was calculated using this library. Other indices are calculated in a similar manner using this library as well (Python Software Foundation, Python 3.12, 2024).

https://drive.google.com/file/d/1e_b84Olw8EWEyoH8XXC3OyxLa_8cXZ8-/view?usp=sharing

REFERENCES

[1] A. Jahanbani, R. Khoeilar, and M. Cancan, "On the Temperature Indices of Molecular Structures of Some Networks," J. Math., vol. 2022, pp. 1–7, 2022.

[2] B. Lučić and N. Trinajstić, "New developments in QSPR/QSAR modeling based on topological indices," SAR and QSAR in Environmental Research, vol. 7, pp. 45–62, 1997.

[3] J. Ramezani Tousi and M. Ghods, "Computing K Banhatti and K Hyper Banhatti Indices of Titania Nanotubes TiO2[m, n]," J. Inf. Optim. Sci., vol. 44, pp. 207–216, 2023.

[4] J.Ramezani Tousi and M. Ghods, "Investigating Banhatti indices on the molecular graph and the line graph of Glass with M-polynomial approach," Proyecciones J. Math., vol. 43, pp. 199–219, 2024.

[5] J. Ramezani Tousi and M. Ghods, "Some polynomials and degree-based topological indices of molecular graph and line graph of Titanium dioxide nanotubes," J. Inf. Optim. Sci., vol. 45, pp. 95–106, 2024.

[6] L. Huang, Y. Wang, K. Pattabiraman, P. Danesh, M. K. Siddiqui, and M. Cancan, "Topological indices and QSPR modeling of new antiviral drugs for cancer treatment," Polycycl. Aromat. Compd., vol. 43, pp. 8147–8170, 2023.

[7] M. Ghods and J. Ramezani Tousi, "Computing Revan Polynomials and Revan Indices of Copper (I) Oxide and Copper (II) Oxide," Commun. Combin. Cryptogr. Comput. Sci., vol. 1, pp. 50–58, 2021.

[8] M. Ghorbani and M. A. Hosseinzadeh, "A new version of Zagreb indices," Filomat, vol. 26, pp. 93–100, 2012.

[9] N. Kansal, P. Garg, and O. Singh, "Temperature-based topological indices and QSPR Analysis of COVID-19 Drugs," Polycycl. Aromat. Compd., vol. 43, pp. 4148–4169, 2023.

[10] Ö. Ç. Havare, "Quantitative structure analysis of some molecules in drugs used in the treatment of COVID-19 with topological indices," Polycycl. Aromat. Compd., vol. 42, pp. 5249–5260, 2022.

[11] R. HosseiniEshpala, M. Langarizadeh, M. KamkarHaghighi, and T. Banafsheh, "Designing an expert system for differential diagnosis of β-Thalassemia minor and Iron-Deficiency anemia using neural network," Hormozgan Med. J., vol. 20, pp. 1–9, 2010.

[12] R. Natarajan, "New topological indices with very high discriminatory power," SAR and QSAR in Environmental Research, vol. 22, pp. 1–20, 2011.

[13] S. Killip, J. M. Bennett, and M. D. Chambers, "Iron deficiency anemia," Am. Fam. Physician, vol. 75, pp. 671–678, 2010. Available at: PubMed [Google Scholar].

[14] S. Kosari, "On spectral radius and Zagreb Estrada index of graphs," Asian-Eur. J. Math., vol. 16, pp. 4167, 2023.

[15] S. Kosari, N. Dehgardi, and A. Khan, "Lower bound on the KG-Sombor index," Commun. Combin. Optim., vol. 8, pp. 751–757, 2023.

[16] S. Fajtolowicz, "On conjectures of Graffitti," Discrete Math., vol. 72, pp. 113–118, 1988.

[17] S. F. Clark, "Iron deficiency anemia," Nutr. Clin. Pract., vol. 23, pp. 128–141, 2010. Available at: PubMed [Google Scholar].

[18] V. R. Kulli, "Computation of Some Temperature Indices of $HC_5C_5[p, q]$ Nanotubes," Ann. Pure Appl. Math., vol. 20, pp. 69–74, 2019.

[19] V. R. Kulli, "Inverse sum temperature index and multiplicative inverse sum temperature index of certain nanotubes," Int. J. Recent Sci. Res., vol. 12, pp. 40635–40639, 2021.

[20] V. R. Kulli, M. Pal, S. Samanta, and A. Pal, Handbook of Research of Advanced Applications of Graph Theory in Modern Society, Hershey, USA: Global, 2020.

[21] X. Shi, S. Kosari, S. Hameed, A. G. Shah, and S. Ullah, "Application of connectivity index of cubic fuzzy graphs for identification of danger zones of tsunami threat," PLoS ONE, vol. 19, pp. 1–24, 2024.

[22] Y. Zhang, A. Khalid, M. K. Siddiqui, H. Rehman, M. Ishtiaq, and M. Cancan, "On analysis of temperature based topological indices of some Covid-19 drugs," Polycycl. Aromat. Compd., vol. 43, pp. 3810–3826, 2023.

[23] Z. Yılmaz and M. R. Bozkurt, "Determination of women iron deficiency anemia using neural networks," J. Med. Syst., vol. 36, pp. 2941–2945, 2010. Available at: PubMed [Google Scholar].

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

I4CPAPERS-058

Design and Implementation of a Persian Chatbot for Legal Service Applications

Sharifeh Abbaszadeh, Fahimeh Ghasemian
Department of Computer Engineering, Faculty of Engineering, Shahid Bahonar University of Kerman, Kerman, Iran
shabbaszadeh@eng.uk.ac.ir ; ghasemianfahime@uk.ac.ir

ABSTRACT

Chatbots are sophisticated tools that utilize natural language processing to generate clear and comprehensible responses. They have found extensive applications across various service domains, particularly in legal matters. Legal texts are often complex and intricate, making them challenging for many individuals to understand without specialized legal knowledge. Furthermore, consulting a lawyer can sometimes be neither cost-effective nor time efficient. This paper presents the development of a Persian legal chatbot, specifically focusing on family law. By leveraging recent advancements in large language models, our approach emphasizes fine-tuning the Mistral language model using the QLora method, trained on a dataset collected from family court legal texts. Evaluation results demonstrate that this model exhibits high efficiency in addressing legal inquiries in Persian related to family law, thereby potentially mitigating issues arising from a lack of legal awareness within society.

KEYWORDS: Chatbots, Natural Language Processing, Family Law, Persian Language Processing, Legal Services

1 INTRODUCTION

Chatbots represent a significant advancement in artificial intelligence, enabling users to engage in conversational interactions with computer systems. These tools leverage natural language processing (NLP) algorithms and deep learning techniques to understand and respond to user inquiries effectively. In Iran, the deployment of chatbots has gained traction, providing valuable services across various domains and addressing a wide array of user questions through sophisticated linguistic algorithms. The growing adoption of chatbots is attributed to their ability to enhance communication, increase productivity, and improve user experience in diverse sectors, including customer service, education, healthcare, and online retail.

The concept of “legal technology” is increasingly recognized in both Iranian and global legal literature, encompassing the provision of legal services and solutions through technology and online platforms. This field encompasses a diverse range of applications, including legal consulting, documentation management, intelligent evidence gathering, electronic document collection, and comprehensive case management systems.

Legal texts, often characterized by their complexity and technicality, pose significant challenges for individuals lacking specialized legal training [1]. This complexity can hinder access to justice and legal understanding, leading to potential legal pitfalls for those unaware of their rights and obligations.

A promising application of legal technology is the development of chatbots specifically designed to provide rapid responses to legal inquiries. For many individuals, navigating intricate legal texts can be

overwhelming, and traditional consultations with lawyers may not always be feasible due to time constraints or financial considerations. Legal chatbots can bridge this gap by interpreting legal questions and extracting pertinent information from legal texts, thereby mitigating issues arising from a lack of legal awareness. Globally, various legal chatbots are already providing essential information, advice, and assistance to users navigating legal issues. Noteworthy examples include Legal Master AI [2], LawBot [3], Luminance [4], Legal Robot [5], and Kira System [6], each contributing to the evolving landscape of legal technology.

This paper contributes to this field by presenting the development of a Persian legal chatbot focused uniquely on family law. Our methodology involves fine-tuning the Mistral language model using the QLora technique, trained on a dataset derived from family court legal texts. By leveraging advancements in large language models, we aim to enhance the chatbot's ability to address legal inquiries effectively in Persian, providing a tailored solution that reflects the nuances of family law within the Iranian legal context.

The introduction of such a legal chatbot can serve multiple purposes:

-Facilitating easy access to legal information, empowering individuals to obtain answers to their legal questions efficiently.

-Reducing the incidence of legal misunderstandings and issues stemming from ignorance of the law.

-Minimizing the time and financial burden associated with consulting legal professionals.

The paper is structured as follows: we first review related work in the domain of legal chatbots, highlighting key advancements. Next, we present the proposed method for developing the Persian legal chatbot, detailing the model selection and training processes. Following this, we outline the evaluation metrics used to assess the chatbot's performance and present the results of our findings. Finally, we conclude with a discussion of the implications of our work and suggestions for future research directions in legal technology.

2 RELATED WORK

The history of conversational bots dates back more than half a century [7], starting with the creation of Eliza by Joseph Weizenbaum in 1966. Eliza was capable of answering users' questions and simulating a form of psychotherapy. This program marked a significant milestone in the history of artificial intelligence and human-computer interactions.

The 2000s brought notable advancements with the emergence of AIML and bots like A.L.I.C.E, which received various awards. The 2010s witnessed the rise of personal assistants such as Siri, Google Assistant, and Alexa, which utilized natural language processing and more sophisticated algorithms to facilitate more human-like interactions [8]. Since 2018, advanced models like GPT-3 have emerged, demonstrating exceptional capabilities in understanding and generating language. Today, conversational bots are integrated into various applications, including Siri, Alexa, and Cortana, and it is projected that the market for this technology will exceed $1.34 billion by 2024 [9].

Conversational bots can be categorized into several main types:

1. **Rule-based Bots**: These bots operate based on a predefined set of rules and patterns. They are typically suited for answering specific, straightforward questions [10].
2. **Retrieval-based Bots**: This type of bot uses a database of pre-written responses and selects the best answer based on user input [8].
3. **Generative Bots**: These bots utilize deep learning models to generate new responses, allowing them to reply in a more natural and varied manner [10].

Several approaches for implementing chatbots have been discussed in various articles:

- **Machine Learning-based Models**: These models employ machine learning algorithms for natural language analysis and processing, utilizing architectures such as Long Short-Term Memory (LSTM) or Gated Recurrent Units (GRUs) for processing text sequences [11].
- **Transformer Models**: Models like BERT and GPT are highly regarded for their superior capabilities in understanding and generating natural language, making them especially prominent in the implementation of conversational bots [10].

- **Dialogue-based Systems**: These systems are designed to manage multi-turn conversations and maintain conversational context. They can leverage reinforcement learning techniques to enhance interactions [12].

Conversational bots have become increasingly popular in the judicial domain due to their ability to automate and streamline processes [13]. This technology has multiple applications, including precise data collection, criminal identification, estimating the likelihood of recidivism, and ensuring fair judgment. Artificial intelligence can assist judges in their decision-making by analyzing a defendant's criminal history and assessing the probability of reoffending.

An example of such a bot is "DoNotPay," created by Joshua Browder, which assists users with legal claims. However, this bot operates without a legal license, resulting in criticism. Browder asserts that the bot merely provides information and guidance, helping thousands of individuals who lack access to traditional legal services. Overall, intelligent legal bots are recognized as reliable tools for legal consultation and assisting attorneys in these matters. By utilizing advanced algorithms, they contribute to resolving legal issues with greater accuracy and speed.

Currently, Iran's judicial centers operate according to traditional systems and methods, with little to no application of artificial intelligence. The judiciary's desire, particularly among courts, to adopt artificial intelligence technology is evident, and necessary infrastructure must be established.

Several legal chatbots exist in Iran that offer various services. Some of these services include:

- **Answering Legal Questions**: Chatbots can respond to users' legal inquiries and provide them with legal information.
- **Drafting Legal Documents**: Some chatbots can prepare and drafting legal documents such as contracts and wills.
- **Legal Consultation**: Chatbots can provide users with legal advice and guide them regarding their rights and obligations.
- **Responding to Inquiries About Laws and Regulations**: Chatbots can answer users' questions concerning Iranian laws and regulations.

Some notable examples of the use of bots in legal matters in Iran include:

- **Vakilbashi**: is an Iranian legal chatbot that leverages artificial intelligence to assist users in navigating legal questions and issues. It is designed to provide accessible legal advice in Persian, making it easier for users to understand their rights and legal responsibilities [14].
- **Botava**: A Persian legal chatbot that utilizes artificial intelligence to answer legal questions.

Overall, legal chatbots in Iran can offer various legal services, assisting users in accessing legal information and benefiting from legal services although their numbers remain limited [15].

3 PROPOSED METHOD

In this section, the proposed method for developing a legal chatbot in the field of family law is examined. This method utilizes the Mistral large language model, which has been fine-tuned on the collected dataset using the QLoRa technique. Various techniques exist for fine-tuning models, which can enhance performance and efficiency in specific tasks. The choice of the appropriate technique depends on the type of data, the project's objectives, and the available resources. Figure 1 presents an overview of the proposed method for developing the conversational bot.

For the development of the chatbot, the Mistral large language model was utilized. The Mistral-7B-Instruct-v0.2 model is a seven billion parameter model developed by Mistral, a prominent artificial intelligence research company. This model quickly gained attention due to its high quality and efficiency [16].

Key features of the Mistral models include a novel attention mechanism, which allows for faster inference, and an effective management of longer sequences that reduces computational costs. These innovations contribute to the overall enhanced performance and efficiency of the model. The Mistral architecture is based on the transformer model, featuring characteristics like those found in LLaMA language models.

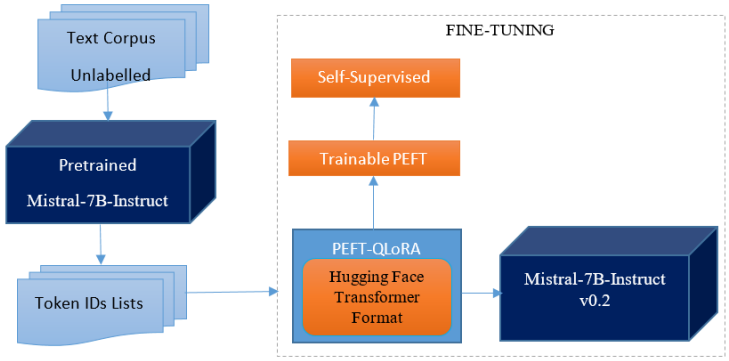


Figure 1: Diagram of the proposed method

In the following, we explain the phases involved in developing a legal chatbot, focusing on data collection, data preparation, and fine-tuning a language model. Each phase plays a crucial role in ensuring the chatbot functions effectively and provides accurate legal information.

- Phase 1: Data Collection

Collecting raw data is the initial step in the data processing cycle, and the type of data gathered significantly impacts the final output. To ensure the quality of the output, data must be sourced from reputable references. In this study, data were collected from two primary sources: a collection of legal questions sourced from the internet, and a set of questions and answers extracted from the text of the Family Court Support Law, which was retrieved from the official website of the Iranian Parliament [17]. Ultimately, a total of 16,184 questions and answers were compiled. To ensure compatibility with the Mistral model, all training data underwent consistent preprocessing. This process included text normalization, sentence segmentation, and tokenization using a subword tokenizer that was also utilized during the pre-training and fine-tuning stages. This approach ensures that the model operates on a uniform representation at the subword level across all data, facilitating fair comparisons.

- Phase 2: Data Preparation

Data preparation or cleansing involves the removal of unnecessary and low-quality data, which contributes to improved model performance. This phase pertains to the preprocessing of data and includes the cleaning and transformation of raw text data into an appropriate format for analysis and modeling.

  - Noise Removal: Text data typically contains noise such as punctuation marks, numbers, and abbreviations, which can adversely affect model accuracy.
  - Tokenization: This process entails breaking the text into meaningful units (words, phrases). For this phase, the Byte Pair Encoding (BPE) tokenizer of the Mistral model was employed, assisting in the management of out-of-vocabulary tokens. This transforms the text into a numerical format that machine learning models can interpret.

- Phase 3: Fine-Tuning the Mistral Language Model

The primary goal of fine-tuning the model for the Persian language is to enhance its performance and accuracy. The training process for large language models is challenging due to its complexity and the requirement for powerful computational resources. The success of this training relies on various factors, including the quality and volume of the dataset, the model architecture, and the training parameters.

For the fine-tuning process, we employed Quantized Low-Rank Adaptation (QLoRA), which optimizes the model by reducing the precision of weight parameters to 4 bits. This method is particularly beneficial in scenarios with limited memory, as it decreases the model size while allowing for effective fine-tuning of large language models [18].

4 EVALUATION AND RESULT

During the fine-tuning process of the Mistral model, we utilized the Tesla A100-SXM4-40GB GPU for a duration of 2 hours. The configuration for fine-tuning included the following parameters:

Table 1: The Value of Parameters During the Fine-Tuning Process

LoRA_alpha	8
LoRA_dropout	0.1
LoRA_rank	16
bias	None
Other parameters	
num_train_epochs	1
per_device_train_batch_size	2
gradient_accumulation_steps	1
optimizer	paged_adamw
learning_rate	5e-4
fp16	True
max_grad_norm	0.3
warmup_ratio	0.01
max_length	4k
lr_scheduler_type	constant

To evaluate the performance of the model, we utilized the BLEU (Bilingual Evaluation Understudy) score, a widely accepted metric for assessing the quality of text produced by machine translation and other natural language processing tasks. The BLEU score quantifies the overlap between n-grams in the produced text and a set of reference texts, ranging from 0 to 1; a higher score indicates greater correspondence between the two [19]. Additionally, BLEU applies a brevity penalty to prevent the generation of overly short translations. BLEU-1 specifically measures the overlap of unigrams (single words) between the machine-generated translation and one or more reference translations.

The metric is calculated as the geometric mean of the accuracy scores for 1-grams:

$$\text{BLEU-1}=\text{BP}\times\text{Precision} \quad (1)$$

The results of our evaluation, which included various models for comparison and were fine-tuned using the gathered dataset, are summarized in Table 2:

Table 2: Comparison of Different Models Based on BLEU

BLEU	**Model**
0.21	google/mt5-base
0.11	google/mt5-small
0.23	google/mt5-large
0.40	Helsinki-NLP
0.42	Mistral /Mistral-7B-Instruct-v0.2

The BLEU scores indicate that our implemented Mistral model, fine-tuned for the domain of family law, achieved a BLEU score of 0.42. This score positions the Mistral model as the best-performing model among those evaluated in this study, surpassing others such as the Helsinki-NLP model at 0.40 and various configurations of Google's T5 and mT5 models.

Our finetuned Mistral model's score reflects its effectiveness in generating coherent and contextually relevant responses in legal language, particularly in the family law domain. The application of QLoRA, which allows for efficient model training with reduced memory usage, likely contributed to the enhanced performance by enabling more effective learning on the dataset.

5 CONCLUSION

In this research, an effort was made to develop a conversational bot for legal services in the Persian language. To achieve this goal, the fine-tuning of large language models was employed, as it is the most effective method for implementing a conversational bot. Using the QLoRa quantization technique, the Mistral language model was fine-tuned on a Persian text dataset that was collected for this study. The results obtained from the comparison and evaluation with other methods indicated that the proposed approach demonstrated higher performance based on the Blue metric compared to alternative methods. Future work may involve further optimizing hyperparameters, increasing the training data coverage, and exploring additional evaluation metrics to enhance and validate model performance further.

REFERENCES

[1] Bahman Capital, "Legal Tech | Helsinki University," [Online]. Available: http://bahmancapital.com/legal-tech-helsinki-university. [Accessed: Nov. 27, 2024].

[2] Legal Master AI, "LegalMaster AI," [Online]. Available: https://legalmasterai.com. [Accessed: Nov. 27, 2024].

[3] LawBot Pro, "LawBotPro," [Online]. Available: https://lawbotpro.com. [Accessed: Nov. 27, 2024].

[4] Luminance, "Luminance," [Online]. Available: https://www.luminance.com/. [Accessed: Nov. 27, 2024].

[5] Top Apps, "Legal Robot," [Online]. Available: https://topapps.ai/ai-apps/legal-robot. [Accessed: Nov. 27, 2024].

[6] Kira Systems, "Kira Systems," [Online]. Available: https://kirasystems.com/. [Accessed: Nov. 27, 2024].

[7] W. Huang, K. F. Hew, and L. K. Fryer, "Chatbots for language learning—Are they really useful?," Journal of Computer Assisted Learning, vol. 38, no. 1, pp. 237-257, 2021.

[8] K. Ramesh, S. Ravishankaran, A. Joshi, and K. Chandrasekaran, "A survey of design techniques for conversational agents," in Proc. International Conference on Information, Communication and Computing Technology, 2017, pp. 336-350.

[9] K. Elkins and J. Chun, "Can GPT-3 pass a writer's Turing test?," Journal of Cultural Analytics, vol. 5, no. 2, 2020.

[10] G. Caldarini, S. Jaf, and K. McGarry, "A literature survey of recent advances in chatbots," Information, vol. 13, no. 1, p. 41, 2022.

[11] M. Nuruzzaman and O. K. Hussain, "A survey on chatbot implementation in customer service industry through deep neural networks," in Proc. 2018 IEEE 15th International Conference on E-Business Engineering (ICEBE), Oct. 2018, pp. 54-61.

[12] N. Shakhovska, O. Basystiuk, and K. Shakhovska, "Development of the Speech-to-Text Chatbot Interface Based on Google API," in Proc. MoMLeT, May 2019, pp. 212-221.

[13] Judicial Applications of AI, [Online]. Available: https://cipg.ir/judicial-applications-of-ai/. [Accessed: Nov. 27, 2024].

[14] Vakilbashi, "Lawyers," [Online]. Available: https://vakilbashi.org/lawyers. [Accessed: Nov. 27, 2024].

[15] Amerandish, "Botava," [Online]. Available: https://amerandish.com/botava. [Accessed: Nov. 27, 2024].

[16] A. Q. Jiang, A. Sablayrolles, A. Mensch, C. Bamford, D. S. Chaplot, D. D. L. Casas, and W. E. Sayed, "Mistral 7B," arXiv preprint arXiv:2310.06825, 2023.

[17] Iranian Parliament, "Judicial Applications of AI," [Online]. Available: https://rc.majlis.ir/fa/law/show/840814. [Accessed: Nov. 27, 2024].

[18] E. J. Hu et al., "LoRA: Low-rank adaptation of large language models," arXiv preprint arXiv:2106.09685, 2021.

[19] K. Papinesi, "BLEU: A method for automatic evaluation of machine translation," in Proc. 40th Annual Meeting of the Association for Computational Linguistics *(ACL)*, 2002, pp. 311-318.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A QSPR Study Employing Degree-Based Topological Indices and Regression Modelling of Some Poisons

Shabnam Homam, Masoud Ghods
Semnan University
Department of Applied Mathematics, Semnan University, Semnan 35131-19111, Iran
ShabnamHomam@semnan.ac.ir; mghods@semnan.ac.ir

ABSTRACT

This study employed M-polynomials to calculate topological indices based on degree for a set of commonly used poisons, including Abrine, Aconitine, Atropine, Carfentanil, Cocaine, Fentanyl, Heroin, Ketamine, Methamphetamine, Morphine, Nicotine, Quinine, Ricinin, Sarin, Scopolamine, Strychnidin, and VX. These indices were integrated into QSPR models to predict diverse compound properties. Our analysis demonstrates that the developed regression models effectively predict these physicochemical properties using topological indices as predictors. The findings demonstrate the potential of topological indices as valuable tools for designing and optimizing poisons, supported by statistically significant results ($p < 0.05$).
KEYWORDS: Topological indices, M-polynomial, Quantitative structure-property relationship (QSPR), poisons.

1 INTRODUCTION

A poison is any substance that, when introduced into or absorbed by a living organism, inflicts harm by either causing fatality or compromising health. Toxicology, the scientific study of poisons, examines the adverse effects of chemical or physical agents on living organisms. These adverse effects can manifest in various forms, ranging from immediate fatality to subtle changes that may remain undetected for months or even years. The effects of poisons can be acute, meaning they can induce sudden and severe adverse outcomes shortly after exposure. Chronic toxicity is characterized by adverse effects that arise from prolonged or repeated exposure over an extended period. For instance, a poison may initially impact the nervous system following acute exposure but target the liver during chronic exposure.[1]

QSPR analysis has become an indispensable computational tool in drug discovery and design. This growing interest has spurred advancements in chemical graph theory, which explores the relationships between molecular structure, properties, and activity. Molecular graphs represent molecules as networks of atoms (vertices) connected by chemical bonds (edges). Topological indices, mathematical descriptors of these graphs, are used to analyze molecular structure and properties. [2,3]. A fundamental approach to exploring the relationships between physicochemical properties and topological indices (TIs) involves quantitative structure-property relationship (QSPR) modelling. These models employ regression analysis to establish correlations between physicochemical properties and their

corresponding molecular descriptors. Similarly, quantitative structure-activity relationship (QSAR) studies frequently employ topological indices (TIs) to analyze drug activity. [4,5,6]. This research aims to investigate the application of diverse topological indices to elucidate the relevant physicochemical properties and potential chemical reactivity of poisons. Contemporary research extensively employs quantitative structure-property relationship (QSPR) and quantitative structure-activity relationship (QSAR) models, in conjunction with M-polynomial indices, to predict the physical or chemical characteristics of compounds based on their molecular connectivity descriptors. This procedure has found widespread application in various scientific disciplines, including cancer research, nanotube studies, and the investigation of M-polynomials. It effectively communicates the recent research focus on the relationship between M-polynomials and topological indices. [7,8,9,10].

2 GRAPH-THEORETICAL PRELIMINARIES

A molecular graph is a graphical representation of the structure of a chemical compound, utilizing principles of graph theory. Atoms are depicted as vertices, and bonds as edges in a simple, finite, and connected graph G (V, E). The degree of a vertex, d(v), corresponds to the valence of the atom it represents. For a more comprehensive understanding, please refer to the cited references. [11,12]. A connectivity index is a numerical descriptor that quantifies the structural properties of a graph. It is calculated solely from the graph's topology, which refers to the arrangement of vertices and edges, independent of the graph's spatial embedding. It provides a quantitative representation of the arrangement of atoms and their connectivity within a molecule and is employed in the development of quantitative structure-activity relationship (QSAR) and quantitative structure-property relationship (QSPR) models. Three primary categories of structural descriptors exist: degree-based, distance-based, and spectral. Among these, degree-based connectivity indices have been extensively studied and exhibit a strong correlation with a wide range of molecular properties. The M-polynomial was introduced by S. Klavžar and E. Deutsch in 2015.

2.1 Equations

Some Connectivity descriptors based on Degree Define as below:

$$M_1(G) = \sum_{uv \in E(G)} (d_u + d_v) \tag{1}$$

$$M_2(G) = \sum_{uv \in E(G)} (d_u . d_v) \tag{2}$$

$$M_3(G) = \sum_{uv \in E(G)} |d_u - d_v| \tag{3}$$

$$H_1M(G) = \sum_{uv \in (G)} (d_u + d_v)^2 \tag{4}$$

$$H_2M(G) = \sum_{uv \in E(G)} (d_u . d_v)^2 \tag{5}$$

$$H(G) = \sum_{uv \in E(G)} \frac{2}{d_u + d_v} \tag{6}$$

$$ABC(G) = \sum_{uv \in E(G)} \sqrt{\frac{d_u + d_v - 2}{d_u . d_v}} \tag{7}$$

$$F(G) = \sum_{uv \in E(G)} \left[(d_u)^2 + (d_v)^2 \right] \quad (8)$$

$$R(G) = \sum_{uv \in E(G)} \sqrt{\frac{1}{d_u . d_v}} \quad (9)$$

$$SCI(G) = \sum_{uv \in E(G)} \sqrt{\frac{1}{d_u + d_v}} \quad (10)$$

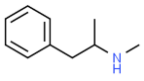
$$GA(G) = \sum_{uv \in E(G)} \frac{2\sqrt{d_u . d_v}}{d_u + d_v} \quad (11)$$

$$So(G) = \sum_{uv \in E(G)} \sqrt{(d_u)^2 + (d_v)^2} \quad (12)$$

$$M(G; x, y) = \sum_{i \le j} m_{ij}(G) x^i y^j \quad (13)$$

2.2 Methodology

Theorem 1. Let M represent the graph of Methamphetamine

(a) 

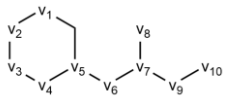
(b) 

Figure1.Chemical Structure (a) and Chemical Graph (b) of Methamphetamine

Then:

i. $M_1(G)=48$
ii. $M_2(G)=51$
iii. $M_3(G)=8$
iv. $HM_1(G)=214$
v. $HM_2(G)=257$
vi. $H(G)=5.17$
vii. $ABC(G)=7.8$
viii. $F(G)=112$
ix. $R(G)=5.3$
x. $SCI(G)=5.31$
xi. $GA(G)=10.71$
xii. $SO(G)=34.74$

Proof. Consider M as the graph of Methamphetamine, featuring an edge set E, let $E_{u,v}$ represents the category of edges of M linking vertices of degrees u and v through , $|E_{1,2}|=1, |E_{1,3}|=1$ $|E_{2,2}|=4$, $|E_{2,3}|=5$.

By using the Definition above-given edge partitions $E_{u,v}$ we get,

$$M-Polynomial = xy^2 + xy^3 + 4x^2y^2 + 5x^2y^3$$

$$M_1(G) = (1+2)+(1+3)+4(2+2)+5(2+3) = 48$$

$$M_2(G) = (1\times 2)+(1\times 3)+4(2\times 2)+5(2\times 3) = 51$$

$$M_3(G) = |1-2| + |1-3| + 4|2-2| + 5|2-3| = 8$$

$$HM_1(G) = (1+2)^2 + (1+3)^2 + 4(2+2)^2 + 5(2+3)^2 = 214$$

$$HM_2(G) = (1\times 2)^2 + (1\times 3)^2 + 4(2\times 2)^2 + 5(2\times 3)^2 = 257$$

$$H(G) = \left(\frac{2}{1+2}\right) + \left(\frac{2}{1+3}\right) + 4\left(\frac{2}{2+2}\right) + 5\left(\frac{2}{2+3}\right) = 5.17$$

$$ABC(G) = \sqrt{\frac{1+2-2}{1\times 2}} + \sqrt{\frac{1+3-2}{1\times 3}} + 4\sqrt{\frac{2+2-2}{2\times 2}} + 5\sqrt{\frac{2+3-2}{2\times 3}} = 7.8$$

$$F(G) = (1+4) + (1+9) + 4(4+4) + 5(4+9) = 112$$

$$R(G) = \sqrt{\frac{1}{1\times 2}} + \sqrt{\frac{1}{1\times 3}} + 4\sqrt{\frac{1}{2\times 2}} + 5\sqrt{\frac{1}{2\times 3}} = 5.3$$

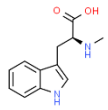
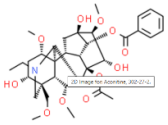
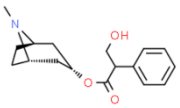
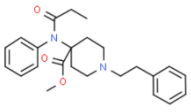
$$SCI(G) = \sqrt{\frac{1}{1+2}} + \sqrt{\frac{1}{1+3}} + 4\sqrt{\frac{1}{2+2}} + 5\sqrt{\frac{1}{2+3}} = 5.31$$

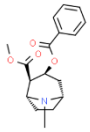
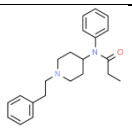
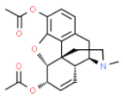
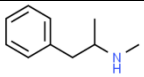
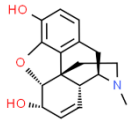
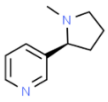
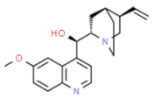
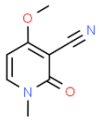
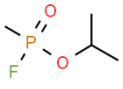
$$GA(G) = \left(\frac{2\sqrt{1\times 2}}{1+2}\right) + \left(\frac{2\sqrt{1\times 3}}{1+3}\right) + 4\left(\frac{2\sqrt{2\times 2}}{2+2}\right) + 5\left(\frac{2\sqrt{2\times 3}}{2+3}\right) = 10.71$$

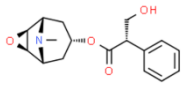
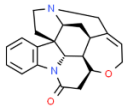
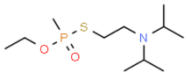
$$SO(G) = \sqrt{1+4} + \sqrt{1+9} + 4\sqrt{4+4} + 5\sqrt{4+9} = 34.74$$

2.3 Tables and Figures

Table 1. Poisons with their Molecule Title, Construction, Structural Depiction

Title	Construction	M-Polynomial	Structural Depiction
Abrine	$C_{12}H_{14}N_2O_2$	$Xy^2+2xy^3+4x^2y^2+7x^2y^3+3x^2y^3$	
Aconitine	$C_{34}H_{47}NO_{11}$	$5xy^2+5xy^3+xy^4+5x^2y^2+13x^2y^3+4x^2y^4+8x^3y^3+11x^3y^4$	
Atropine	$C_{17}H_{23}NO_3$	$Xy^2+2xy^3+5x^2y^2+10x^2y^3+4x^3y^3$	
Carfentanil	$C_{24}H_{30}N_2O_3$	$2xy^2+2xy^3+11x^2y^2+10x^2y^3+2x^2y^4+3x^3y^3+2x^3y^4$	

Molecule Title	Construction	M-Polynomial	Structural Depiction
Cocaine	$C_{17}H_{21}NO_4$	$Xy^2+3xy^3+5x^2y^2+9x^2y^3+5x^3y^3$	
Fentanyl	$C_{22}H_{28}N_2O$	$Xy^2+xy^3+11x^2y^2+11x^2y^3+3x^3y^3$	
Heroin	$C_{21}H_{23}NO_5$	$5xy^3+3x^2y^2+13x^2y^3+x^2y^4+6x^3y^3+3x^3y^4$	
Ketamine	$C_{13}H_{16}ClNO$	$Xy^2+2xy^3+6x^2y^2+3x^2y^3+2x^2y^4+x^3y^3+2x^3y^4$	
Methamphetamine	$C_{10}H_{15}N$	$Xy^2+xy^3+4x^2y^2+5x^2y^3$	
Morphine	$C_{17}H_{19}NO_3$	$3xy^3+3x^2y^2+9x^2y^3+x^2y^4+6x^3y^3+3x^3y^4$	
Nicotine	$C_{10}H_{14}N_2$	$Xy^3+6x^2y^2+4x^2y^3+2x^3y^3$	
Quinine	$C_{20}H_{24}N_2O_2$	$2xy^2+xy^3+4x^2y^2+14x^2y^3+6x^3y^3$	
Ricinin	$C_8H_8N_2O_2$	$2xy^2+2xy^3+x^2y^2+4x^2y^2+3x^3y^3$	
Sarin	$C_4H_{10}FO_2P$	$2xy^3+3xy^4+x^2y^3+x^2y^4$	

Title	Construction	M-Polynomial	Structural Depiction
Scopolamine	$C_{17}H_{21}NO_4$	$Xy^2+2xy^3+4x^2y^2+11x^2y^3+7x^3y^3$	
Strychnine	$C_{21}H_{22}N_2O_2$	$7x^2y^2+11x^2y^3+x^2y^4+8x^3y^3+3x^3y^4$	
VX	$C_{11}H_{26}NO_2PS$	$Xy^2+4xy^3+2xy^4+3x^2y^2+x^2y^3+2x^2y^4+2x^3y^3$	

2.4 Topological Descriptors and QSPR Modelling

Twelve topological indices, including the (M_1) Index, (M_2) Index, (M_3) Index,(HM_1) Index, (HM_2) Index, (H) Index, (ABC) Index, (F) Index, (R) Index, (S) Index, (GA) Index, (SO) Index, were employed to model seven representative physical features: Complexity (COM), Boiling Point (BP), Enthalpy of Vaporization (EN), Molar Refractivity (MR), Polarizability (PO), Molar Volume (MV), Molar Weight (MW), with seventeen poisons: Abrine, Aconitine, Atropine, Carfentanil, Cocaine, Fentanyl, Heroin, Ketamine, Methamphetamine, Morphine, Nicotine, Quinine, Ricinin, Sarin, Scopolamine, Strychnidin, VX. Topological indices, derived from the degree of precision and experimentally measured values of characteristics of seventeen poisons (obtained from ChemSpider [13]), are presented in Tables 2, 3, and 4. As shown in Table 5, these values exhibit a normal distribution, prompting the use of regression modelling to analyze the data.

2.4.1 Regression Models

We used a linear regression model to analyze the relationship between characteristics of poisons (P) and topological indices (TI): P=B+A (TI)
While B represents a constant, A denotes the regression coefficient, and TI signifies the topological Descriptor. SPSS software was used to analyze seven characteristics and twelve topological indices for seventeen poisons. Using this equation, Types of linear models were developed for different topological indices.

1.First Zagreb Index [$M_1(G)$]

COM=-99.713+4.610[$M_1(G)$], BP=169.384+2.216[$M_1(G)$], EV=37.772+0.279[$M_1(G)$], MR=20.997+0.526[$M_1(G)$], PO=8.314+0.209[$M_1(G)$], MV=91.570+1.303[$M_1(G)$], MW=59.989+2.050[$M_1(G)$]

2.Second Zagreb Index [$M_2(G)$]

COM=-46.099+3.383[$M_2(G)$], BP=197.547+1.609[$M_2(G)$], EV=41.258+0.203[$M_2(G)$], MR=28.701+0.374[$M_2(G)$], PO=11.370+0.148[$M_2(G)$], MV=112.401+0.915[$M_2(G)$], MW=88.490+1.471[$M_2(G)$]

3.Third Zagreb Index [$M_3(G)$]

COM=-6.367+23.743[$M_3(G)$], BP=246.204+9.623[$M_3(G)$], EV=46.815+1.249[$M_3(G)$], MR=33.842+2.585[$M_3(G)$], PO=13.408+1.025[$M_3(G)$], MV=111.716+7.062[$M_3(G)$], MW=96.311+10.852[$M_3(G)$]

4.First Hyper Zagreb [$HM_1(G)$]

COM=-53.700+0.821[$HM_1(G)$], BP=196.373+0.386[$HM_1(G)$], EV=41.072+0.049[$HM_1(G)$], MR=27.962+0.091[$HM_1(G)$], PO=11.077+0.036[$HM_1(G)$], MV=109.607+0.223[$HM_1(G)$], MW=84.564+0.358[$HM_1(G)$]

5.Second Hyper Zagreb [$HM_2(G)$]

COM=45.072+0.383[$HM_2(G)$], BP=247.572+0.175[$HM_2(G)$], EV=47.439+0.022[$HM_2(G)$], MR=40.782+0.040[$HM_2(G)$], PO=16.161+0.016[$HM_2(G)$], MV=142.391+0.098[$HM_2(G)$], MW=132.629+0.162[$HM_2(G)$]

6. Harmonic Index [H(G)]

COM=-157.487+59.605[H(G)], BP=130.461+29.813[H(G)], EV=33.075+3.736[H(G)], MR=9.220+7.337[H(G)], PO=3.640+2.910[H(G)], MV=57.989+18.639[H(G)], MW=20.642+27.927[H(G)]

7. Atomic Bond Connectivity Index [ABC(G)]

COM=-152.220+35.227[ABC(G)], BP=139.857+17.201[ABC(G)], EV=34.155+2.161[ABC(G)], MR=12.364+4.182[ABC(G)], PO=4.890+1.659[ABC(G)], MV=67.378+10.537[ABC(G)], MW=29.074+16.136[ABC(G)]

8. Forgotten Topological Index [F(G)]

COM=-59.500+1.589[F(G)], BP=195.952+0.740[F(G)], EV=40.983+0.094[F(G)], MR=27.417+0.175[F(G)], PO=10.861+0.069[F(G)], MV=107.330+0.435[F(G)], MW=81.447+0.695[F(G)]

9. Randić Index [R(G)]

COM=-166.354+58.452[R(G)], BP=129.222+28.916[R(G)], EV=32.861+3.629[R(G)], MR=8.437+7.164[R(G)], PO=3.330+2.842[R(G)], MV=54.883+18.312[R(G)], MW=16.159+27.420[R(G)]

10. Sum-Connectivity Index [SCI(G)]

COM=-149.994+54.406[SCI(G)], BP=136.703+26.973[SCI(G)], EV=33.821+3.383[SCI(G)], MR=11.502+6.567[SCI(G)], PO=4.547+2.605[SCI(G)], MV=65.139+16.552[SCI(G)], MW=27.913+25.130[SCI(G)]

11. Geometric Arithmetic Index [GA(G)]

COM=-129.554+24.717[GA(G)]**,** BP=147.181+12.239[GA(G)], EV=35.126+1.536[GA(G)], MR=15.063+2.934[GA(G)], PO=5.960+1.164[GA(G)], MV=76.044+7.308[GA(G)], MW=41.090+11.248[GA(G)]

12. Sombor Index [SO(G)]

COM=-103.755+6.415[SO(G)]**,** BP=168.910+3.066[SO(G)], EV=37.688+0.387[SO(G)], MR=20.622+0.731[SO(G)], PO=8.166+0.290[SO(G)], MV=90.072+1.818[SO(G)], MW=57.887+2.857[SO(G)]

Table 2. Physical features of poisons.

Name	COM	BP	EV	MR	PO	MV	MW
Abrine	257	439.1	73.4	62.5	24.8	171.5	218.25
Aconitine	1210	717.2	110	163.1	64.7	468.2	645.7
Atropine	353	429.8	72.2	80.8	32	242.4	289.4
Carfentanil	530	508.1	77.8	114.5	45.4	345.4	394.5
Cocaine	432	395.2	64.5	81.1	32.2	248.1	303.35
Fentanyl	391	466.2	72.8	103.7	41.1	309.4	336.5
Heroin	692	492.9	76	97.2	38.5	273.7	369.4
Ketamine	269	363.8	61	65.7	26.1	202.6	237.72
Methamphetamine	95	215.5	45.2	48.6	19.3	164.5	149.23
Morphine	494	476.2	77.9	78	30.9	197.6	285.34
Nicotine	147	244.4	48.2	49.3	19.5	157.2	162.23
Quinine	457	495.9	80.4	95.8	38	266.4	324.4
Ricinin	319	370.9	61.8	42.1	16.7	132.6	164.16
Sarin	113	147	36.8	29.3	11.6	130.9	140.09
Scopolamine	418	460.3	76	80.4	31.9	231	303.35
Strychnine	689	559.9	84.2	93.2	36.9	234.8	334.4
VX	220	318.8	56	73.3	29	262.6	267.37

Table 3. The calculated values of the topological indices for poisons under investigation.

Name	M_1	M_2	M_3	HM_1	HM_2	H
Abrine	80	93	12	388	581	7.47
Aconitine	273	360	51	1515	3072	21.14
Atropine	110	130	16	540	822	9.90
Carfentanil	146	172	22	718	1140	13.74
Cocaine	116	139	16	578	921	10.27
Fentanyl	124	142	14	584	828	12.07
Heroin	160	203	28	852	1543	12.39
Ketamine	82	99	14	418	723	7.44
Methamphetamine	48	51	8	214	257	5.17
Morphine	132	173	20	720	1381	9.79
Nicotine	60	69	6	284	411	5.77
Quinine	132	161	18	664	1071	11.43
Ricinin	56	65	10	274	429	5.43
Sarin	34	32	16	168	166	2.93
Scopolamine	124	153	16	632	1049	10.40
Strychnidin	158	210	16	858	1652	11.76
VX	70	74	20	340	446	6.70

Table 4. The quantitative parameters of the topological descriptors of poisons.

Name	ABC	F	Ra	SCI	GA	So
Abrine	12.12	202	7.72	7.93	16.53	57.84
Aconitine	36.51	795	22.06	23.24	50.22	198.32
Atropine	16.32	280	10.19	10.63	22.45	79.33
Carfentanil	21.93	374	14.10	14.52	30.28	105.39
Cocaine	17.06	300	10.61	11.05	23.36	83.77
Fentanyl	19.08	300	12.28	12.72	26.59	88.90
Heroin	22.04	446	12.91	13.81	29.98	116.10
Ketamine	12.08	220	7.70	7.90	16.48	59.53
Methamphetamine	7.89	112	5.33	5.31	10.71	34.74
Morphine	17.58	374	10.13	11.02	24.33	95.35
Nicotine	9.22	146	5.88	6.11	12.79	43.04
Quinine	18.96	342	11.71	12.37	26.47	94.88
Ricinin	8.58	144	5.70	5.67	11.54	40.78
Sarin	5.65	104	3.42	3.20	6.05	26.77
Scopolamine	17.61	326	10.69	11.35	24.45	89.23
Strychnidin	20.70	438	11.88	13.23	29.69	112.87
VX	11.28	192	7.30	7.05	13.87	52.65

Table 5. Correlation coefficients associated with the physical properties of poisons.

	COM	**BP**	**EV**	**MR**	**PO**	**MV**	**MW**
M_1	0.975	0.929	0.934	0.955	0.955	0.881	0.973
M_2	0.982	0.925	0.932	0.932	0.932	0.849	0.957
M_3	0.881	0.707	0.732	0.823	0.823	0.838	0.903
HM_1	0.984	0.917	0.925	0.932	0.932	0.856	0.962
HM_2	0.985	0.893	0.909	0.889	0.889	0.806	0.933
HG	0.934	0.926	0.925	0.987	0.987	0.934	0.982
ABC	0.958	0.927	0.929	0.976	0.976	0.917	0.985
F	0.985	0.908	0.917	0.931	0.931	0.861	0.966
R	0.939	0.92	0.921	0.988	0.988	0.941	0.988
SCI	0.948	0.931	0.931	0.981	0.982	0.922	0.982
GA	0.955	0.937	0.937	0.973	0.973	0.903	0.975
So	0.977	0.925	0.93	0.955	0.954	0.885	0.976

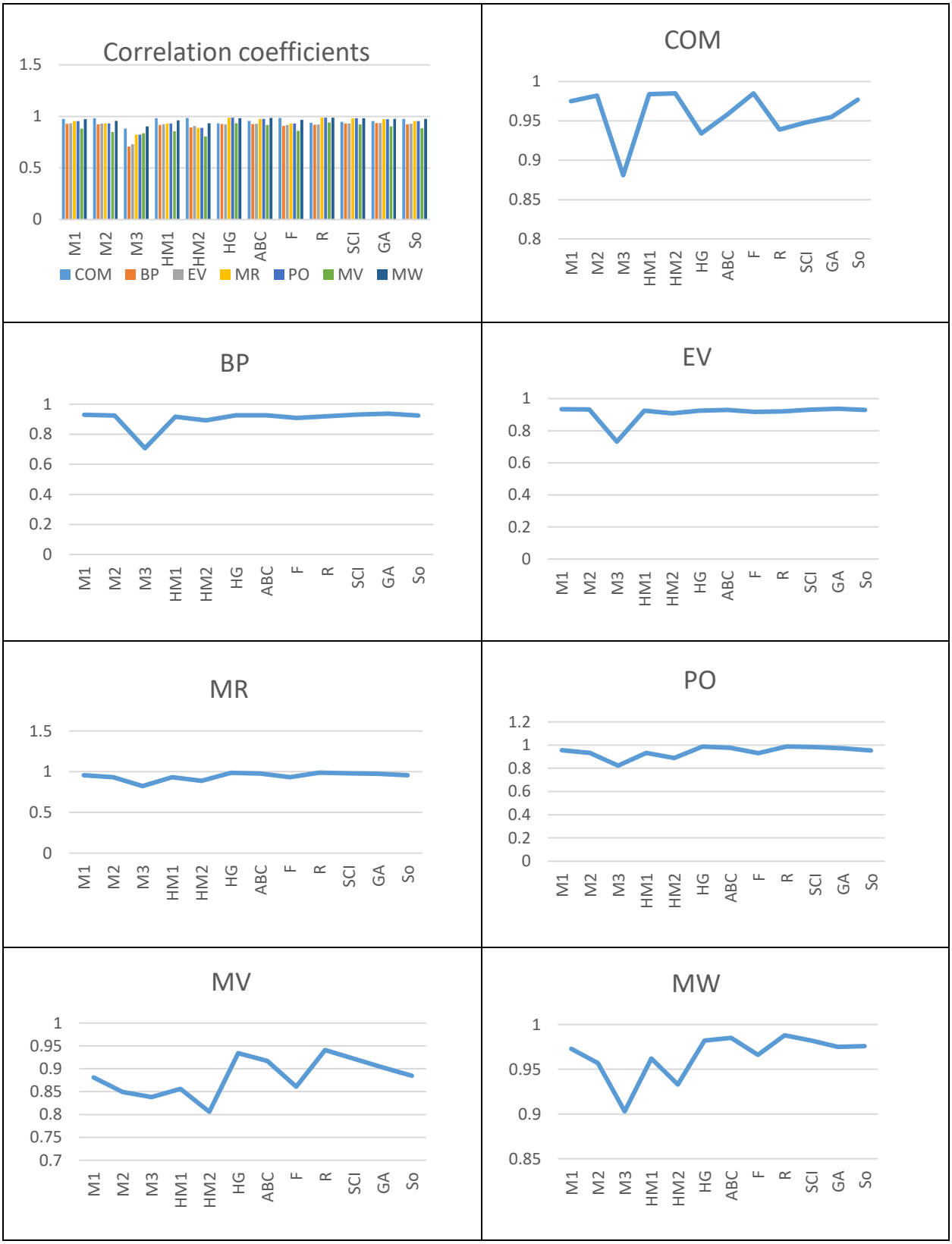


Figure 2. Correlation Coefficients on Physicochemical Features

Table 6. Statistical analysis of the M_1 index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	4.61	-99.713	**0.975**	**0.951**	33.743	91.762	0.000	significant
BP	17	2.216	169.384	0.929	0.863	28.484	94.634	0.000	significant
EV	17	0.279	37.772	0.934	0.872	3.459	101.927	0.000	significant
MR	17	0.526	20.997	0.955	0.911	5.302	153.735	0.000	significant
PO	17	0.209	8.314	0.955	0.911	2.103	153.706	0.000	significant
MV	17	1.303	91.570	0.881	0.777	22.536	52.267	0.000	significant
MW	17	2.05	59.989	0.973	0.947	15.720	265.912	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 7. Statistical analysis of the M_2 index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	3.383	-46.099	**0.982**	**0.964**	26.412	402.210	0.000	significant
BP	17	1.609	197.547	0.925	0.856	26.651	89.357	0.000	significant
EV	17	0.203	41.258	0.932	0.869	3.195	99.205	0.000	significant
MR	17	0.374	28.701	0.932	0.869	5.881	99.292	0.000	significant
PO	17	0.148	11.370	0.932	0.869	2.333	99.267	0.000	significant
MV	17	0.915	112.401	0.849	0.721	23.021	38.714	0.000	significant
MW	17	1.471	88.490	0.957	0.917	17.935	164.844	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 8. Statistical analysis of the M_3 index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	23.743	-6.367	0.881	0.776	66.899	51.934	0.000	significant
BP	17	9.623	246.204	0.707	0.500	50.407	15.026	0.001	significant
EV	17	1.249	46.815	0.732	0.536	6.095	17.305	0.001	significant
MR	17	2.585	33.842	0.823	0.677	9.358	31.459	0.000	significant
PO	17	1.025	13.408	0.823	0.677	3.711	31.465	0.000	significant
MV	17	7.062	111.716	0.838	0.702	24.137	35.292	0.000	significant
MW	17	10.852	96.311	**0.903**	**0.815**	27.066	66.278	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 9. Statistical analysis of the HM_1 index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	0.821	-53.700	**0.984**	**0.968**	25.036	49.414	0.000	significant
BP	17	0.386	196.373	0.917	0.841	28.293	79.608	0.000	significant
EV	17	0.049	41.072	0.925	0.856	3.382	89.117	0.000	significant
MR	17	0.091	27.962	0.932	0.869	5.933	99.746	0.000	significant
PO	17	0.036	11.077	0.932	0.869	2.353	99.705	0.000	significant
MV	17	0.223	109.607	0.856	0.732	22.778	41.758	0.000	significant
MW	17	0.353	84.564	0.962	0.926	17.039	181.581	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 10. Statistical analysis of the HM_2 index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	0.383	45.072	**0.985**	**0.970**	20.657	480.085	0.000	significant
BP	17	0.175	247.572	0.893	0.798	26.945	59.107	0.000	significant
EV	17	0.022	47.439	0.905	0.820	3.190	68.148	0.000	significant
MR	17	0.04	40.782	0.889	0.791	6.320	56.840	0.000	significant
PO	17	0.016	16.161	0.889	0.791	2.507	56.841	0.000	significant
MV	17	0.098	142.391	0.806	0.650	21.956	27.864	0.000	significant
MW	17	0.162	132.629	0.933	0.871	18.983	101.523	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 11. Statistical analysis of the H index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	59.605	-157.487	0.934	0.873	61.475	103.157	0.000	significant
BP	17	29.813	130.461	0.926	0.858	32.856	90.348	0.000	significant
EV	17	3.736	33.075	0.925	0.856	4.142	89.260	0.000	significant
MR	17	7.337	9.220	**0.987**	**0.974**	3.242	561.908	0.000	significant
PO	17	2.91	3.640	**0.987**	**0.974**	1.280	567.367	0.000	significant
MV	17	18.639	57.989	0.934	0.873	19.240	102.983	0.000	significant
MW	17	27.927	20.642	0.982	0.964	14.539	404.868	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 12. Statistical analysis of the ***ABC*** index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	35.227	-152.220	0.958	0.919	47.783	169.481	0.000	significant
BP	17	17.201	139.857	0.927	0.860	31.634	92.201	0.000	significant
EV	17	2.161	34.155	0.929	0.863	3.920	94.798	0.000	significant
MR	17	4.182	12.364	0.976	0.953	4.226	305.319	0.000	significant
PO	17	1.659	4.890	0.976	0.953	1.675	305.670	0.000	significant
MV	17	10.537	67.378	0.917	0.840	20.943	78.933	0.000	significant
MW	17	16.136	29.074	**0.985**	**0.970**	12.984	481.600	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 13. Statistical analysis of the ***F*** index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	1.589	-59.500	**0.985**	**0.970**	24.731	479.963	0.000	significant
BP	17	0.74	195.952	0.908	0.825	29.963	70.873	0.001	significant
EV	17	0.094	40.983	0.917	0.842	3.578	79.746	0.000	significant
MR	17	0.175	27.417	0.931	0.867	6.031	98.030	0.000	significant
PO	17	0.069	10.861	0.931	0.867	2.393	97.977	0.000	significant
MV	17	0.435	107.330	0.861	0.741	22.596	4.993	0.000	significant
MW	17	0.695	81.447	0.966	0.933	16.414	208.318	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 14. Statistical analysis of the ***R*** index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	58.452	-66.354	0.939	0.882	59.845	111.889	0.000	significant
BP	17	28.916	129.222	0.920	0.847	34.323	83.243	0.000	significant
EV	17	3.629	32.861	0.921	0.849	4.286	84.084	0.000	significant
MR	17	7.164	8.437	**0.988**	**0.975**	3.188	592.254	0.000	significant
PO	17	2.842	3.330	**0.988**	**0.976**	1.258	598.132	0.000	significant
MV	17	18.312	54.883	0.941	0.885	18.474	115.234	0.000	significant
MW	17	27.42	16.159	**0.988**	**0.976**	11.954	617.045	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 15. Statistical analysis of the ***SCI*** index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	54.406	-149.994	0.948	0.898	53.817	132.246	0.000	significant
BP	17	26.973	136.730	0.931	0.867	31.057	97.608	0.000	significant
EV	17	3.383	33.821	0.931	0.867	3.891	97.857	0.000	significant
MR	17	6.567	11.502	0.981	0.963	3.765	393.675	0.000	significant
PO	17	2.605	4.547	**0.982**	**0.964**	1.490	395.309	0.000	significant
MV	17	16.552	65.139	0.922	0.850	20.431	84.933	0.000	significant
MW	17	25.13	27.913	**0.982**	**0.964**	14.247	402.632	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 16. Statistical analysis of the ***GA*** index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	24.717	-129.554	0.955	0.912	48.191	155.539	0.000	significant
BP	17	12.239	147.181	0.937	0.878	28.644	107.940	0.000	significant
EV	17	1.536	35.126	0.937	0.879	3.581	108.692	0.000	significant
MR	17	2.934	15.063	0.973	0.946	4.398	263.074	0.000	significant
PO	17	1.164	5.960	0.973	0.946	1.743	263.492	0.000	significant
MV	17	7.308	76.044	0.903	0.815	21.853	66.117	0.000	significant
MW	17	11.248	41.090	**0.975**	**0.950**	16.157	286.542	0.000	significant
Bold numbers indicate the strongest correlations.									

Table 17. Statistical analysis of the ***SO*** index

Physical features	N	A	b	R	R^2	SE	F	P	Indicant
COM	17	6.415	-103.755	**0.977**	**0.954**	32.945	310.108	0.000	significant
BP	17	3.066	168.910	0.925	0.856	29.417	88.844	0.000	significant
EV	17	0.387	37.688	0.930	0.865	3.562	96.392	0.000	significant
MR	17	0.731	20.622	0.955	0.911	5.330	153.680	0.000	significant
PO	17	0.29	8.166	0.954	0.911	2.114	153.638	0.000	significant
MV	17	1.818	90.072	0.885	0.783	22.343	54.133	0.000	significant
MW	17	2.857	57.887	0.976	0.952	15.004	296.526	0.000	significant
Bold numbers indicate the strongest correlations.									

3 SUBMITTING THE PAPER

The full paper has to be submitted electronically via the website of the conference) by Paper number (in the format "XXX") is assigned to each abstract after it was submitted through our OpenConf system and authors are kindly asked to place this paper number to the correct positions in the header and footer before submitting the final version.

4 CONFERENCE PROGRAM AND PROCEEDINGS

The extended abstracts and full manuscripts are compiled into the conference Proceedings DVD-ROM.

5 CONCLUSION

Table 5 and Figure 2 present the relationship between the physicochemical properties of the analyzed poisons and the corresponding topological indices. In this paper, the complexity property exhibited a strong positive correlation with the Second Hyper Zagreb index ($HM_2(G)$) and the Forgotten index (F(G)), with a correlation coefficient of (r=0.985). Additionally, this property demonstrated high correlations with the First Hyper Zagreb index ($HM_1(G)$) and the Second Zagreb index ($M_2(G)$), with correlation coefficients of (r=0.984), (r = 0.982), respectively. The Randic index (RA(G)) exhibits the highest and most significant correlation with Molar Refractivity (MR), Polarizability (PO), and Molecular Weight (MW), with a correlation coefficient of (r=0.988). The Atomic- Bond-Connectivity (ABC(G)), the Sum-Connectivity Index (SCI(G)), and the Geometric Arithmetic index (GA(G)) demonstrated a high and significant correlation value (r=0.985), (r=0.982) and (r=0.975) with Molar Weight (MW) property. In summary, a strong relationship was identified between the physicochemical properties of poisons and the connectivity indices. Regression models presented in Tables 6 to 17 reveal statistically significant correlations ($r>0.7$, $p<0.05$), highlighting the robustness of the linear predictive relationships. Equations were selected based on minimum standard error (SE), maximum coefficient of determination (R^2), and maximum F-statistic (F). All physicochemical properties were highly significant, emphasizing the potential importance of these topological indices in QSPR analysis for poisons. The plotted regression lines further corroborate this conclusion. These findings may contribute to the improvement of the production, development, and efficacy of poisons. Additionally, the methodology can be applied to investigate the structures of other drug compounds.

6 ACKNOWLEDGEMENTS

The authors are very grateful to the editor and the anonymous referee(s) for their comments and suggestions which led to the present improved version of the manuscript.

REFERENCES

[1] Available online. Http://www.rsc.org (accessed on 28 November 2024)

[2] Zaman, S., Ahmed, W., Sakeena, A. *et al.* Mathematical modeling and topological graph description of dominating David derived networks based on edge partitions 2023. *Sci Rep* **13**, 15159.

[3] Ghods, M.; Ramezani Tousi, J. Computing Revan Polynomials and Revan Indices of Copper (I) Oxide and Copper (II) Oxide.Commun. Comb. Cryptogr. Comput. Sci 2021, 1, 50–58.

[4] Havare, Ö. Ç. Quantitative structure analysis of some molecules in drugs used in the treatment of COVID-19 with topological indices. Polycyclic Aromatic Compounds 2022. 42(8), 5249-5260.

[5] Huang, L.; Wang, Y.; Pattabiraman, K.; Danesh, P.; Siddiqui, M. K., & Cancan, M. Topological indices and QSPR modeling of new antiviral drugs for cancer treatment. Polycyclic Aromatic Compounds 2023.43(9), 8147-8170.

[6] Aslam, Y.; Bashir, S.; Ahmad, W., & Gao, W. On topological indices of certain dendrimer structures. Zeitschrift für Naturforschung B 2017. 72(4), 481-486.

[7] Adnan, M.; Bokhary, S.A.U.H.; Abbas, G.; Iqbal, T. Degree-based topological indices and QSPR analysis of antituberculosis drugs.J. Chem 2022, 5748626.

[8] Altassan, A.; Rather, B.A.; Imran, M. Inverse Sum Indeg Index (Energy) with Applications to Anticancer Drugs. Mathematics 2022, 10, 4749.

[9] Hasani, M., Ghods, M. Calculation of topological indices along with MATLAB coding in QSPR analysis of calcium channel-blocking cardiac drugs. *J Math Chem* **62** 2024. 2456–2477.

[10] Sadati, S, H., Talebi Rostami, A, A. A Description of Connectivity Indices in a Cubic Fuzzy Graph with an Application. Journal of Multiple-valued Logic and Soft Computing, 2023. 40(5-6):569-585

[11] Tousi, Jaber Ramezani & Ghods, M. Some polynomials and degree-based topological indices of molecular graph and line graph of Titanium dioxide nanotubes, *Journal of Information and Optimization Sciences 2024.*45:1, 95–106.

[12] Lee, YT., Chen, SJ. Graph theory applications in congenital heart disease. *Sci Rep* **13**,2023. 11135.

[13] ChemSpider. Available online: http://www.chemspider.com (accessed on 10 November 2024).

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A Robust RGB Image Encryption Scheme Based on Chaos Synchronization

Ali Hassan[1], Liangqiang Zhou
School of Mathematics, Nanjing University of Aeronautics and Astronautics
Nanjing, China
ali.hassan3512@hotmail.com[1]

Ayesha Tariq
Department of Zoology, The Govt. Sadiq College Women University
Bahawalpur, Pakistan

ABSTRACT

This paper studies the finite-time synchronization of hyperchaotic systems used for image encryption. We proposed an efficient encryption scheme that employs Arnold map scrambling and Henon map diffusion techniques. The practicality of the approach is measured by performing entropy analysis, which results in an entropy value of 7.9993 that is close to the ideal value. Furthermore, the method provides an extended key space of 10^{120}, which guarantees robust defense against brute-force attacks. The findings of our study show that the synchronization of hyperchaotic systems considerably improves the security of image encryption, providing optimistic prospects in the field of secure communication.

KEYWORDS: Arnold map scrambling, Finite-time synchronization, Henon map diffusion, Image encryption.

1 INTRODUCTION

Chaotic systems show unusual, irregular dynamics, instability, and a high degree of sensitivity to initial values, such that even small changes may result in significantly unique output. These characteristics make chaotic systems particularly beneficial in implementations such as secure communication, image encoding, and weak signal detection [1-3].

Chaotic synchronization is a significant area of study in chaotic systems. Researchers have designed various techniques to achieve synchronization, including fixed-time synchronization [4], complete synchronization [5], and adaptive synchronization [6]. Sangpet and Kuntanapreeda [7] achieved finite-time synchronization of complex systems using feedback passivation, and Laarem explored chaos synchronization between higher-dimensional systems using sliding mode control [8]. Despite such developments, it is necessary to keep discovering synchronization methods for chaotic systems. In this study, we propose a new hyperchaotic system integrated with a finite-time synchronization strategy to achieve finite-time synchronization.

In the current era, as the use of digital images for information transmission increases, it is essential to ensure their security. Various conventional encryption algorithms, including DES (Data Encryption Standard), AES (Advanced Encryption Standard), and RSA (Rivest-Shamir-Adleman), are more ideal for text encoding than image encoding. Recently, scholars have started exploring stronger and more reliable encryption algorithms for images, including DNA-based encryption [9], chaotic systems [10], quantum cryptography [11], and the Fibonacci Q-matrix encryption methods [12]. Gan et al. introduced a 2D

compressed sensing technique for image compression and encryption [13]. Compressed sensing may reduce image processing performance by compressing the image volume, but it may additionally contribute to the loss of data in the decrypted image. Furthermore, image encryption methods that rely on chaotic systems continue to face security issues. Xu et al. [14] created an algorithm that depends on three-dimensional chaotic systems to perform encryption work efficiently. However, it is important to note that low-dimensional chaotic systems have a limited key space and provide less safety due to their small number of parameters and initial values. Thus, it is important to build an encryption algorithm that can be both rapid and secure.

In this paper, we build a four-dimensional (4D) hyperchaotic system to realize finite-time synchronization. By incorporating this system with the Arnold Cat Map and Henon Map, we design a robust image encryption algorithm for finite-time synchronization. This paper presents three main innovations:

1. Construction of a 4D Hyperchaotic System: We develop a four-dimensional hyperchaotic system and achieve its finite-time synchronization.
2. Enhanced Henon Map: We propose an improved version of the Henon Map (2D-EHM) with superior sequence generation performance compared to the original.
3. Central Diffusion Strategy: We introduce a central diffusion strategy that combines the three-color channels of an image and diffuses them simultaneously.

The subsequent sections of this article have been arranged in the following order: Section 2 presents the background of the research, which includes chaotic maps and a 4D hyperchaotic system. Section 3 focuses on the synchronization of the 4D hyperchaotic system. The unique characteristics of our image encryption scheme are explained in Section 4. Section 5 focuses on experiments and results. Section 6 came to a final conclusion.

2 PRELIMINARIES

2.1 4D Hyperchaotic System

A novel 4D Hyperchaotic system is proposed by introducing additional state variable to Yang's chaotic system [15].

$$\begin{cases} \dot{y_1} = \sigma(y_2 - y_1) \\ \dot{y_2} = \rho y_1 - y_1 y_3 + y_4 \\ \dot{y_3} = -\gamma y_3 + y_1 y_2 \\ \dot{y_4} = -m y_1 + n y_2 y_3 \end{cases}, \tag{1}$$

When the parameter values $\sigma = 10$, $\gamma = 8/3$, $\rho = 22$, $m = 8$, $n = 0.01$ are selected, the system is hyperchaotic, as shown in Fig. 1.

2.2 2D-EHM

The Henon map [16] is described by a mathematical equation, as presented below:

$$G_{Henon} = \begin{cases} G_1 : g_1(n+1) = g_2(n) - \varphi g_1(n)^2 + 1, \\ G_2 : g_2(n+1) = \zeta g_1(n). \end{cases} \tag{2}$$

Where $g_1(1)$ and $g_2(1)$ are the initial conditions of Henon map, φ and ζ are the adjustable parameters of Henon map.

The standard 2D Henon chaotic map has a bounded parameter range, leading to decreased efficiency in constructing sequences. For optimal security and performance, it is vital to develop a novel chaotic map precisely designed for encryption images. However, by implementing the sin function, one can achieve a more complicated chaotic model, thereby strengthening performance capabilities. The 2D-EHM is described by a mathematical equation, as shown below:

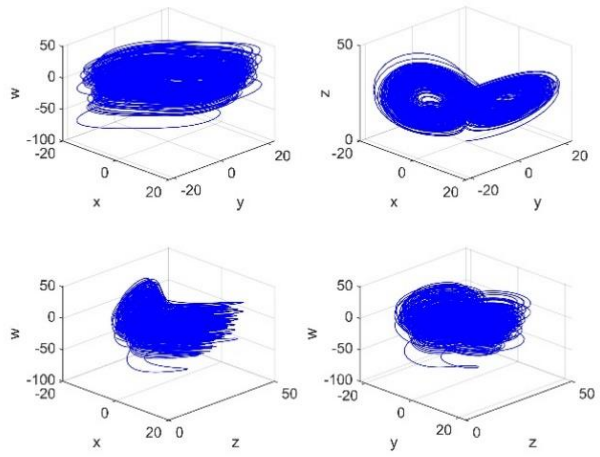


Fig. 1. Hyperchaotic attractors in System (1).

$$G_{2D-EHM} = \begin{cases} G_1 : g_1(n+1) = \sin(g_2(n) - \varphi g_1(n)^2 + 1), \\ G_2 : g_2(n+1) = \sin(10^3 \zeta g_1(n)). \end{cases} \tag{3}$$

Where $g_1(1)$ and $g_2(1)$ are the initial conditions of 2D-EHM, φ and ζ are the adjustable parameters of 2D-EHM.

2.3 Arnold Map

The Arnold map is a non-singular, two-dimensional nonlinear map identified in the 1960s by Valdimir Arnold utilizing an image of a cat, as defined below [17]:

$$\begin{bmatrix} p_{i+1} \\ q_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & n \\ m & mn+1 \end{bmatrix} \begin{bmatrix} p_i \\ q_i \end{bmatrix} \bmod N, \tag{4}$$

Where (p_i, q_i) represents the initial positions of the pixel, (m, n) denotes control parameters, and (p_{i+1}, q_{i+1}) signifies the new position of the pixels in the scrambled image.

3 SYNCHRONIZATION METHODS

From Eq. (1), we formulate driving system as

$$\begin{cases} \dot{y_{m1}} = \sigma(y_{m2} - y_{m1}) \\ \dot{y_{m2}} = \rho y_{m1} - y_{m1} y_{m3} + y_{m4} \\ \dot{y_{m3}} = -\gamma y_{m3} + y_{m1} y_{m2} \\ \dot{y_{m4}} = -m y_{m1} + n y_{m2} y_{m3} \end{cases}, \tag{5}$$

Where σ, ρ, γ, m, n are the parameters and y_{m1}, y_{m2}, y_{m3}, and y_{m4} are the state variables of the driving system.

The subsequent system is considered a response system, defined as:

$$\begin{cases} \dot{y_{s1}} = \sigma(y_{s2} - y_{s1}) + \hat{u}_1 \\ \dot{y_{s2}} = \rho y_{s1} - y_{s1} y_{s3} + y_{s4} + \hat{u}_2 \\ \dot{y_{s3}} = -\gamma y_{s3} + y_{s1} y_{s2} + \hat{u}_3 \\ \dot{y_{s4}} = -m y_{s1} + n y_{s2} y_{s3} + \hat{u}_4 \end{cases}, \tag{6}$$

Where σ, ρ, γ, m, n are the parameters, y_{s1}, y_{s2}, y_{s3}, and y_{s4} are the state variables of the response system and $\hat{u}_1$, $\hat{u}_2$, $\hat{u}_3$, and $\hat{u}_4$ are the controller.

We represent the errors e_1, e_2, e_3, and e_4 as $y_{s1} - y_{m1}$, $y_{s2} - y_{m2}$, $y_{s3} - y_{m3}$, and $y_{s4} - y_{m4}$, respectively. From Eqs. (5) and (6), we derived the error dynamics

$$\begin{cases} \dot{e_1} = \sigma e_2 - \sigma e_1 + \hat{u}_1 \\ \dot{e_2} = \rho e_1 - y_{s1} y_{s3} + y_{m1} y_{m3} + e_4 + \hat{u}_2 \\ \dot{e_3} = -\gamma e_3 + y_{s1} y_{s2} - y_{m1} y_{m2} + \hat{u}_3 \\ \dot{e_4} = -m e_1 + n y_{s2} y_{s3} - n y_{m2} y_{m3} + \hat{u}_4 \end{cases}, \tag{7}$$

Therefore, to achieve synchronization between the drive system and the response system in a finite time, it is essential to determine a time $\tau_1 > 0$, such that $\lim_{\tau \to \tau_1} | e_i | = 0$ and for $\tau > \tau_1$, $| e_i | = 0$.

Theorem 1. [18] If the $U(\tau)$ is a positive definite function such that:

$$\dot{U}(\tau) \le -\psi U^{\varepsilon}(\tau), \ \forall \tau \ge \tau_0, \ U(\tau_0) \ge 0 \tag{8}$$

Where $\psi > 0$, $0 < \varepsilon < 1$, the function $U(\tau)$ satisfies:

$$U^{1-\varepsilon}(\tau) \le U^{1-\varepsilon}(\tau) - \psi(1-\varepsilon)(\tau - \tau_0), \ \tau_1 \ge \tau \ge \tau_0 \tag{9}$$

also

$$U(\tau) = 0, \ \forall \tau \ge \tau_1 \tag{10}$$

time τ_1 satisfies:

$$\tau_1 \le \tau_0 + \frac{U^{1-\varepsilon}}{\psi(1-\varepsilon)} \tag{11}$$

Theorem 2. For any real numbers $\alpha_1, \alpha_2, \alpha_3 ... \alpha_n$ and $0 < q < 1$, the following inequality holds.

$$\sum |\alpha_j|^{q+1} \geq \left(\sum_{j=1}^{n} |\alpha_j|^2 \right)^{\frac{q+1}{2}} \tag{12}$$

By using Eq. (7), the controller is defined as

$$\begin{cases} \hat{u}_1 = \sigma e_1 - \sigma e_2 - k_1 e_1 - k_2 \operatorname{sgn}(e_1) |e_1|^q \\ \hat{u}_2 = -\rho e_1 + y_{s1} y_{s3} - y_{m1} y_{m3} - e_4 - k_1 e_2 - k_2 \operatorname{sgn}(e_2) |e_2|^q \\ \hat{u}_3 = \gamma e_3 - y_{s1} y_{s2} + y_{m1} y_{m2} - k_1 e_3 - k_2 \operatorname{sgn}(e_3) |e_3|^q \\ \hat{u}_4 = m e_1 - n y_{s2} y_{s3} + n y_{m2} y_{m3} - k_1 e_4 - k_2 \operatorname{sgn}(e_4) |e_4|^q \end{cases} \tag{13}$$

Where k_1 and k_2 are constants.

Consider a Lyapunov function:

$$U = \frac{1}{2} \sum_{i=1}^{4} e_i^2 \tag{14}$$

Combining with Eq. (7), we can write as

$$\begin{aligned} \dot{U} &= e_1 \dot{e}_1 + e_2 \dot{e}_2 + e_3 \dot{e}_3 + e_4 \dot{e}_4 \\ &= e_1(\sigma e_2 - \sigma e_1 + \hat{u}_1) + e_2(\rho e_1 - y_{s1} y_{s3} + y_{m1} y_{m3} + e_4 + \hat{u}_2) \\ &+ e_3(-\gamma e_3 + y_{s1} y_{s2} - y_{m1} y_{m2} + \hat{u}_3) + e_4(-m e_1 + n y_{s2} y_{s3} \\ &- n y_{m2} y_{m3} + \hat{u}_4) \end{aligned} \tag{15}$$

Furthermore, substitute Eq. (13) in Eq. (15)

$$\begin{aligned} \dot{U} &= e_1(\sigma e_2 - \sigma e_1 + \sigma e_1 - \sigma e_2 - k_1 e_1 - k_2 \operatorname{sgn}(e_1) |e_1|^q) \\ &+ e_2(\rho e_1 - y_{s1} y_{s3} + y_{m1} y_{m3} + e_4 - \rho e_1 + y_{s1} y_{s3} - y_{m1} y_{m3} \\ &- e_4 - k_1 e_2 - k_2 \operatorname{sgn}(e_2) |e_2|^q) + e_3(-\gamma e_3 + y_{s1} y_{s2} - y_{m1} y_{m2} \\ &+ \gamma e_3 - y_{s1} y_{s2} + y_{m1} y_{m2} - k_1 e_3 - k_2 \operatorname{sgn}(e_3) |e_3|^q) \\ &+ e_4(-m e_1 + n y_{s2} y_{s3} - n y_{m2} y_{m3} + m e_1 - n y_{s2} y_{s3} + n y_{m2} y_{m3} \\ &- k_1 e_4 - k_2 \operatorname{sgn}(e_4) |e_4|^q) \\ &= -k_1(e^2_1 + e^2_2 + e^2_3 + e^2_4) - k_2(\operatorname{sgn}(e_1) |e_1|^{q+1} \\ &+ \operatorname{sgn}(e_2) |e_2|^{q+1} + \operatorname{sgn}(e_3) |e_3|^{q+1} + \operatorname{sgn}(e_4) |e_4|^{q+1}) \\ &\leq -k_2(\operatorname{sgn}(e_1) |e_1|^{q+1} + \operatorname{sgn}(e_2) |e_2|^{q+1} + \operatorname{sgn}(e_3) |e_3|^{q+1} \\ &+ \operatorname{sgn}(e_4) |e_4|^{q+1}) \end{aligned} \tag{16}$$

According to Theorem 2,

$$(|e_1|^{q+1} + |e_2|^{q+1} + |e_3|^{q+1} + |e_4|^{q+1}) \geq (|e_1|^2 + |e_2|^2 + |e_3|^2 + |e_4|^2)^{\frac{q+1}{2}}$$

$$\dot{U} \leq -k_2(|e_1|^2 + |e_2|^2 + |e_3|^2 + |e_4|^2)^{\frac{q+1}{2}}$$

$$\leq -k_2 (2U)^{\frac{q+1}{2}}$$
$$\leq -2^{\frac{q+1}{2}} k_2 U^{\frac{q+1}{2}} \tag{17}$$

Implementing finite time synchronization between systems (5) and (6) is achievable, as described in Theorem 1, and the synchronization time is:

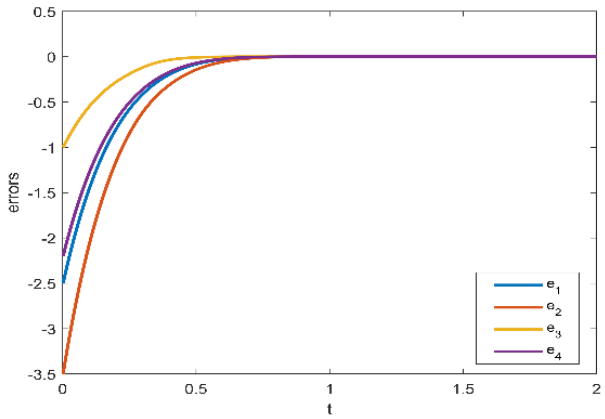


Fig. 2. Error dynamics of systems (5) and (6).

$$\tau_1 \leq \frac{(U(\tau_0))^{\frac{1-q}{2}}}{2^{\frac{q-1}{2}} k_2 (1-q)} \tag{18}$$

Finally, a numerical simulation has been performed to further study synchronization. By settling the initial values of system (5) as $(1.5, 2.5, 0, 1.2)$ and system (6) as $(-1, -1, -1, -1)$ and adjusting the parameters $k_1 = 3$, $k_2 = 3$ and $q = 0.7$ in theorem 1, the upper limit of synchronization time is :

$$\tau_1 \leq 1.7935 \tag{19}$$

Fig. 2. shows the error dynamics of the systems, confirming that the error converges to zero over a finite time. Which verifies that systems (5) and (6) can achieve synchronization in a finite time.

4 ALGORITHM

In the following subsection, we study the unique feature of our encryption technique. Our encryption method incorporates plaintext-related random sequences, decimal-level scrambling, decimal-level diffusion, Arnold scrambling, and Henon diffusion. Fig.3. shows a comprehensive flow diagram of our encryption method. The process of encryption is described in the subsequent subsection, assuming the dimensions of the plain image are $M \times N \times 3$.

4.1 Generating the keystreams

The steps for generating the keystreams can be separated into two stages, which involve generating random sequences using the 4D hyper chaotic system and 2D-EHM. Here are the specific details of the implementation.

Step 1 Replace the initial conditions and parameter values $g_1(0) = 0.5648,\ g_2(0) = 0.9845,$ and $\varphi = 0.9137,$ $\zeta = 0.9678,$ respectively, into Eq. 3, then apply 2D-EHM for $3MN$ times to create two sequences, as follows:

$$\begin{cases} G_1 = \{g_1(1), g_1(2), ..., g_1(3MN)\}, \\ G_2 = \{g_2(1), g_2(2), ..., g_2(3MN)\}. \end{cases} \tag{20}$$

Step 2 Set up the values $y_1(0) = 0.2345$, $y_2(0) = 0.9873$, $y_3(0) = 0.9137$, and $y_4(0) = 0.8246$ into Eq. (1) and perform the 4D hyper chaotic system for $MN + 700$ iterations to produce six random sequences, as follows:

$$\begin{cases} x = \{y_1(1), y_2(2), ..., y_1(MN + 700)\}, \\ y = \{y_2(1), y_2(2), ..., y_2(MN + 700)\}, \\ z = \{y_1(1) + y_2(1), y_1(2) + y_2(2), ..., y_1(MN + 700) + y_2(MN + 700)\}, \\ u = \{y_3(1), y_3(2), ..., y_3(MN + 700)\}, \\ v = \{y_4(1), y_4(2), ..., y_4(MN + 700)\}, \\ w = \{y_3(1) + y_4(1), y_3(2) + y_4(2), ..., y_3(MN + 700) + y_4(MN + 700)\}. \end{cases} \tag{21}$$

Step 3 In order to set up for further processing, it is necessary to perform additional preliminary processing on each of these six sequences by

$$\begin{cases} y_1(i) = \mathrm{mod}(round(y_1(i) \times 10^3), p) + 1, \\ y_2(i) = \mathrm{mod}(round(y_2(i) \times 10^3), p) + 1, \\ y_3(i) = \mathrm{mod}(round(y_3(i) \times 10^3), p) + 1, \\ y_4(i) = \mathrm{mod}(round(y_4(i) \times 10^3), p) + 1. \end{cases} \tag{22}$$

Where $i \in [1, MN + 700]$, the function round (a) gives the nearest integer to a using computing rule and the function mod (a, b) evaluates the modulo of a on b.

In addition to the operation mentioned above, eight keystreams are obtained for use in the later encryption. G_1 and G_2 are two sequences utilized for Henon diffusion. Sequences x, y, z, u, v, and w have been used for decimal-level scrambling and diffusion.

4.2 Image encryption and decryption scheme

Here is an overview of the image encryption technique, as follows:

Step 1 Initiate with a $M \times N \times 3$ plain RGB image P, represented by matrix B_1.

- Generate six chaotic sequences $[x, y, z, u, v, w]$, integrating a 4D hyper chaotic system using initial conditions $y_1(0)$, $y_2(0)$, $y_3(0)$, and $y_4(0)$.
- Organize the six chaotic sequences into 2 matrices $m_1(x, y, z)$, and $m_2(u, v, w)$, with each matrix possessing a size of $M \times N \times 3$.
- Covert the chaotic matrices to the $unit8$ representation.

$$\begin{cases} m_1(t) = \text{mod}(\ floor(m_1, M \times N) + 1, t \in [1, M \times N \times 3]), \\ m_2(t) = \text{mod}(\ floor(m_2, M \times N) + 1, t \in [1, M \times N \times 3]). \end{cases} \tag{23}$$

Step 2 Create a zero matrix B_2 with dimensions $M \times N \times 3$.

- Separate m_1 into $m_1 1,\ m_1 2,\ m_1 3$.
- Perform scrambling operations on the RGB channels of matrix B_1 to generate matrix B_2.

$$\begin{cases} Swap(B_1 1(t), B_1 2(m_1 1(t)), t \in [1, M \times N]) \\ Swap(B_1 2(t), B_1 2(m_1 2(t)), t \in [M \times N, 2 \times M \times N]) \\ Swap(B_1 2(t), B_1 3(m_1 3(t)), t \in [2 \times M \times N, 3 \times M \times N]) \end{cases} \tag{24}$$

$$B_2(t) = B_1(t), t \in [1, M \times N \times 3] \tag{25}$$

Step 3 Create a zero matrix B_3 of size $M \times N \times 3$.

- Perform a bitwise XOR operation between each pixel of matrix B_2 and the corresponding values from sequence s_2.

$$B_3 = bitxor(B_2(t), m_2(t)), t \in [1, M \times N \times 3] \tag{26}$$

Step 4 Utilize the diffused image matrix B_3.

- Set $m = 3$ and $n = 5$ as the parameters of the Arnold map.
- Apply the Arnold map scrambling technique on B_3.
- Store the scrambled output in matrix B_4.

Step 5 Use the matrix B_4 and the sequences G_1 and G_2.

- Reshape G_1 and G_2 into matrices:

$$\begin{cases} GG_1 = unit8(reshape(\ floor(G_1(1: M \times 3N) \times 10^{12} \bmod 256), M, 3N)), \\ GG_2 = unit8(reshape(\ floor(G_2(1: M \times 3N) \times 10^{12} \bmod 256), M, 3N)). \end{cases} \tag{27}$$

- Perform cross-plane diffusion on B_4 using GG_1 and GG_2, resulting in the Cipher image C with size $M \times N \times 3$.

Because our technique is reversible, the decoding procedure is simply the opposite of the encoding procedure.

5 EXPERIMENTAL RESULTS AND ANALYSIS

The experiments were performed on a laptop with an Intel (R) Core i5-10300H 2.50 GHz CPU, 32 GB of RAM and a 512 GB SSD, running the window 11 operating system. The encryption algorithm was implemented using MATLAB R2023a. We choose the experimental images peppers, airplane, and baboon, all of which have dimensions of $512 \times 512 \times 3$. However, the initial values and parameters of the 4D hyper chaotic system defined as $y_1(0) = 0.2345,\ y_2(0) = 0.9873,\ y_3(0) = 0.9137,\ y_4(0) = 0.8246$ and $\sigma = 10$, $\gamma = 8/3$, $\rho = 22$, $m = 8$, $n = 0.01$, respectively. Fig. 4(a), 4(d) and 4(g) display the original images of Airplane, Peppers and Baboon, respectively. The associated encrypted images are presented in Fig. 4(b), 4(e) and

4(h), respectively. Additionally, the decrypted version of encrypted images of Airplane (Fig. 4(b)), Peppers (Fig. 4(e)), and Baboon (Fig. 4(h)) are shown in Fig. 4(c), 4(f), and 4(i), respectively.

In addition, we conducted standard security tests on three colour images (i.e., Airplane, Peppers, and Baboon) collected from a collection of conventional test images to support the strength of our method. The findings of these analyses were discussed in the subsequent subsections.

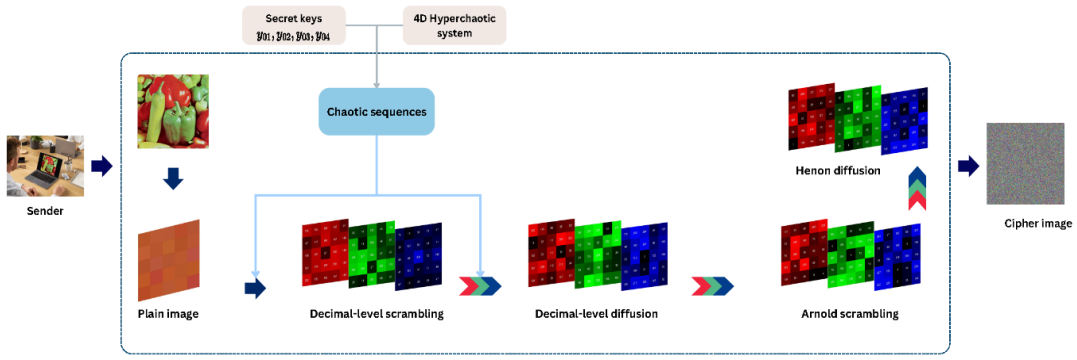


Fig. 3. Flow chart of proposed image encryption scheme.

5.1 Key Space Analysis

The resistance of the encrypted algorithm against a brute-attack can be tested by key space analysis, and it must exceed the ideal value of 2^{128}. The algorithm's Key consists of the parameters y_1, y_2, y_3, y_4, g_1, g_2, p_i and q_i. The Key space formed by them can be outlined below:

$$10^{15\times 8} = 10^{120} > 2^{128}. \tag{28}$$

This shows that our encryption algorithm is unbreakable by brute-force attack with our present processing power.

5.2 Histogram analysis

Histograms are a simple way of visualizing the distribution of pixels in an image. A histogram with a more uniform distribution indicates that the information contained in the image is more unpredictable. Fig.5. presents the histograms from various original images alongside their corresponding cipher images. We observed that the histograms of the encrypted images produced by our method show a consistent distribution. This consistency further shows the algorithm's outstanding resistance to statistical attacks and its universality by blocking attackers from gathering any information about the source images.

5.3 Correlation coefficient analysis

Original images often show a significant correlation between neighboring pixels. Although encryption algorithms attempt to reduce these connections, simple encryption methods frequently face complications in achieving this, which might expose the algorithm to attacks. In order to test the performance of our encryption scheme, we performed an analysis of the correlation coefficients of images using the mathematical formula described in reference [19].

For this study, we sampled 3000 pairs of neighboring pixels from both the original and encrypted airplane image in a chaotic way. The outcomes for the airplane image are shown in Fig. 6.

The research clearly shows a robust correlation in the original image. However, the association between pixels in the encrypted image is extensively decreased, consequently masking the image's information. Furthermore, the correlation coefficient of the encrypted image produced by our technique is closer to zero, indicating its greater capacity to endure statistical attacks.

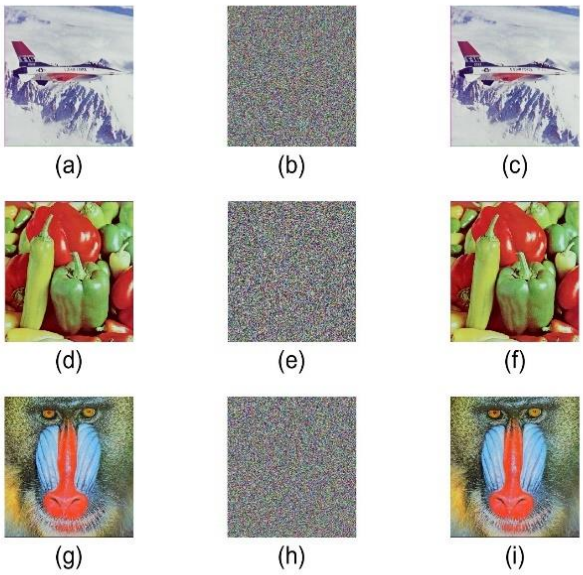


Fig. 4. Experimental results: (a) Plain image of Airplane (b) Cipher image of Airplane (c) Decrypted image of Airplane (d) Plain image of Peppers (e) Cipher image of Peppers (f) Decrypted image of Peppers (g) Plain image of Baboon (h) Cipher image of Baboon (i) Decrypted image of Baboon.

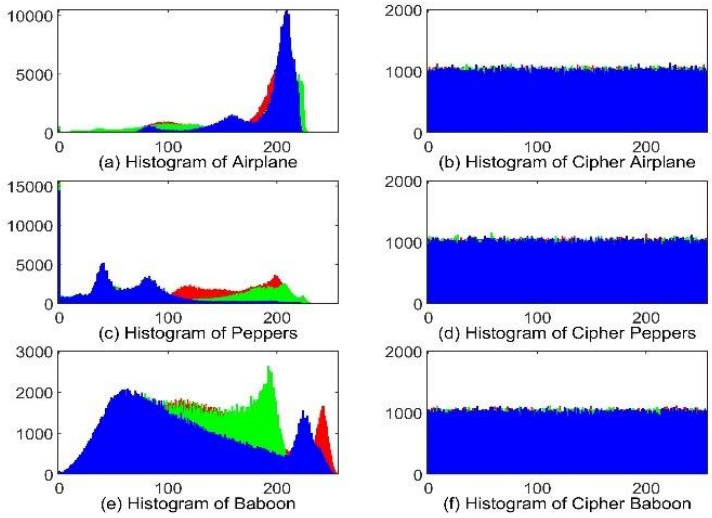


Fig. 5. Histogram analysis results.

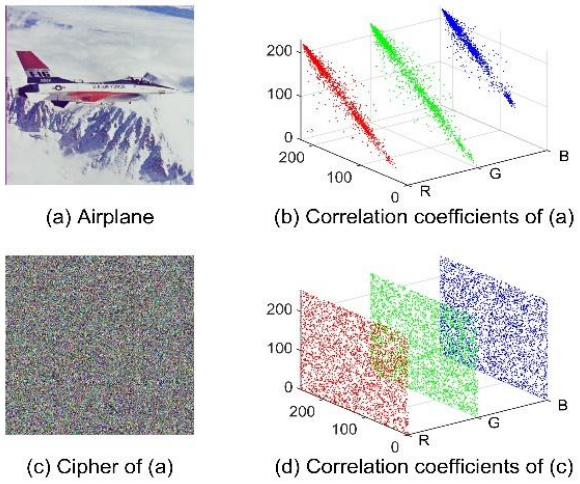


Fig. 6. Correlation plots of the airplane and its cipher image.

5.4 Information entropy analysis

Entropy is an important parameter used to measure the degree of inconsistency in a grayscale image. For an 8-bit image, an efficient encryption system would ensure that the entropy of its cipher image is about 8. The mathematical description of the information entropy can be stated by equation (29), as described in reference [20]:

$$E(s) = \sum_{j=0}^{2^P-1} Q(s_j) \log_2 \frac{1}{Q(s_i)}. \tag{29}$$

Where s_j denotes the numerical values assigned to each pixel in an image; the notation $Q(s_j)$ represents the probability of s_j.

P is the number of bits. Table I, clearly shows that the entropy value of our encryption system nearly approaches the theoretical highest value of 8.

TABLE I
Information entropy

	Plain image			Cipher image		
image	R	G	B	R	G	B
Airplane	6.7178	6.7990	6.2138	7.9993	7.9993	7.9993
Baboon	7.7068	7.4744	7.7522	7.9993	7.9994	7.9992
Peppers	7.3388	7.4963	7.0583	7.9993	7.9993	7.9993

5.5 Key Sensitivity analysis

This subsection of the article discusses the sensitivity of the key. Initially, the color image of the peppers is encrypted using our encryption method with key K1. The values assigned to K1 are the

parameters and initial values of 2D-EHM, as follows: $g_1(1) = 0.5648$, $g_2(1) = 0.9845$ and $\varphi = 0.9137$, $\zeta = 0.9678,$ respectively. Subsequently, a modified key, K2, is used to decrypt the image. The values assigned to the parameters and initial values K2 are as follows: $g_1(1) = 0.5648000001$, $g_2(1) = 0.9845$, and $\varphi = 0.9137$, $\zeta = 0.9678,$ respectively. Fig.7. shows the original image of peppers in (a), the encoded image using the key K1 shown in (b), the image that has been decoded using the 2nd and 1st keys shown in (c), and (d) accordingly. The results clearly suggest that even a small alteration in the initial values can lead to a substantial change in the final output, suggesting that the proposed system is robust against threats.

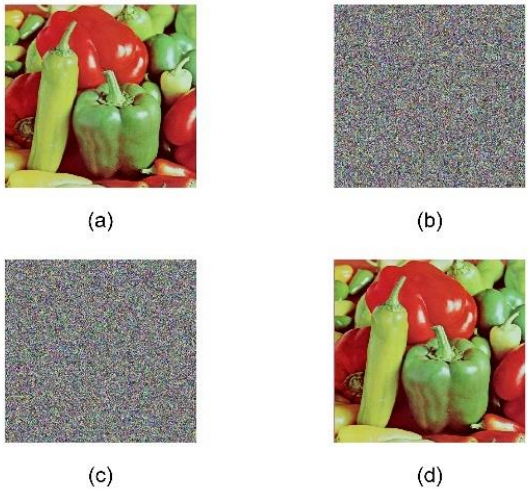


Fig. 7. Key sensitivity test: (a) Original image; (b) Encoded image using key K1; (d) Decoded image using key K2; (d) Decoded image using key K1.

6 CONCLUSION

This study identified the success of developing an image encryption scheme using a novel 4D hyper-chaotic system that utilizes synchronized chaos for both encryption and decryption methods. Our method integrates the use of Arnold map scrambling and Henon map diffusion, leading to strong security features. This can be seen by the existence of nearly ideal entropy levels, uniformly distributed histogram variation, high sensitivity to the encryption key, and a wide range of key combinations.

The research goal was successfully attained, showing that synchronization may significantly improve encryption systems. In the context of these achievements, it would be useful to conduct more investigations into other chaotic maps and evaluate their resilience against complex cryptographic attacks.

By utilizing the complex nature of chaotic systems, this method shows potential for improving secure digital communication.

REFERENCES

[1] Y. Zhang, "A chaotic system based image encryption scheme with identical encryption and decryption algorithm," *Chinese Journal of Electronics,* vol. 26, no. 5, pp. 1022-1031, 2017.

[2] G. Li and B. Zhang, "A novel weak signal detection method via chaotic synchronization using Chua's circuit," *IEEE transactions on industrial electronics,* vol. 64, no. 3, pp. 2255-2265, 2016.

[3] J. L. Mata-Machuca, R. Martínez-Guerra, R. Aguilar-López, and C. Aguilar-Ibañez, "A chaotic

system in synchronization and secure communications," *Communications in Nonlinear Science and Numerical Simulation,* vol. 17, no. 4, pp. 1706-1713, 2012.
[4] H. Tian, Z. Wang, H. Zhang, Z. Cao, and P. Zhang, "Dynamical analysis and fixed-time synchronization of a chaotic system with hidden attractor and a line equilibrium," *The European Physical Journal Special Topics,* vol. 231, no. 11, pp. 2455-2466, 2022.
[5] N. Jiang, K. Sun, K. Li, L. Liu, and R. Guo, "Complete Synchronization of Lorenz System with Unbounded External Disturbance by DE-Based Controller," in *2023 42nd Chinese Control Conference (CCC)*, 2023: IEEE, pp. 1-6.
[6] E. Ozpolat and A. Gulten, "A novel 4D hyperchaotic system with its dynamical analysis and synchronization," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 2023: IEEE, pp. 1-5.
[7] T. Sangpet and S. Kuntanapreeda, "Finite-time synchronization of hyperchaotic systems based on feedback passivation," *Chaos, Solitons & Fractals,* vol. 132, p. 109605, 2020.
[8] G. Laarem, "A new 4-D hyper chaotic system generated from the 3-D Rösslor chaotic system, dynamical analysis, chaos stabilization via an optimized linear feedback control, it's fractional order model and chaos synchronization using optimized fractional order sliding mode control," *Chaos, Solitons & Fractals,* vol. 152, p. 111437, 2021.
[9] M. Dua, A. Wesanekar, V. Gupta, M. Bhola, and S. Dua, "Differential evolution optimization of intertwining logistic map-DNA based image encryption technique," *Journal of Ambient Intelligence and Humanized Computing,* vol. 11, pp. 3771-3786, 2020.
[10] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in engineering,* vol. 88, pp. 197-213, 2017.
[11] J. Zhang, Z. Huang, X. Li, M. Wu, X. Wang, and Y. Dong, "Quantum image encryption based on quantum image decomposition," *International journal of theoretical physics,* vol. 60, pp. 2930-2942, 2021.
[12] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm," *Neural Computing and Applications,* vol. 34, no. 21, pp. 19313-19341, 2022.
[13] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Processing,* vol. 176, p. 107684, 2020.
[14] J. Xu, C. Zhao, and J. Mou, "A 3D image encryption algorithm based on the chaotic system and the image segmentation," *IEEE Access,* vol. 8, pp. 145995-146005, 2020.
[15] Q. Yang and G. Chen, "A chaotic system with one saddle and two stable node-foci," *International Journal of Bifurcation and Chaos,* vol. 18, no. 05, pp. 1393-1414, 2008.
[16] S. Zhou, Y. Qiu, X. Wang, and Y. Zhang, "Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box," *Nonlinear Dynamics,* vol. 111, no. 10, pp. 9571-9589, 2023.
[17] K. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *Journal of Information Security and Applications,* vol. 50, p. 102428, 2020.
[18] S. P. Bhat and D. S. Bernstein, "Finite-time stability of continuous autonomous systems," *SIAM Journal on Control and optimization,* vol. 38, no. 3, pp. 751-766, 2000.
[19] A. Latoui and M. E. H. Daachi, "A two-parameter extended logistic chaotic map for modern image cryptosystems," *Digital Signal Processing,* vol. 148, p. 104463, 2024.
[20] C. He, Z. Chen, L. Wang, X. Wu, T. Liu, and B. Long, "An algorithm based on 6D fractional order hyperchaotic system and knight tour algorithm to encrypt image," *Physica Scripta,* vol. 99, no. 5, p. 055205, 2024.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Dominating Sets in Bipolar Fuzzy Graphs

Sahar Motlagh

Department of Mathematics, Faculty of Mathematical Sciences, University of Mazandaran,

Babolsar, Iran

s.motlagh02@stu.umz.ac.ir

Ali Asghar Talebi
Department of Mathematics, Faculty of Mathematical Sciences, University of Mazandaran,
Babolsar, Iran
a.talebi@umz.ac.ir

ABSTRACT

Most of the current research on domination deals only with ordinary fuzzy systems, but in this paper we present certain computational properties of bipolar fuzzy graphs for the first time and examine the limitations of current methods. Bipolar fuzzy graphs allow us to model conflicting attributes. Let V be a set of vertices and E be a set of edges in a bipolar fuzzy graph G = $(\sigma^+, \sigma^-, \mu^+, \mu^-)$. A set of vertices S⊆ V in the BFG G is a dominating set if every vertex in V - S has at least one neighbor in S. Every bipolar fuzzy graph contains multitude dominating sets such that their strength differs from each other. This paper introduce the concept of strength of dominating sets in bipolar fuzzy graphs.

KEYWORDS: Dominating set; Strength of dominating set; Bipolar fuzzy graphs

1 INTRODUCTION

In 1994, Zhang et al. [4] initiated the concept of bipolar fuzzy sets as a extension of Zadeh's fuzzy set theory. In a bipolar fuzzy set, each element has a membership degree range between [-1,1], such that the zero degree membership of a member shows that irrelevance of the member to the corresponding property, the membership degree between (0,1] indicates that the element somewhat satisfies the property, and the membership degree [-1,0) indicates the element dissatisfaction of the implicit property. Utilizing effective edges, Somasundaram [6,7] explored domination in fuzzy graphs. Zhang et al. [4] developed the concept of bipolar fuzzy domination. A bipolar fuzzy graph (BFG) G is defined on a set of vertices V and edges E, represented as G = $(\sigma^+, \sigma^-, \mu^+, \mu^-)$, where: σ^+:X → [0, 1], σ^-:X → [-1, 0], μ^+: V ×V → [0, 1] and μ^-: V ×V → [-1, 0], satisfying:
$\mu^+(v_iv_j) \leq \sigma^+(v_i) \wedge \sigma^+(v_j)$ and $\mu^-(v_iv_j) \geq \sigma^-(v_i) \vee \sigma^-(v_j)$ for all $v_iv_j \in E$. The maximum degree (minimum degree) among all vertices of the bipolar fuzzy graph G is denoted by Δ(G) (δ (G)). A bipolar fuzzy relation A= $(\sigma^+, \sigma^-, \mu^+, \mu^-)$ on X is called symmetric if $\mu^+(v_iv_j) = \mu^+(v_jv_i)$ and $\mu^-(v_iv_j) = \mu^-$

$(v_j v_i)$ for all x, y ∈ X. The vertices with maximum and minimum memberships are v_s and v_w, and similarly, edges with maximum and minimum memberships are e_s and e_w. Let G be a BFG on V and u,v ∈ V, we say that the vertex u dominates v in G, if there μ^+ (uv) >0. A subset S of V is called a dominating set in G, if for every v ∈ V/ S, there exists u ∈ S such that u dominates v. A dominating set S of a BFG is said to be minimal dominating set if no proper subset of S is a dominating set. Minimum (Maximum) cardinality among all minimal dominating set is called lower domination number of G, and is denoted by γ_b(G) . A bipolar fuzzy graph G = (σ +, σ−, μ+, μ−) is called a complete bipolar fuzzy graph on σ = (σ +, σ−) if μ^+ $(v_i v_j)$ = min(σ^+ (v_i), σ^+ (v_j)) and μ^- $(v_i v_j)$= max(σ^- (v_i),σ^- (v_j)) for all $v_i, v_j \in V$, and denoted by K_σ.

Definition 1: Let G = (σ^+, σ^-, μ^+, μ^-) be a bipolar fuzzy graph and S be a dominating set. For two vertices u\in S and v∈ G\S, we define $\bar{\bar{\mu}}$ (u,v)=min{$\frac{1+\mu^+(uv)+\mu^-(uv)}{2}$},$\frac{1+\sigma^+(v)+\sigma^-(v)}{2}$},$\frac{1+\sigma^+(u)+\sigma^-(u)}{2}$},as the *minimum degree* of edge (uv) in the bipolar fuzzy graph G.

Definition 2: For a vertex u ∈ G\S we have sdom(u,S)=max{$\bar{\bar{\mu}}$(u,v)| v ∈ S} as the strength of dominance on v. sdom(G\S, S)=min{sdom(u,S)| u∈ G\S } as the *dominate strength* of S.

Definition 3: The set of minimum dominating sets with maximum sdom (G\S, S) is denoted by S_s(G). Let G be a bipolar fuzzy graph. A set with maximum bipolar fuzzy cardinality between all minimum dominating sets of S_s(G) is called the *strongest dominating set* in the bipolar fuzzy graph G and its bipolar fuzzy cardinality is called strength of strongest dominating set in the bipolar fuzzy graph G and is denoted it by ssd(G).

2. Main results

3. **Theorem 3:** For any bipolar fuzzy graph G = (σ^+, σ^-, μ^+, μ^-) of order p, we have ssd(G) ≤ p, and equality holds if and only if each vertex of G is an isolated vertex.
4. **Proof:** Let G be a bipolar fuzzy graph of order p and S a strongest dominating set of G. Because ssd(G) is the bipolar fuzzy cardinality of and S ⊆ V(G), we have |S| ≤ |V(G)| =$\sum_{v_i \in V}\{\frac{1+\sigma^+(v_i)+\sigma^-(v_i)}{2}\}$ = p. We next prove the equality part. Assume that all vertices of the fuzzy graph G are isolated vertices. Then V(G) is only dominating set of G, and so S = V(G) is the strongest dominating set of G. Thus, ssd(G) = |S|= $\sum_{v_i \in S}\{\frac{1+\sigma^+(v_i)+\sigma^-(v_i)}{2}\}$= $\sum_{v_i \in V}\{\frac{1+\sigma^+(v_i)+\sigma^-(v_i)}{2}\}$ = p. Conversely, let ssd(G) = p. If x is a vertex of G that is not an isolated vertex and is a vertex adjacent to x, then x is dominated by y and the set V(G)\{x} is a dominating set of G, whose order is less than p. Since the order of any other minimum dominating set of is smaller than the order of the dominating set V(G) {x}, implying that ssd(G) <p, a contradiction. Thus each vertex of G is an isolated vertex.
5. **Theorem 4:** For every bipolar fuzzy graph G = (σ^+, σ^-, μ^+, μ^-), we have γ_b(G) ≤ ssd(G).
6. **Proof :** Let S be a dominating set of a bipolar fuzzy graph G such that $|S|= γ_b(G). So S has minimum bipolar fuzzy cardinality among all dominating sets of G. Let S' be a minimum dominating set of S_s(G) with maximum bipolar fuzzy cardinality, and |S'| =ssd(G). Then γ_b(G)= |S|≤ min {|S"|| S"∈ S_s(G)} |≤ max{|S"|| w ∈ S_s(G)}= |S'| = ssd(G).
7. **Proposition 5:** Let G = (σ^+, σ^-, μ^+, μ^-) be a complete bipolar fuzzy graph K_σ. Then $ssd($K_\sigma$) = max{$\frac{1+\sigma^+(v)+\sigma^-(v)}{2}$| v ∈ S}, where S is the set of vertices of K_σ with maximum depth.

8. **Corollary 6** : If D = $\{v_1, v_2, \ldots, v_n\}$ be a dominating set of a bipolar fuzzy graph G = (σ +, σ−, μ+, μ−). For a vertex u ∈ D \ S, we define sdom(u, D) = $d_b\ (v_1) \wedge d_b\ (v_2). \ldots, d_b\ (v_n)$ such that $d_b(v_i)$ is the depth of the vertex v_i for i = 1, 2, . . . n in the bipolar fuzzy graph G.
9.
10. **Example 7:** Let G = (V, E) be a bipolar fuzzy graph and V = $\{v_1, v_2, \ldots, v_5\}$ given in Figure 1.

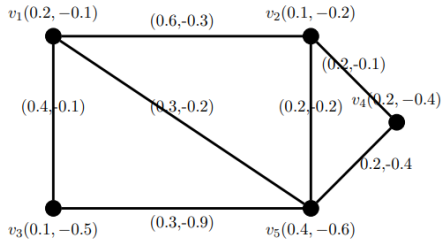


Figure 1: a bipolar fuzzy graph

For this bipolar fuzzy graph, the subsets $S_1 = \{v_1, v_2\}$, $S_2 = \{v_5, v_1\}$, $S_3 = \{v_5, v_4\}$ and $S_4 = \{v_3, v_5\}$ are minimum dominating sets. Now we calculate sdom(G \ S_i , S_i) for i = 1, 2, 3, 4. For S_1 we have sdom(v_3, S_1) = 0.3, sdom(v_4, S_1) = 0.4, sdom(v_5, S_1) = 0.4. So sdom(G \ S_1, S_1) = 0.3. For S_2 we have sdom(v_2, S_2) = 0.4, sdom(v_3, S_2) = 0.3, sdom(v_4, S_2) = 0.4. So sdom(G \ S_2, S_2) = 0.3. For S_3 we have sdom(v_1, S_3) = 0.4, sdom(v_2, S_3) = 0.4 sdom(v_3, S_3) = 0.3. So sdom(G \ S_3, S_3) = 0.3. Finally for S_4we have sdom(v_1, S_4) = 0.4, sdom(v_2, S_4) = 0.4, sdom(v_4, S_4) = 0.4. So sdom(G \ S_4, S_4) = 0.4. Then S_s= $S_4$and $S_4$is the strongest dominating set of bipolar fuzzy graph G and ssd(G) = |S4| = 0.3 + 0.4 = 0.7.

2 CONCLUSION

In this paper, we introduced the concept of domination and the strength of dominating sets in bipolar fuzzy graph, as well as the concept of strongest dominating set in bipolar fuzzy graphs, using membership and non-membership values. We expand the research on domination in Fuzzy graph theory to the framework of bipolar fuzzy systems. One illustrative example is also added. The results discussed may be useful for further research in domination properties of bipolar fuzzy graphs

REFERENCES

[1] J.N. Mordeson and P.S. Nair, Fuzzy Graphs and Fuzzy Hypergraphs, vol. 46, Physicaverlage, Heidelberg, New York, 2012.

[2] A. Rosenfeld, Fuzzy graphs, in: L.A. Zadeh, K.S. Fu, M. Shimura (Eds.), Fuzzy Sets and their Applications, Academic Press, New York, 1975, pp. 77– 95.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] T. Madhavi and A. John Arul Smija, Bipolar fuzzy graph model with application to human traff icking, 2013R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] W.-R. Zhang, Bipolar fuzzy sets, in: Proceedings of FUZZ-IEEE, 1998, pp. 835– 840M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] W.-R. Zhang, Bipolar fuzzy sets, in: Proceedings of FUZZ-IEEE, 1998, pp. 835– 840

[6] Somasundaram A (2005) Domination in products of fuzzy graphs. Int J Uncertain Fuzziness Knowl Based Syst 13(2):195–204.

[7] Somasundaram A, Somasundaram S (1998) Domination in fuzzy graphs-i. Pattern Recogn Lett 19(9):787–791.

[8] M.Akram, M.G.Karunambigai and K.Palanivel, Domination in Bipolar Fuzzy Graphs, 2013 FUZZ-IEEE International Conference on Fuzzy Systems July 7-10, 2013, Hyderabad, India

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

M-Polynomials and Banhatti indices in $HAC_5C_6C_7[p,q]$ nanotubes

Fatemeh Shirkhani[1], Jaber Ramezani Tousi[2], Ali Asghar Talebi[3]
1.University of Mazandaran, Department of Mathematics
Babolsar 4741613534, Iran
f.shirkhani01@umail.umz.ac.ir
2.University of Mazandaran, Department of Mathematics
Babolsar 4741613534, Iran
jaber.ramezani@umz.ac.ir
3.University of Mazandaran, Department of Mathematics
Babolsar 4741613534, Iran
a.talebi@umz.ac.ir

ABSTRACT

Graph theory of chemistry is an interdisciplinary science that is used to study molecular structures and create correlations between different activities, properties, and events. Carbon nanotubes are cylinders of carbon with wall diameters in the nanometer range. The mass production of multi-walled nanotubes, the abundance of the product, the cheapness of raw materials, the low production of by-products, and the low energy usage have made the production of these tubes cheap.
In this article, first, M-polynomials are calculated for molecular graph, line graph, and subdivision graph of $HAC_5C_6C_7[p,q]$ nanotubes. Then, using M-polynomials, Banhatti indices are obtained, and the results are expressed.

KEYWORDS: M-Polynomials, Banhatti indices, Molecular graph, nanotube, Line graph, Subdivision graph.

1 INTRODUCTION

Carbon nanotubes (CNTs) are types of nanostructures that are carbon allotropes and have a cylindrical shape. One of the best and most widely used carbon structures is carbon nanotubes, which in addition to high durability, also have good flexibility and conductivity.
In nanoscience, the study of atomic, molecular, and macromolecular dimensions was discussed, and research in these dimensions led to a drastic change in the properties of materials. Numerical calculations are of particular importance in nanoscale simulations.
The molecular graph is related to the structural formula of a chemical compound, and the vertices and edges of the graph correspond to the atoms and chemical bonds of the compound, respectively. Chemical graph theory has provided creative and unique tools for the study of chemical structures, among which topological indices can be mentioned.
The topological index is used as the descriptor to study the structure and some properties of a molecular graph and is expressed as a real number [2, 3, 10].
Many studies were conducted on molecular graphs, especially nanotubes, and pharmaceutical structures, using topological indices [4, 5, 6, 7, 8, 9, 11].
One of the practical tools in the study of topological indices is M-polynomial [1]. Topological indices can also be calculated using mathematical operations on M-polynomial. Therefore, from a computational and mathematical point of view, determining topological indices as M-polynomials is very important.

In this article, the Banhatti indices of $HAC_5C_6C_7[p,q]$ nanotubes are studied using the M-polynomial approach.

2 PRELIMINARIES

This section provides some definitions needed. Suppose *G = (V, E)* is a simple and connected graph. We denote the degree of vertex u by d_u and if there is an edge between two vertices u, v, denote by $uv \in E(G)$.

In graph G, we represent the minimum vertex degree by $\delta(G)$ and the maximum vertex degree by $\Delta(G)$.

2.1 Definition

The M-Polynomial of graph G is defined as [1]:

$$M(G;\mathrm{x},\mathrm{y}) = \sum_{\delta \le i \le j \le \Delta} m_{ij}(G)x^i y^j.$$

Where $m_{ij}(G)$ is the number of edges $uv \in E(G)$ such that $d_u = i$ and $d_v = j$.

Some operators, which are used further, are defined as:

$$D_x M(G;\mathrm{x},\mathrm{y}) = x \times \frac{\partial M(G;\mathrm{x},\mathrm{y})}{\partial x}, \quad (1)$$

$$D_y M(G;\mathrm{x},\mathrm{y}) = y \times \frac{\partial M(G;\mathrm{x},\mathrm{y})}{\partial y}, \quad (2)$$

$$Q_{x(\alpha)} M(G;\mathrm{x},\mathrm{y}) = x^{\alpha} M(G;\mathrm{x},\mathrm{y}), \quad (3)$$

$$Q_{y(\alpha)} M(G;\mathrm{x},\mathrm{y}) = y^{\alpha} M(G;\mathrm{x},\mathrm{y}). \quad (4)$$

The conceptual δ-vertex degree in graph G is defined by as [8]:

$$\delta_u = d_u - \delta(G) + 1.$$

And the degree of an edge *"e"* is denoted by d_e, where $d_e = d_u + d_v - 2$.

Table (1) lists Banhatti indices and how to derive them from the M-polynomial [8].

Table 1- Derivation of Banhatti indices from M-polynomial.

Topological Index	**Formula**	**Drivation from *M(G; x, y)***
First K-Banhatti [2]	$\sum_{re}[d_r + d_e]$	$2D_x + 3D_y + D_X Q_{X(-4)} M(G;x,y)\|_{x=y=1}$
Second K-Banhatti [2]	$\sum_{re}[d_r . d_e]$	$\left(D_x^2 + D_y^2 + 2D_x D_y - 2(D_x + D_y)\right) M(G;x,y)\|_{x=y=1}$
First δ -Banhatti [2]	$\sum_{rs \in E(G)} (\delta_r + \delta_s)$	$(D_x + D_y)\left(Q_{x(-\delta+1)} Q_{y(-\delta+1)}\right) M(G;x,y)\|_{x=y=1}$
Second δ -Banhatti [2]	$\sum_{rs \in E(G)} \delta_r . \delta_s$	$(D_x D_y)\left(Q_{x(-\delta+1)} Q_{y(-\delta+1)}\right) M(G;x,y)\|_{x=y=1}$

2.2 Definition

In a non-empty graph G, if each edge is considered as a vertex and the two vertices are connected, if the corresponding edges of the two vertices are adjacent to G, the resulting graph is denoted by L(G) and is called the line graph of G [3].

2.3 Definition

Subdivision graph of graph G is a graph obtained by placing an extra vertex on each edge of G. In other words, each edge G is replaced by a path of length 2. The subdivision graph is denoted by S(G) [3].

In $HAC_5C_6C_7[p,q]$ nanotube, p represents the number of pentagons in a row, and q represents the number of periods, a period consisting of the first three rows with all its vertices and edges.

Figure (1) shows a section of nanotube $HAC_5C_6C_7[4,2]$ with its number of vertices.

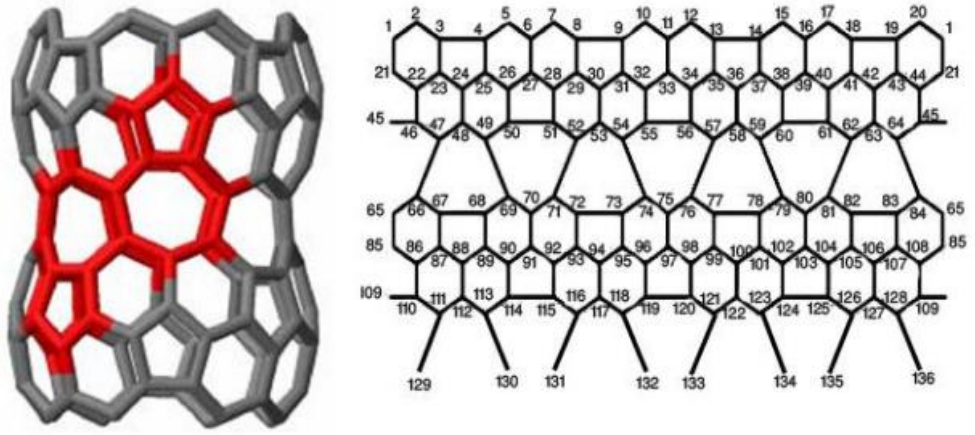


Figure 1: $HAC_5C_6C_7[p,q]$ nanotube.

Figure (2) and Figure (3) show the line graph and the subdivision graph of nanotube $HAC_5C_6C_7[p,q]$, respectively.

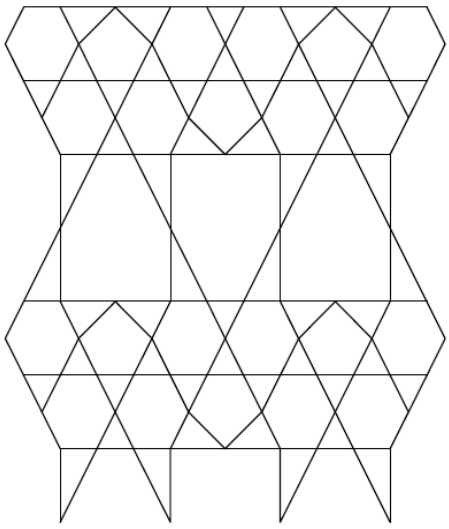


Figure 2- $L(HAC_5C_6C_7[2,2])$.

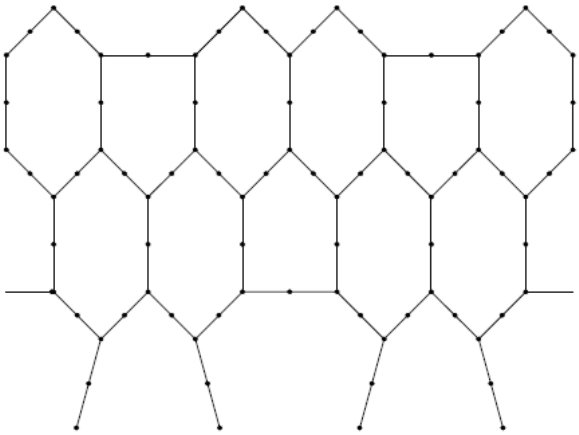


Figure 3- $S(HAC_5C_6C_7[2,1])$.

3 MAIN RESULTS

In the following, M-polynomials, Banhatti indices are obtained in the general case of $HAC_5C_6C_7[p,q]$ nanotubes.

There are four types of edges in $HAC_5C_6C_7[p,q]$ as follows:

$e_1=\{(d_u,d_v)|uv\in E(G),d_u=1,d_v=3\}$, $e_2=\{(d_u,d_v)|uv\in E(G),d_u=2,d_v=2\}$,

$e_3=\{(d_u,d_v)|uv\in E(G),d_u=2,d_v=3\}$, $e_4=\{(d_u,d_v)|uv\in E(G),d_u=3,d_v=3\}$.

We want to calculate the number of edges and the types of the above edges and obtain a general formula for it by generalizing it to the nanotube.

We have the following table for nanotubes:

Table 2- Types and number of $HAC_5C_6C_7[p,q]$ edges.

Number of edges	Edge type
2p	e_1
2q+2	e_2
8q+4p-4	e_3
24pq-10q-6p+2	e_4

There are six types of edges in $L(HAC_5C_6C_7[p,q])$ as follows:

$e_1'=\{(d_u,d_v)|uv\in E(L(G)),d_u=2,d_v=2\}$, $e_2'=\{(d_u,d_v)|uv\in E(L(G)),d_u=2,d_v=3\}$,

$e_3'=\{(d_u,d_v)|uv\in E(L(G)),d_u=2,d_v=4\}$, $e_4'=\{(d_u,d_v)|uv\in E(L(G)),d_u=3,d_v=3\}$,

$e_5'=\{(d_u,d_v)|uv\in E(L(G)),d_u=3,d_v=4\}$, $e_6'=\{(d_u,d_v)|uv\in E(L(G)),d_u=4,d_v=4\}$.

The number of edges is calculated and by generalizing it to the nanotube line graph, a general formula is obtained for it.

We have the following table for the $L(HAC_5C_6C_7[p,q])$ line graph:

Table 3- Types and number of $L(HAC_5C_6C_7[p,q])$ edges.

Number of edges	Edge type
2	e_1'
4q+2	e_2'
4p-2	e_3'
4q+3p-3	e_4'
12q+6p-8	e_5'
48pq-26q-16p+9	e_6'

There are three types of edges in $S(HAC_5C_6C_7[p,q])$ as follows:

$e_1''=\{(d_u,d_v)|uv\in E(S(G)),d_u=1,d_v=2\}$, $e_2''=\{(d_u,d_v)|uv\in E(S(G)),d_u=2,d_v=2\}$ *and*

$e_3''=\{(d_u,d_v)|uv\in E(S(G)),d_u=2,d_v=3\}$.

Table 4- Types and number of $S(HAC_5C_6C_7[p,q])$ edges.

Number of edges	Edge type
2p	e_1''
12q+4p	e_2''
48pq-12q-6p	e_3''

3.1 THEOREM

Suppose *G*, *G'* and *G"* are the molecular graph, the line graph and the subdivision graph $HAC_5C_6C_7[p,q]$ nanotube, respectively. Then their M-polynomials are as follows:

$$M(G;\mathrm{x},\mathrm{y}) = (2\,\mathrm{p})x^1y^3 + (2\,\mathrm{q}+2)x^2y^2 + (8q+4p-4)x^2y^3 + (24pq-10q-6p+2)x^3y^3, \quad (1)$$

$$M(G';\mathrm{x},\mathrm{y}) = (2)x^2y^2 + (4q+2)x^2y^3 + (4p-2)x^2y^4 + (4q+3p-3)x^3y^3 + (12q+6p-8)x^3y^4 + (48pq-26q-16p+9)x^4y^4, \quad (2)$$

$$M(G'';\mathrm{x},\mathrm{y}) = (2)x^2y^2 + (4q+2)x^2y^3 + (4p-2)x^2y^4 + (4q+3p-3)x^3y^3 + (12q+6p-8)x^3y^4 + (48pq-26q-16p+9)x^4y^4. \quad (3)$$

Proof:
By substituting the values of Tables 2, 3, and 4 into Definition 1, the proof is complete. □

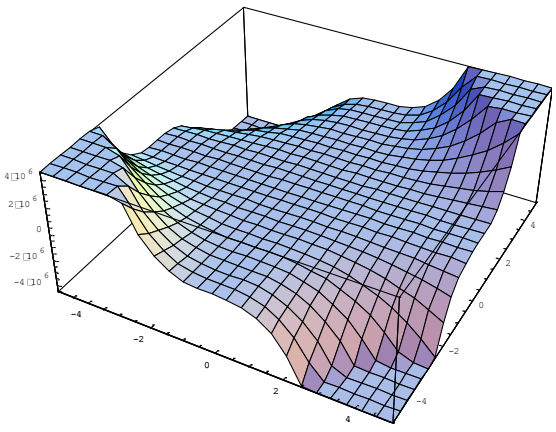


Figure 4- M-polynomial of $HAC_5C_6C_7[10,10]$.

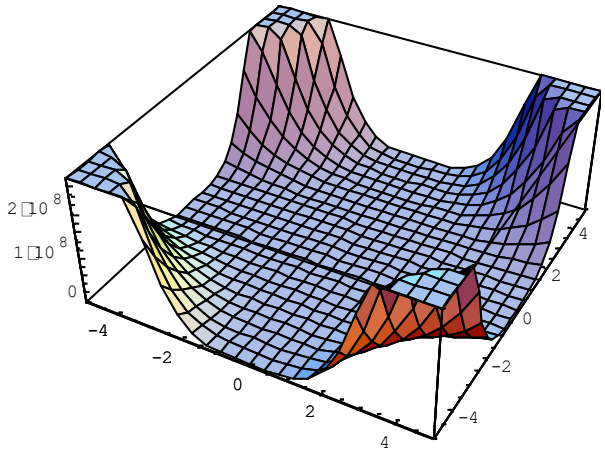


Figure 5- M-polynomial of $L(HAC_5C_6C_7[10,10])$.

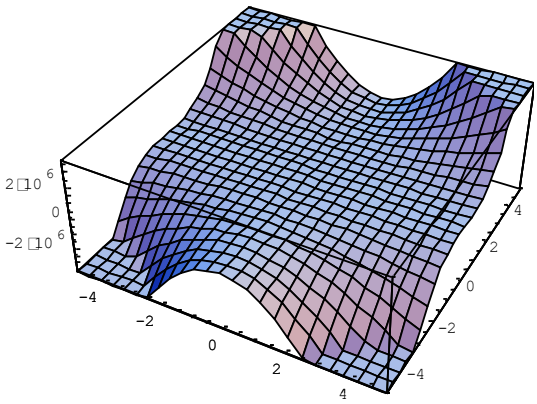


Figure 6- M-polynomial of $S(HAC_5C_6C_7[10,10])$.

3.2 THEOREM

Let *G* be the graph of $HAC_5C_6C_7[p,q]$ nanotube. Then,

$$B_1(G) = 336pq - 34q - 24p + 2, \quad (1)$$

$$B_2(G) = 576pq - 104q - 68p + 4, \quad (2)$$

$$\delta B_1(G) = 144pq - 12q - 8p - 18, \quad (3)$$

$$\delta B_2(G) = 216pq - 34q - 24p + 2. \quad (4)$$

Proof:

Let $M(G) = (2\,\mathrm{p})x^1y^3 + (2\,\mathrm{q}+2)x^2y^2 + (8q+4p-4)x^2y^3 + (24pq-10q-6p+2)x^3y^3$,

Then,

$$D_x(M(G;\mathrm{x},\mathrm{y})) = (2\,\mathrm{p})x^1y^3 + 2(2\,\mathrm{q}+2)x^2y^2 + 2(8q+4p-4)x^2y^3 + 3(24pq-10q-6p+2)x^3y^3.$$

$$D_y(M(G;\mathrm{x},\mathrm{y})) = 3(2\,\mathrm{p})x^1y^3 + 2(2\,\mathrm{q}+2)x^2y^2 + 3(8q+4p-4)x^2y^3 + 3(24pq-10q-6p+2)x^3y^3.$$

$$D_xD_y(M(G;\mathrm{x},\mathrm{y})) = 3(2\,\mathrm{p})x^1y^3 + 4(2\,\mathrm{q}+2)x^2y^2 + 6(8q+4p-4)x^2y^3 + 9(24pq-10q-6p+2)x^3y^3.$$

$$D_y^2(M(G;\mathrm{x},\mathrm{y})) = 9(2\,\mathrm{p})x^1y^3 + 4(2\,\mathrm{q}+2)x^2y^2 + 9(8q+4p-4)x^2y^3 + 9(24pq-10q-6p+2)x^3y^3.$$

$$D_x{}^2(M(G;\mathrm{x},\mathrm{y})) = (2\,\mathrm{p})x^1y^3 + 4(2\,\mathrm{q}+2)x^2y^2 + 4(8q+4p-4)x^2y^3 + 9(24pq-10q-6p+2)x^3y^3.$$

$$Q_{x(-4)}(M(G;x,y) = (2\,\mathrm{p})x^{-3}y^3 + (2\,\mathrm{q}+2)x^{-1}y^2 + (8q+4p-4)x^{-2}y^3 + (24pq-10q-6p+2)x^{-1}y^3.$$

$$D_xQ_{x(-4)}(M(G;x.y)) = -3(2\,p)x^{-3}y^3 + (-1)(2q+2)x^{-1}y^2 + (-2)(8p+4p-4)x^{-2}y^3$$
$$+ (-1)(24pq-10q-6p+2)x^{-1}y^3$$

we know $\delta(G) = 1$ so $-\delta(G)+1 = 0$ then we have:

$$Q_{x(-\delta+1)}Q_{y(-\delta+1)}(M(G;x,y)) = Q_{x(0)}Q_{y(0)}(M(G;x,y)) = M(G;x,y)$$

Now using table (1) and the relationships above, we have:

$$B_1(G) = 2D_x + 3D_y + D_XQ_{X(-4)}M(G;x,y)\,|_{x=y=1}$$
$$= (8)(2p) + (9)(2q+2) + (11)(8q+4p-4) + (14)(24pq-10q-6p+2) \quad (1)$$
$$= 336pq - 34q - 24p + 2$$

$$B_2(G) = \left(D_x^2 + D_y^2 + 2D_xD_y - 2(D_x + D_y)\right)M(G;x,y)|_{x=y=1}$$
$$= 8(2\,\mathrm{p}) + 8(2\,\mathrm{q}+2) + 15(8q + 4p - 4) + 24(24pq - 10q - 6p + 2) \quad (2)$$
$$= 576pq - 104q - 68p + 4$$
$$\delta B_1(G) = (D_x + D_y)\left(Q_{x(0)}Q_{y(0)}\right)M(G;x,y)|_{x=y=1} = (D_x + D_y)M(G;x,y)|_{x=y=1}$$
$$= 4(2\,\mathrm{p}) + 4(2\,\mathrm{q}+2) + 5(8q + 4p - 4) + 6(24pq - 10q - 6p + 2) \quad (3)$$
$$= 144pq - 12q - 8p - 18$$
$$\delta B_2(G) = (D_xD_y)\left(Q_{x(-\delta+1)}Q_{y(-\delta+1)}\right)D_xD_y(M(G;\mathrm{x},\mathrm{y})) = (D_xD_y)\left(Q_{x(0)}Q_{y(0)}\right)M(G;x,y)|_{x=y=1} \quad (4)$$
$$= (D_xD_y)M(G;x,y)|_{x=y=1} = 3(2\,\mathrm{p}) + 4(2\,\mathrm{q}+2) + 6(8q + 4p - 4) + 9(24pq - 10q - 6p + 2)$$
$$= 216pq - 34q - 24p + 2.\square$$

3.3 THEOREM

Let G' be the Line graph of $HAC_5C_6C_7[p,q]$ nanotube. Then,

$$B_1(G') = 336pq - 34q - 24p + 2, \quad (1)$$
$$B_2(G') = 768pq - 248q - 140p + 28, \quad (2)$$
$$\delta B_1(G') = 288pq - 68q - 32p - 4, \quad (3)$$
$$\delta B_2(G') = 432pq - 138q - 84p + 21. \quad (4)$$

Proof: According to the definition ۲،۱ and using the relation in Table 1, it is proved similarly.

3.4 THEOREM

Let G'' be the subvision graph of $HAC_5C_6C_7[p,q]$ nanotube. Then,

$$B_1(G'') = 528pq - 36q - 14p, \quad (1)$$
$$B_2(G'') = 720pq - 84q - 52p, \quad (2)$$
$$\delta B_1(G'') = 240pq - 12q - 8p, \quad (3)$$
$$\delta B_2(G'') = 288pq - 24q - 16p. \quad (4)$$

Proof: According to the definition 2.1 and using the relation in Table 1, it is proved similarly.

4 CONCLUSION

In this article, Banhatti indices were calculated using M-polynomials for $HAC_5C_6C_7[p,q]$ nanotubes and their line graph and subdivision graph. Knowing these indices can be effectively used to develop predictive models of chemical compound behavior, which gives insights to scientists or chemists to predict physicochemical properties, enabling them to explore Nanotube further. The method used in this article can be checked on other molecular graphs.

Use of AI tools declaration: The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] Deutsch, E. and Klavzar, S., "M-Polynomial and Degree-Based Topological Indices", Iranian Journal of Mathematical Chemistry, Vol. 6 (2015) 93−102.

[2] Ghods, M.; Ramezani Tousi, J. Computing Revan Polynomials and Revan Indices of Copper (I) Oxide and Copper (II) Oxide. Communications in Combinatorics, Cryptography and Computer Science. (2021), 1, 50–58.

[3] Kulli, V. R.; Pal, M.; Samanta, S.; Pal, A. Handbook of Research of Advanced Applications of Graph Theory in Modern Society. IGI Global: Pennsylvania, PA, USA, 2020.

[4] Ramezani Tousi, J.; Ghods, M. Calculation of Gourava topological indices in HAC5C6C7[p, q] nanotubes. Journal of Information and Optimization Sciences. 2023, 44.

[5] Ramezani Tousi, J.; Ghods, M. Calculation of Revan topological indices in TiO2[m, n] nanotubes. Journal of Information and Optimization Sciences. (2023), 44. 845–854.

[6] Ramezani Tousi, J.; Ghods, M. Computational Analysis of the Molecular Graph and the Line Graph of Glass by Studying Their M-Polynomial and Topological Indices. Discontinuity, Nonlinearity, and Complexity, (2024), 13(02), 361-371.

[7] Ramezani Tousi, J.; Ghods, M. Computing K Banhatti and K Hyper Banhatti indices of Titania nanotubes TiO2[m, n], Journal of Information and Optimization Sciences, (2023), 44:2, 207-216.

[8] Ramezani Tousi, J.; Ghods, M. Investigating Banhatti indices on the molecular graph and the line graph of Glass with M-polynomial approach. Proyecciones Journal of Mathematics, (2024), 43(1), 225-245.

[9] Ramezani Tousi, J.; Ghods, M. Some polynomials and degree-based topological indices of molecular graph and line graph of Titanium dioxide nanotubes. Journal of Information and Optimization Sciences. (2024), 45. 0252-2667.

[10] Rashmanlou, H., Samanta, S., Pal, M., Borzooei, R. A. A study on vague graphs. *SpringerPlus*, (**2016**) 5(1), 1234.

[11] Talebi, A.A., Rashmanlou, H. and Sadati, S.H., Certain properties of interval-valued intuitionistic fuzzy graph. *International Journal of Advanced Intelligence Paradigms*, (**2024**) 27(3-4), 376-394.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A GENERALIZATION OF HIRANO INVERSES IN BANACH ALGEBRA

Tahereh Haddadi*, Ali Ghaffari
Department of Mathematics, Semnan Branch, Islamic Azad University, Semnan, Iran
Department of Mathematics, Semnan University, p.o.box 35195-363, Semnan, Iran
thaddadi@semnan.ac.ir; aghaffari@semnan.ac.ir

ABSTRACT

Cryptography is one of the key branches of computer science and mathematics. In this field, matrices and their inverse are known as one of the powerful tools for encryption and decryption of information. In this article, we investigate the existence of the π-Hirano inverse for the anti-triangular operator matrices.

We introduce a new class of generalized inverse which is called π-Hirano inverse. In this paper some elementary properties of the π-Hirano inverse are obtained. We investigate the existence of the π-Hirano inverse for the anti-triangular operator matrix $N = \begin{bmatrix} 0 & B \\ C & D \end{bmatrix}$ with DCB=0 and et al. Certain multiplicative and additive results for the π-Hirano inverse in a Banach algebra are presented. We then apply some conditions under which a 2×2 block operator matrix has π-Hirano inverse over Banach spaces.

KEYWORDS: Drazin inverse, π-Hirano inverse, additive property, Block matrix, Schur complement, Banach algebra.

1 INTRODUCTION

It Let $\mathcal{A}$ be a Banach algebra with an identity. We first recall the definitions of some generalized inverses. As is well known, in 1958, Drazin [3] defined, an element $a \in \mathcal{A}$ has Drazin inverse if there is the element $x \in \mathcal{A}$ which satisfies

$$ax = xa,\ xax = x \text{ and } a - a^2x \in \mathcal{N}(\mathcal{A}) \tag{1}$$

or

$$ax = xa,\ xax = x \text{ and } a^k = a^{k+1}x. \tag{2}$$

Here $\mathcal{N}(\mathcal{A})$ is the set of all nilpotent elements in $\mathcal{A}$. The element x above is uniqe if it exists and is denoted by a^d and called the Drazin inverse of a. Recently, several subclasses of the Drazin inverse have been studied.

In 2017, Chen and Sheibani [1] definded, the Hirano inverse of $a \in \mathcal{A}$ is the uniqe element $x \in \mathcal{A}$ satisfying

$$ax = xa,\ xax = x \text{ and } a^2 - ax \in \mathcal{N}(\mathcal{A}) \tag{3}$$

and we denoted by a^h. They characterized the Hirano inverse by tripotents. In addition, they obtained $\mathcal{A}^H \subseteq \mathcal{A}^D$.

In 2019 [7], Zou and Mosic et al. investigate the structure of a ring in which every element satisfies the condition $a - a^{n+1} \in \mathcal{A}$ is nilpotent for a fixed n. This inspires us to introduce and study a new class of generalized inverse. In fact, it forms a subclass of Drazin inverses in a Banach algebra. We say that an element $a \in \mathcal{A}$ has π-Hirano inverse if there exists $x \in \mathcal{A}$ such that

$$ax = xa,\ xax = x \text{ and } a - a^{n+2}x \in \mathcal{N}(\mathcal{A}) \tag{4}$$

for some $n \in \mathbb{N}$ and we denoted by $a^{\pi h}$. The preceding x shall be unique, if such element exists.

2 ADDITIVE RESULTS

In this section we are concern on additive property of the π-Hirano inverse of the sum in a Banach algebra $\mathcal{A}$. We introduce two known Lemmas which are related to the nilpotency.

2.1 THEOREM

Let $n \in \mathbb{N}$. Then $a \in \mathcal{A}^{\pi \mathrm{H}}$ if and only if $a - a^{n+1} \in \mathcal{N}(\mathcal{A})$.

2.2 COROLLARY

Every Hirano invertible element in a Banach algebra is π-Hirano invertible element and every π-Hirano invertible element in a Banach algebra is Deazin invertible element.

2.3 LEMMA

Let $a, b \in \mathcal{A}$ and $ab = 0$. Then $a, b \in \mathcal{A}^{\pi \mathrm{H}} \Leftrightarrow a + b \in \mathcal{A}^{\pi \mathrm{H}}$.

2.4 THEOREM

Let $a, b \in \mathcal{A}^{\pi \mathrm{H}}$. If $a^3 b = 0$, $ba^2 b = 0$, $abab = 0$ and $b^2 ab = 0$, then $a + b \in \mathcal{A}^{\pi \mathrm{H}}$.

PROOF: Let

$$M = \begin{bmatrix} ab^2 + a^2 b + bab + b^3 & a^2 + ab + ba + b^2 \\ ab^3 + a^2 b^2 & a^3 + ab^2 + a^2 b + aba \end{bmatrix} = F + G$$

where

$$F = \begin{bmatrix} b^3 & a^2 + ab + ba + b^2 \\ 0 & a^3 \end{bmatrix} \text{ and } G = \begin{bmatrix} ab^2 + a^2 b + bab & 0 \\ ab^3 + a^2 b^2 & ab^2 + a^2 b + aba \end{bmatrix}.$$

Obviously, we have $FG =$ and $G^2 = 0$. Further, we see that

$$F = \begin{bmatrix} 0 & a^2 + ba \\ 0 & a^3 \end{bmatrix} + \begin{bmatrix} b^3 & ab + b^2 \\ 0 & 0 \end{bmatrix} = K + L$$

It is easy to verify that

$$K = \begin{bmatrix} 0 & a^2 + ba \\ 0 & a^3 \end{bmatrix} = \begin{bmatrix} a + b \\ a^2 \end{bmatrix} [0 \quad a]$$

Since $[0 \quad a] \begin{bmatrix} a + b \\ a^2 \end{bmatrix} = a^3 \in \mathcal{A}^{\pi \mathrm{H}}$ and K has π-Hirano inverse. Similarly, L has π-Hirano inverse. Obviously, $KL = 0$, then F has π-Hirano inverse and so M is π-Hirano invertible. Also we compute that

$$M = \left(\begin{bmatrix} 1 \\ a \end{bmatrix} [b \quad 1] \right)^3$$

which implies that $[b \quad 1] \begin{bmatrix} 1 \\ a \end{bmatrix} = a + b \in \mathcal{A}^{\pi \mathrm{H}}$.■

We are now ready to prove:

2.5 THEOREM

Let $a, b \in \mathcal{A}^{\pi \mathrm{H}}$. If $ab^2 = 0$, $aba^2 = 0$ and $(ab)^2 = 0$, then $a + b \in \mathcal{A}^{\pi \mathrm{H}}$.

PROOF: Let $p = a^2 + ab$ and $q = b^2 + ba$. Clearly, $ab, ba \in \mathcal{A}^{\pi \mathrm{H}}$. Since $(ab)a^2 = 0$ and $(ba)b^2 = 0$ it follows by Lemma 2.3, that $p,\ q \in \mathcal{A}^{\pi \mathrm{H}}$. Clearly, $pq^2 = 0$ and $pqp = 0$. Then $(a + b)^2 = p + q \in \mathcal{A}^{\pi \mathrm{H}}$. Therefore $a + b \in \mathcal{A}^{\pi \mathrm{H}}$. ■

2.6 PROPOSITION

Let $a, b \in \mathcal{A}^{\pi \mathrm{H}}$. If $ab^2 = 0$, $a^2ba = 0$ and $(ab)^2 = 0$, then $a + b \in \mathcal{A}^{\pi \mathrm{H}}$.

3 OPERATOR MATRICES

To illustrate the preceding results, we are concerned with the π-Hirano inverse for an operator matrix. Throughout this section, the operator matrix $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. Using different splitting approach and Theorem 2.5, we will obtain various conditions for the π-Hirano inverse of M.

3.1 LEMMA

Let $A \in L(X)^{\pi H}$ and $D \in L(Y)^{\pi H}$. Then $I = \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}$, $J = \begin{bmatrix} 0 & 0 \\ 0 & D \end{bmatrix}$ and $L = \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix}$ have π-Hirano inverse.

3.2 THEOREM

Let $B \in L(X, Y)$, $C \in L(Y, X)$. If $D, CB \in L(Y)^{\pi H}$ and $DCB = 0$, then $K = \begin{bmatrix} 0 & B \\ C & 0 \end{bmatrix}$ and $N = \begin{bmatrix} 0 & B \\ C & D \end{bmatrix}$ have π-Hirano inverse.

3.3 THEOREM

Let $A \in L(X)^{\pi H}$ and $D, CB \in L(Y)^{\pi H}$. If $DCB = 0$, $ABC = 0$ and $ABD = 0$, then $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ has π-Hirano inverse.

It is of interest to consider the π-Hirano inverse of M under generalized Schur condition $D = CA^{\pi h}B$ [5, Theorem 2.1]. Let $W = AA^{\pi h} + A^{\pi h}BCA^{\pi h}$. We now derive

3.4 THEOREM

Let $A \in L(X)^{\pi H}$, $D \in L(Y)^{\pi H}$ and $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. If $BCAA^{\pi} = 0$, $BCA^{\pi}BC = 0$, $A^{\pi}BCA = 0$, $D = CA^{\pi h}B$ and AW has π-Hirano inverse, then $M \in L(X, Y)^{\pi H}$.

PROOF: Clearly, we have $M = \begin{bmatrix} A & B \\ C & CA^{\pi h}B \end{bmatrix} = P + Q$ where

$$P = \begin{bmatrix} A & B \\ CA^{\pi h}A & CA^{\pi h}B \end{bmatrix} \text{ and } Q = \begin{bmatrix} 0 & 0 \\ CA^{\pi} & 0 \end{bmatrix}$$

By assumption, we verify that $PQ^2 = 0$, $PQP^2 = 0$ and $(PQ)^2 = 0$. In view of Theorem 2.5, Q is nilpotent, and then it has π-Hirano inverse. We see that

$$P = P_1 + P_2 = \begin{bmatrix} AA^{\pi} & A^{\pi}B \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} A^2A^{\pi h} & AA^{\pi h}B \\ CAA^{\pi h} & CA^{\pi h}B \end{bmatrix}$$

That $P_1P_2 = 0$ and P_1 is nilpotent. Moreover, we have $P_2 = \begin{bmatrix} AA^{\pi h} \\ CA^{\pi h} \end{bmatrix}[A \quad AA^{\pi h}B]$. By hypothesis, we see that $[A \quad AA^{\pi h}B]\begin{bmatrix} AA^{\pi h} \\ CA^{\pi h} \end{bmatrix} = A^2A^{\pi h} + AA^{\pi h}BCA^{\pi h} = AW$ has π-Hirano inverse. Therefore P_2 has π-Hirano inverse. ■

3.5 COROLLARY

Let $A \in L(X)^{\pi H}$, $D \in L(X)^{\pi H}$ and $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$. If $BCA^{\pi} = 0$, $D = CA^{\pi h}B$ and AW has π-Hirano inverse, then $M \in L(X,Y)^{\pi H}$.

Regarding a complex matrix as the operator matrix on $\mathbb{C} \times \cdots \times \mathbb{C}$, we now present a numerical example to demonstrate Theorem 3.4.

3.6 EXAMPLE

Let $A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 1 & 1 & 0 \\ -1 & 1 & 1 & 0 \end{bmatrix}$ and $D = \begin{bmatrix} -1 & 0 \\ -1 & 0 \end{bmatrix}$ be complex matrices and set $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ then

$$A^{\pi h} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } A^{\pi} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

We easily check that $BCAA^{\pi} = 0$, $BCA^{\pi}BC = 0$, $A^{\pi}BCA = 0$ and $D = CA^{\pi h}B$. In this case, A and D have π-Hirano inverses.

4 ACKNOWLEDGEMENTS

The authors wish to thank an anonymous referee for his/her remarks and corrections.

REFERENCES

[1] H. Chen and M. Sheibani, "On Hirano inverse in rings", *Turkish Journal of Mathematics*, vol. 43, 2049–2057, 2019.

[2] C. Deng and Y. Wei, "A note on the Derazin inverse of an anti- tringular matrix", *Linear Algebra and its Applications*, vol. 431, pp. 1910–1922, 2009.

[3] M. P. Drazin, “Pseudo-Inverses in Associative Rings and Semigroups”, *The American Mathematical Monthly*, vol. 41, pp. 520–531, 2013.

[4] A. Gaffari, T. Haddadi and M. Sheibani, “Extension of Hirano inverse in Banach algebra”, *The American Mathematical Monthly*, vol. 41, pp. 520–531, 2021.

[5] D. Mosic and D. S. Djordjevic, “Several expressions for the generalized Drazin inverse of a block matrix in a Banach algebra”, *Applied Mathematics and Computation*, vol. 220, pp. 374–381, 2013.

[6] Z. L. Ying, T. Kosan and Y. Q. Zhou, “Rings in which every element is a sum of two tripotents”, *Canadian Mathematical Bulletin*, Vol. 59, pp. 661–672, 2016.

[7] H. Zou, D. Mosic, K. Zuo and Y. Chen, “On the n-strong Drazin invertibility in rings”, *Turkish Journal of Mathematics*, vol. 43, pp. 2659–2679, 2019.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

On singleton coalition graphs

Javad B. Ebrahimi[1,2], Hasti Karimi[3]
[1]Department of Mathematical Sciences, Sharif University of Technology
[2]IPM, Institute for Research in Fundamental Sciences
[3]Department of Computer Engineering, University of Tehran
javad.ebrahimi@sharif.ir, hasti.karimi1893@gmail.com

ABSTRACT

For any graph with no vertex connected to all other vertices, the singleton coalition graph, also known as SC-graph, is another graph with the same vertex set such that two vertices are connected in the coalition graph when they form a dominating set in the original graph. Haynes and her collaborators posed the problem of characterizing all the SC-graphs. In this paper, we present a classification of these graphs and their connection to common neighborhood graphs. From this result, we show that all graphs are induced subgraphs of some SC-graphs. We also give an easy-to-check characterization of SC-graphs with independence number 2.

Keywords: Coalition, SC-graphs, singelton coalition graph, domination, common neighborhood graph

1 Introduction

Let $G(V, E)$ be a graph with the vertex set V, and the edge set E. If $e = uv \in E$, then we say u and v are adjacent, and each of them is incident with the edge e. If u and v are adjacent, we say u *dominates* v, and we write $u \sim v$.

A *path* is a sequence of non-repeated vertices, ordered in a way so that two consecutive vertices are adjacent. A *cycle* consists of a sequence of distinct vertices in a graph in which the first and last vertices, and also every pair of consecutive vertices in that sequence are adjacent. A graph G is *connected* if each pair of vertices in G belongs to a path, otherwise, G is *disconnected*. The *complement* of a graph G is a graph $\overline{G}$ on the same set of vertices as of G such that there will be an edge between two vertices u, v in $\overline{G}$, if and only if there is no edge in between u, v in G.

For any vertex $v \in V$, we denote by $N(v)$ the set of all the vertices that are dominated by v. Equivalently, $N(v)$ is the set of all the vertices adjacent to v. We call the set $N(v)$ the *neighborhood* of v. Each element of $N(v)$ is called a *neighbor* of v. We also denote by $N[v]$ the set $N(v) \cup \{v\}$. For any subset W of the vertices, we denote the union of the sets $N[w]$'s where $w \in W$, by $N[W]$.

A subset of the vertices of G is called an independent subset when no two elements of the subset are adjacent. The maximum size of an independent subset of G is called the independence number of G and is denoted by $\alpha(G)$.

A subset $W \subseteq V$ is called a *dominating set* of G if $N[W] = V$. Equivalently, W is a dominating set when each vertex outside W is a neighbor of at least one vertex in W. For more details about the topic of domination in graphs and its variants, we refer the interested reader to [2].

In [1], the notion of *domination coalition* in graphs is introduced. A partition $V_1, V_2, \ldots, V_m$ of V is called a domination coalition (or coalition, for short) for G if the sets V_i are pairwise disjoint, and no individual



Figure 1: The union of the neighbors of vertices 2 and 3 covers all the vertices, indicating that they form a dominating set. This results in their connection in $SC(G)$. On the other hand, vertices 2 and 4 do not form a dominating set, as their neighbors do not include vertex 5. Consequently, they are not adjacent in $SC(G)$, as can be observed.

set V_i is a dominating set of G. However, for any V_i, there exists at least one other set V_j such that the union $V_i \cup V_j$ forms a dominating set of G.

For any graph $G(V, E)$, the *singleton coalition graph* of G, denoted by $SC(G)$, is defined as follows: The vertex set of $SC(G)$ is the same as the vertex set of G. Two vertices u and v are adjacent in $SC(G)$ if and only if $\{u, v\}$ is a dominating set in G.

Example: In Figure 1, a graph G and its singleton coalition graph $SC(G)$ are depicted.

A graph H is called a *singleton coalition graph* when there exists a graph G such that H is isomorphic to $SC(G)$. In [1], the authors posed the problem of characterizing all coalition graphs. In this paper, we present a characterization of these graphs. Furthermore, we give a simple classification of singleton coalition graphs with independence number 2.

2 Main results

This section is devoted to stating and proving the main results of this work. We start with the main theorem. Then, we present some implications of it.

Theorem 2.1. *A graph G is an SC-graph if and only if $\overline{G}$ is a common neighborhood graph.*

Notice that the previous theorem follows directly from the following lemma.

Lemma 2.2. *A graph G is the SC-graph of a graph H if and only if $\overline{G}$ is the common neighborhood graph of $\overline{H}$.*

Proof. Assume G is the SC-graph of a graph H. We aim to prove that $\overline{G}$ is the common neighborhood graph of $\overline{H}$. Suppose u and v are adjacent in $\overline{G}$. We must show that in the graph $\overline{H}$, these vertices have a common neighbor.

Since $uv \in E(\overline{G})$ and $\overline{G}$ is the complement of G, it follows that u and v are not connected in G. This implies that the corresponding vertices u and v in H do not form a dominating set by their union. Consequently, there exists a vertex k in H that is not adjacent to either u or v.

Thus, in $\overline{H}$, the vertex k is adjacent to both u and v, meaning u and v have a common neighbor in $\overline{H}$, as required.

On the other hand, if u and v are not adjacent in $\overline{G}$, they are adjacent in G. Thus, they form a domination set in H. Hence, every vertex w in the graph H is dominated by at least one of the vertices u or v. Alternatively, there is no vertex of $\bar{H}$ that is a common neighbor of u and v. Thus, in the graph $\bar{H}$, the vertices u and v have no common neighbor. This completes the proof. □

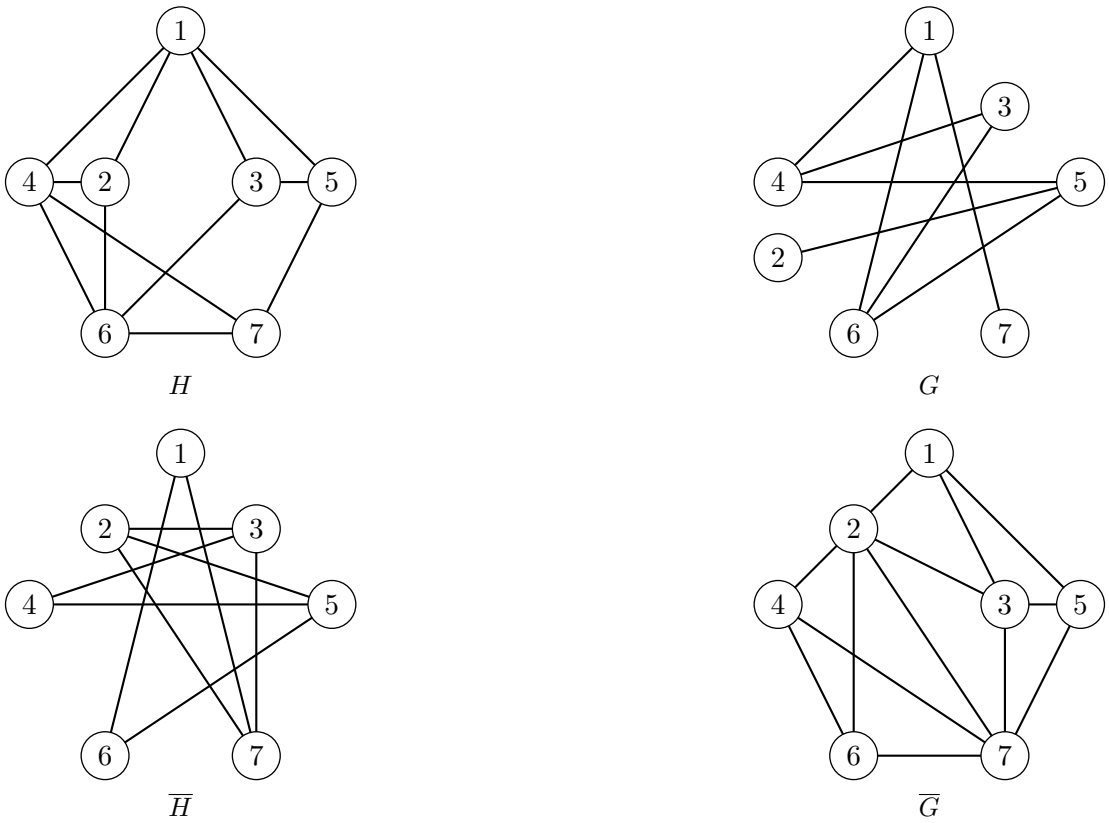


Figure 2: A graph H, its complement, $\bar{H}$, the singleton coalition graph of H, and the common neighborhood graph of $\bar{H}$ are presented.

Example:

In graph H of Figure 2, it is evident that vertices 2 and 3 do not form a dominating set in H because the union of their neighbors does not include vertex 7, which violates the condition of covering all the vertices. This implies that they are not connected in G, as can be observed. Additionally, they have a common neighbor (vertex 7) in $\bar{H}$, so they are connected in the corresponding common neighborhood graph $\bar{G}$.

On the other hand, consider vertices 4 and 5, which do form a dominating set in H through the union of their neighbors. This results in their adjacency in G. Furthermore, they do not share a common neighbor in $\bar{H}$, so they are not connected in $\bar{G}$ either.

As a consequence of Theorem 2.1, we have the following result.

Theorem 2.3. *For every graph G with $\Delta(G) < |V(G)| - 1$, there exists a graph G' such that G' is an SC-graph, and G is an induced subgraph of G'.*

Proof. We first show that for every graph G_0 with $\delta(G_0) > 0$, there exists a graph G_1 such that G_0 is an induced subgraph of G_1, and G_1 is a common neighborhood graph.

In order to show the existence of such G_1, we initially define a graph H, then we define G_1 as the common neighborhood graph of H. Finally, we show that G_1 has all the requirements of the claim.

Let U, W be two disjoint sets of the cardinality $V(G_0)$ and $E(G_0)$, respectively. Also, label the vertices in U and W with the vertices and the edges of G_0, respectively. Construct the bipartite graph H with the vertex set $U \cup W$ as follows. The vertex with the label v in U is connected to the vertex with label e in W, if and only if v is incident with e in G_0.

Let G_1 be the common neighborhood graph of H. Clearly, G_1 is a common neighborhood graph. It remains to show that G_0 is an induced subgraph of G_1. Consider the induced subgraph of G_1 on the set U. Recall that the vertex set of a graph is the same as the vertex set of its common neighborhood graph. Therefore, even though U is a subset of the vertices of H, we can regard it as a subset of the vertices of G_1, as well.

Consider two vertices of U with labels v_1 and v_2. These vertices are connected in G_1 if and only if they share a common neighbor e in H. By the definition of H, a vertex with label e is connected to v_1, v_2 if and only if in the graph G_0, the edge e is incident with both v_1, v_2. In other words, v_1 and v_2, as the vertices of G_1, are connected if and only if they are adjacent in G_0. This is an alternative way of saying that G_0 is an induced subgraph of G_1.

We now prove the statement of the theorem. Let G be a graph with $\Delta(G) < |V(G)| - 1$. Let G_0 be the complement of G. Thus, for the graph G_0 we have $\delta(G_0) > 0$. According to the earlier claim, there exists a graph G_1 such that G_1 is a common neighborhood graph and G_1 has G_0 as its induced subgraph.

Let G' be the complement of G_1 graph. Since G_1 is a common neighborhood graph, by Theorem 2.1, we know that G' is an SC-graph. It remains to show that G is an induced subgraph of G'. This is also true since $G = \bar{G}_0$, $G' = \bar{G}_1$, and G_0 is an induced subgraph of G_1. This completes the proof of the theorem. □

An important consequence of this theorem is that there is no classification of SC-graphs in terms of forbidden subgraphs or minors. That is, there is no way to find a set $\mathcal{F}$ of graphs with the property such that G is an SC-graph if and only if G has no induced subgraph (or minor) in $\mathcal{F}$.

In other words, if G_1 is not an SC-graph and G_2 has G_1 as an induced subgraph, then G_2 may or may not be an SC-graph.

By Theorem 2.1, we can also conclude that there is no classification for common neighborhood graphs in terms of forbidden induced subgraphs or forbidden minors.

The next result is a classification of triangle-free common neighborhood graphs. Note that a graph is called triangle-free when it has no C_3 cycle subgraph.

Theorem 2.4. *A triangle-free graph G is a common neighborhood graph if, and only if, G satisfies the following constraints.*

i) Every connected component of G is either a path or a cycle.

ii) The set of all even cycle components of G are in pairs. That is, for every even number m, the number of connected components of G that are isomorphic to the cycle C_m is an even number.

iii) The set of connected components of G that are paths can be partitioned into pairs such that each pair consists of two paths whose lengths differ by at most 1.

Proof. We first prove the "if" direction. Let G be a triangle-free common neighborhood graph of H. Since G is triangle-free, the maximum degree of H is at most 2. This is because if a vertex $v \in V(H)$ has three neighbors u_1, u_2, u_3, they form a triangle in G since they all have the common neighbor v.

Since the maximum degree of H is at most 2, the graph H is a disjoint union of cycles and paths. Thus, the common neighborhood graph of H is the disjoint union of the common neighborhood graphs of some paths and cycles. Observe that the common neighborhood graph of an odd cycle is isomorphic to itself. The common neighborhood of an even cycle C_{2m} is a disjoint union of two cycles each of which isomorphic to C_m. The common neighborhood graph of the path P_{2k+1} is a disjoint union of two paths isomorphic to P_k and P_{k+1}. Finally, the common neighborhood graph of P_{2k} is a disjoint union of two copies of P_k. This shows that the common neighborhood of the graph H, i.e. the graph G, satisfies the constraints of the theorem.

For the reverse direction, suppose that G satisfies all three constraints. We construct the following graph H.

1) If $C_{2k+1} = v_1, v_2, \ldots, v_{2k+1}$ is a connected component of H which is an odd cycle, then G has the following odd cycle connected component:

$$v_1, v_{k+1}, v_2, v_{k+2}, \ldots, v_{2k+1}, v_k.$$

2) If $C_{2k} = v_1, v_2, \ldots, v_{2k}$ and $C'_{2k} = u_1, u_2, \ldots, u_{2k}$ are two connected components of H which are even cycles of the same length, then G has the following cycle connected component:

$$v_1, u_1, v_2, u_2, \ldots, v_{2k}, u_{2k}.$$

3) If $P = v_1, v_2, \ldots, v_m$ and $P' = v_1, v_2, \ldots, v_n$ where $n < m \leq n+1$ are two path connected components of H, then G has the following connected component:

$$v_1, u_1, v_2, u_2, \ldots.$$

The last vertex in this path is either u_n or v_m depending on whether $m = n$ or $m = n+1$, respectively.

It is straightforward to observe that the defined graph G is the common neighborhood graph of H. Hence, G is a common neighborhood graph. This completes the proof. □

A direct corollary of the above theorem is a classification of the SC-graphs with $\alpha(G) = 2$. Notice that a graph has an independence number of 2 if and only if its complement is triangle-free. Therefore, the following corollary is immediately concluded.

Corollary 2.5. *Let G be a graph with the independence number at most 2. Then, G is an SC-graph if, and only if the complement of G has the following structure.*

i) Every connected component of $\bar{G}$ is either a path or a cycle.

ii) The set of all even cycle components of $\bar{G}$ are in pairs. That is, for every even number m, the number of connected components of $\bar{G}$ that are isomorphic to the cycle C_m is an even number.

iii) The set of connected components of $\bar{G}$ that are paths can be partitioned into pairs such that each pair consists of two paths whose lengths differ by at most 1.

References

[1] T. W. Haynes, J. T. Hedetniemi, S. T. Hedetniemi, A. McRae, and R. Mohan *Coalition Graphs*, Communications in combinatorics and optimization, 8 (2023), pp. 423–430.

[2] T. W. Haynes, J. T. Hedetniemi, and S. T. Hedetniemi, *Domination in Graphs: Core Concepts*, Springer Monographs in Mathematics, 2023.

[3] D. B. West, *Introduction to Graph Theory* , 2nd ed., Prentice Hall, 2010.

Email: javad.ebrahimi@sharif.ir
Email: hasti.karimi1893@gmail.com

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Some applications of Padovan sequences and its generalizations

Azade Rajabinezhad, Mansour Hashemi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran.
a.rajabinejad1373@gmail.com; m_hashemi@guilan.ac.ir

ABSTRACT

In this paper, we consider the Padovan sequence and define the generalized order *k*-Padovan numbers for every $k \geq 1$. Then we obtain their miscellaneous properties such as the Binet formula, the generating function, the generating matrix and some of their properties.

KEYWORDS: The generalized order *k*-Padovan number sequence, The Padovan *k*-matrix, characteristic equation, Length.

1 INTRODUCTION

It is well-known that the Padovan (Cordonnier) sequence {P(n)} is the sequence of integers defined by the following recurrence relation

$$P(n)=P(n-2)+P(n-3), \quad n\geq 3, \tag{1}$$

with initial conditions P(0)=P(1)=P(2)=1. The first few values of Padovan number sequence are 1,1,1,2,2,3,4,5,7,9,12,… . The sequence {P(n)}can be extended to negative subscripts by defining

$$P(-n)=P(-(n-3))-P(-(n-1)), \tag{2}$$

for n=1,2,3,… . Therefore (1) holds for all integers n.

The Padovan sequence was first discovered by a French engineer, Cordonnier in 1924. The name “Padovan numbers” is designated by Stewart [1]. The master study was published in 2006 by Shannon in [2].

In [3], Deveci and Karaduman defined the sequence of the Padovan p-numbers. The relationship between Padovan numbers and other sequences was established in [4,5,6] . The Padovan sequence and its properties have been studied by several authors, see for example [4,7,8,9] .

Definition 1.1. For $k\geq 1$, the generalized order *k*-Padovan number sequence { $P^k(n)$} is defind by the following homogeneous linear recurrence relation

$$P^k(n)= P^k(n-k-2)+ P^k(n-2), \quad n\geq 1, \tag{3}$$

with initial conditions $P^k(0)= P^k(1)= P^k(2)=...= P^k(k+1)=1$. We consider the generalized order *k*-Padovan number sequence modulo *m*. Reducing *k*-Padovan number sequence $P^k(n)$ by a modulus *m*, we can get the repeating sequence. A sequence is *periodic* if, after a certain point, it consists only of repetitions of a fixed subsequence. The number of elements in the shortest repeating subsequence is called the period

of the sequence. Also, a sequence is called *simply periodic* with period k if the first k elements in the sequence form a repeating subsequence.

Theorem 1.2. The sequence $\{ P^k(n) \pmod m\}$ is *simply periodic*.

Proof. Let $X_k = \{(x_1, x_2, \dots, x_{k+2}) | \ x_i$s are integers such that $0 \le x_i \le m\text{-}1\}$, then $|X_k| = m^{k+2}$. Since there are m^{k+2} distinct $(k+2)$- tuples of elements of $\mathbb{Z}_m$ at least one of the $(k+2)$- tuples appears twice in the sequence $\{ P^k(n) \pmod m\}$. Therefore, the subsequence following this $(k+2)$- tuples repeats; Hence, the sequence $\{ P^k(n) \pmod m = P_m^k(n) \}$ is *periodic*. So if

$$P_m^k(a) = P_m^k(b),\ P_m^k(a+1) = P_m^k(b+1),\ P_m^k(a+2) = P_m^k(b+2),\ \dots,\ P_m^k(a+k+2) = P_m^k(b+k+2).$$

and $b > a$, then $b \equiv a \pmod{k+2}$.

From the definition, we have $P^k(n) = P^k(n+k+2) - P^k(n+k)$ .Thus, we obtain

$$P_m^k(a) = P_m^k(b),\ P_m^k(a-1) = P_m^k(b-1),\dots,\ P_m^k(2) = P_m^k(b-a+2),\ P_m^k(1) = P_m^k(b-a+1).$$

which implies that sequence is *simply periodic*.■

Let LP_m^k denote the minimal length of the period of the series $\{ P^k(n) \pmod m\}$.

Lemma 1.3. For integers $m \ge 2$, $k \ge 1$, a and i, we have

(i) $P^k_{LP_m^k + i} \equiv P_i^k \pmod m$.

(ii) $P^k_{a.LP_m^k + i} \equiv P_i^k \pmod m$.

Proof. According to the definition of LP_m^k , the proof of Lemma is trivial. So, we omit it.■

Corollary 1.4. For integers s , $k \ge 1$ and $m \ge 2$, if

$$\begin{cases} P^k(s-2) \equiv 1 \pmod m, \\ P^k(s-1) \equiv 0 \pmod m, \\ P^k(s) \equiv 1 \pmod m, \\ P^k(s+1) \equiv 1 \pmod m, \\ \quad\quad . \\ \quad\quad . \\ P^k(s+k-2) \equiv 1 \pmod m, \\ P^k(s+k-1) \equiv 1 \pmod m, \end{cases}$$

Then LP_m^k |s.

Proof. Let $s = t \times LP_m^k + i$ where $0 \le i < LP_m^k$. Since LP_m^k is the minimal integer such that the assumption holds, the result following Lemma 1.3.■

2. SOME RESULTS OF K- PADOVAN NUMBER SEQUENCES

In this section, we discuss some properties of the generalized order *k*-Padovan number sequences. Consider $k \geq 1$. The generalized order *k*-Padovan number sequence P_n^k is defind by the following homogeneous linear recurrence relation

$P^k(n) = P^k(n\text{-}k\text{-}2) + P^k(n\text{-}2), \quad n \geq 1,$

with initial conditions $P^k(0) = P^k(1) = P^k(2) = \ldots = P^k(k+1) = 1$. If $k=1$ in (3), the generalized order *k*-Padovan number sequence P_n^k, is reduced to the usual Padovan sequence *P(n).*

Remark 2.1. The generalized order *k*-Padovan number sequence has characteristic equation

$$x^{k+2} - x^k - 1 = 0, k \geq 1. \tag{4}$$

By considering the equation (4). For $k=1$, we can see in [10] that the charactristic equation $x^3 - x - 1 = 0$has three roots

$$\alpha = \sqrt[3]{\frac{9+\sqrt{69}}{18}} + \sqrt[3]{\frac{9-\sqrt{69}}{18}},$$

$$\beta = -\sqrt[3]{\frac{9+\sqrt{69}}{144}} - \sqrt[3]{\frac{9-\sqrt{69}}{144}} + i\,\frac{\sqrt{3}}{2}\left(\sqrt[3]{\frac{9+\sqrt{69}}{18}} + \sqrt[3]{\frac{9-\sqrt{69}}{18}}\right),$$

$$\gamma = -\sqrt[3]{\frac{9+\sqrt{69}}{144}} - \sqrt[3]{\frac{9-\sqrt{69}}{144}} - i\,\frac{\sqrt{3}}{2}\left(\sqrt[3]{\frac{9+\sqrt{69}}{18}} + \sqrt[3]{\frac{9-\sqrt{69}}{18}}\right).$$

Lemma 2.2. The characteristic equation of the generalized order *k*-Padovan number sequence $x^{k+2} - x^k - 1 = 0$ for $k \geq 1$ does not have multiple roots.

Proof. Let α be a root of $f(x) = 0$ where $f(x) = x^{k+2} - x^k - 1$ so that $\alpha \notin \{0,1\}$. If possible, α is a multiple root in which case $f(\alpha) = f'(\alpha) = 0$. Now $f'(\alpha) = 0$ and $\alpha \neq 0$ give $\alpha^2 = \frac{k}{k+2}$ while $f(\alpha) = 0$ shows $\alpha^k(\alpha^2 - 1) - 1 = 0$ so that $\left(\frac{k}{k+2}\right)^{\frac{k}{2}} \cdot \left(\frac{-2}{k+2}\right) = 1$, an impossibility since the left hand side is less than 1 for $k \geq 1$. This contradiction proves the Lemma. .■

Let $\alpha_1, \alpha_2, \ldots\ldots, \alpha_{k+2}$ are distinct roots of the equation $x^{k+2} - x^k - 1 = 0$. The generating function and the Binet-like formula for the generalized order k- Padovan number sequence as follow:

Theorem 2.3. The generating function for the generalized order *k*-Padovan number sequence P_n^k is

$$\sum_{r=0}^{\infty} P^k(r) x^r = \frac{1+x}{1-x^2-x^{k+2}}.$$

Proof. Suppose that the generating function for the *k*-Padovan number sequence P_n^k has the form

$$g(x)=\sum_{r=0}^{\infty}P^{k}(r)x^{r}=P^{k}(0)+P^{k}(1)x+P^{k}(2)x^{2}+P^{k}(3)x^{3}+...+P^{k}(r)x^{r}+...$$

Then we have

$$x^{k+2}g(x)=P^{k}(0)x^{k+2}+P^{k}(1)x^{k+3}+P^{k}(2)x^{k+4}+P^{k}(3)x^{k+5}+...+P^{k}(r)x^{k+r+2}+...$$

and

$$x^{2}g(x)=P^{k}(0)x^{2}+P^{k}(1)x^{3}+P^{k}(2)x^{4}+P^{k}(3)x^{5}+...+P^{k}(r)x^{r+2}+... .$$

Then we obtain

$$g(x)-x^{k+2}g(x)-x^{2}g(x)=P^{k}(0)+P^{k}(1)x+(P^{k}(2)-P^{k}(0))x^{2}$$
$$+(P^{k}(3)-P^{k}(1))x^{3}+(P^{k}(4)-P^{k}(2))x^{4}+..+(P^{k}(k+1)-P^{k}(k-1))x^{k+1}$$
$$+(P^{k}(k+2)-P^{k}(k)-P^{k}(0))x^{k+2}+(P^{k}(k+3)-P^{k}(k+1)-P^{k}(1))x^{k+3}+... .$$

Therefore we get

$$g(x)(1-x^{k+2}-x^{2})=1+x+0x^{2}+0x^{3}+...=1+x .$$

Consequently,

$$\sum_{r=0}^{\infty}P^{k}(r)x^{r}=\frac{1+x}{1-x^{2}-x^{k+2}}.\blacksquare$$

Theorem 2.4. Let r≥0 be an integer. Then the Binet-like formula for the generalized order *k*-Padovan number sequence P_n^k is

$$P^{k}(r)=\frac{\alpha_1^{k+r}(\alpha_1+1)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)...(\alpha_1-\alpha_{k+2})}+\frac{\alpha_2^{k+r}(\alpha_2+1)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)...(\alpha_2-\alpha_{k+2})}+...+\frac{\alpha_{k+2}^{k+r}(\alpha_{k+2}+1)}{(\alpha_{k+2}-\alpha_1)(\alpha_{k+2}-\alpha_2)...(\alpha_{k+2}-\alpha_{k+1})}$$

where $\alpha_1,\alpha_2,.....,\alpha_{k+2}$ are the roots of the equation $x^{k+2}-x^{k}-1=0$.

Proof. From Lemma (2.2), we see that the cubic equation $f(x)=x^{k+2}-x^{k}-1=0$ has *k*+2 distinct roots $\alpha_1,\alpha_2,.....,\alpha_{k+2}$. Hence $\frac{1}{\alpha_1},\frac{1}{\alpha_2},...,\frac{1}{\alpha_{k+2}}$ are the roots of $h(x)=f(\frac{1}{x})=1-x^{2}-x^{k+2}$. In exact, we have $h(x)=1-x^{2}-x^{k+2}=(1-\alpha_1 x)(1-\alpha_2 x)...(1-\alpha_{k+2}x)$. According to the generating function of the generalized order *k*-Padovan number sequence, we have

$$g(x)=\frac{1+x}{1-x^{2}-x^{k+2}}=\frac{A_1}{1-\alpha_1 x}+\frac{A_2}{1-\alpha_2 x}+\ldots+\frac{A_{k+2}}{1-\alpha_{k+2}x}=A_1\sum_{r=0}^{\infty}(\alpha_1 x)^r+A_2\sum_{r=0}^{\infty}(\alpha_2 x)^r+\ldots+A_{k+2}\sum_{r=0}^{\infty}(\alpha_{k+2}x)^r$$

Thus

$$g(x)=\frac{1+x}{1-x^{2}-x^{k+2}}=\frac{A_1}{1-\alpha_1 x}+\frac{A_2}{1-\alpha_2 x}+\ldots+\frac{A_{k+2}}{1-\alpha_{k+2}x}=A_1\sum_{r=0}^{\infty}(\alpha_1 x)^r+A_2\sum_{r=0}^{\infty}(\alpha_2 x)^r+\ldots+A_{k+2}\sum_{r=0}^{\infty}(\alpha_{k+2}x)^r$$

Therefore by comparison of the left and right sides of this equality we get that

$$1+x=A_1(1-\alpha_2 x)(1-\alpha_3 x)\ldots(1-\alpha_{k+2}x)+A_2(1-\alpha_1 x)(1-\alpha_3 x)\ldots+(1-\alpha_{k+2}x)+\ldots+A_{k+2}(1-\alpha_1 x)(1-\alpha_2 x)\ldots(1-\alpha_{k+1}x)).$$

If we set $x=\frac{1}{\alpha_1}$ we find that $1+\frac{1}{\alpha_1}=A_1(1-\frac{\alpha_2}{\alpha_1})(1-\frac{\alpha_3}{\alpha_1})\ldots(1-\frac{\alpha_{k+2}}{\alpha_1})$.

Consequently ,we get

$$A_1=\frac{\alpha_1^k(\alpha_1+1)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_{k+2})}$$

Beside we get

$$A_2=\frac{\alpha_2^k(\alpha_2+1)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_{k+2})}\ldots A_{k+2}=\frac{\alpha_{k+2}^k(\alpha_{k+2}+1)}{(\alpha_{k+2}-\alpha_1)(\alpha_{k+2}-\alpha_2)\ldots(\alpha_{k+2}-\alpha_{k+1})}.$$

So we obtain that

$$g(x)=\sum_{r=0}^{\infty}\frac{\alpha_1^{k+r}(\alpha_1+1)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_{k+2})}x^r+\sum_{r=0}^{\infty}\frac{\alpha_2^{k+r}(\alpha_2+1)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_{k+2})}x^r+\ldots+\sum_{r=0}^{\infty}\frac{\alpha_{k+2}^{k+r}(\alpha_{k+2}+1)}{(\alpha_{k+2}-\alpha_1)(\alpha_{k+2}-\alpha_2)\ldots(\alpha_{k+2}-\alpha_{k+1})}x^r$$

$$=\sum_{r=0}^{\infty}[\frac{\alpha_1^{k+r}(\alpha_1+1)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_{k+2})}+\sum_{r=0}^{\infty}\frac{\alpha_2^{k+r}(\alpha_2+1)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_{k+2})}+\ldots+\sum_{r=0}^{\infty}\frac{\alpha_{k+2}^{k+r}(\alpha_{k+2}+1)}{(\alpha_{k+2}-\alpha_1)(\alpha_{k+2}-\alpha_2)\ldots(\alpha_{k+2}-\alpha_{k+1})}]x^r$$

Consequently, we get

$$P^k(r)=\frac{\alpha_1^{k+r}(\alpha_1+1)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_{k+2})}+\frac{\alpha_2^{k+r}(\alpha_2+1)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_{k+2})}+\ldots+\frac{\alpha_{k+2}^{k+r}(\alpha_{k+2}+1)}{(\alpha_{k+2}-\alpha_1)(\alpha_{k+2}-\alpha_2)\ldots(\alpha_{k+2}-\alpha_{k+1})}.$$

3 THE PADOVAN *K*- MATRIX AND ITS PROPERTIES

The generalized order *k*-Padovan number sequence is a special case of a sequence which is defined as a linear combination by Kalman as follows

$$a_{n+k}=c_0a_n+c_1a_{n+1}+c_2a_{n+2}+..c_{k-1}a_{n+k-1}$$

where $c_0, c_1, ..., c_{k-1}$ are real constants. In [11] , Kalman derived a number of closed form formulas for the generalized sequence by the companion matrix method as follows:

$$Q_k = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 0 & 1 & 0 \\ 0 & 0 & 0 & ... & 0 & 0 & 1 \\ c_0 & c_1 & c_2 & ... & c_{k-3} & c_{k-2} & c_{k-1} \end{bmatrix}$$

Then by an inductive argument, he obtained that

$$Q_k^n \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+k-1} \end{bmatrix}$$

Let the $(k+2)\times(k+2)-$ ordered matrix A_k be defined by

$$A_k = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 0 & 1 & 0 \\ 0 & 0 & 0 & ... & 0 & 0 & 1 \\ 1 & 0 & 0 & ... & 0 & 1 & 0 \end{bmatrix}$$

The matrix A_k is called the ***Padovan k-matrix***. So it's clear that

$$A_k^n \begin{bmatrix} P_0^k \\ P_1^k \\ \vdots \\ P_k^k \\ P_{k+1}^k \end{bmatrix} = \begin{bmatrix} P_n^k \\ P_{n+1}^k \\ \vdots \\ P_{n+k}^k \\ P_{n+k+1}^k \end{bmatrix}$$

Lemma 3.1. For every $k \geq 1$ and the Padovan *k*-matrix A_k , we have $\det(A_k)=-\det(A_{k-1})$.

Proof. For *k*=1, we have

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Thus, $\det(A_1)=1$ .Beside for *k*=2,

$$A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

It's clear that by omitting the first row and second column of A_2 , we can reach the matrix A_1 . So we use Laplace expansion to calculate determinant of A_2 .we have

$$\det(A_2)=1\times(-1)^3\times\det(A_1)=-\det(A_1).$$

Similarly, we can reach the matrix A_k by using Laplace expansion relative to second column of A_{k-1} So we have $\det(A_k)=1\times(-1)^3\times\det(A_{k-1})=-\det A_{k-1}$. ■

Corollary 3.2. For every *k≥1*. and the Padovan *k*- matrix A_k , we have $\det(A_k)=(-1)^{k-1}$.

Proof. Lemma 3.1 yields that $\det(A_k)=(-1)^{(k-1)}\det(A_1)$, so it is proved.■

4 CONCLUSION

In this paper, we introduce the generalized order *k*-Padovan number sequence for every $k \geq 1$. Also, we obtain some results on the properties such as the generating function and the Binet-like formula. In the last section, we study about the Padovan *k*-matrix A_k and we obtain its determinant $\det(A_k)=(-1)^{k-1}$.

REFERENCES

[1] I. Stewart, "Tales of a neglected number,". Scientific American., vol 274, pp 102-103, 1996.

[2] A.G. Shannon,P.G. Anderson and A.F. Horadam, "Properties of Cordonnier, Perrin and Van der Laan numbers", International Journal of Mathematical Education in Science and Technology, vol 37,pp 825-831,2006.

[3] O. Deveci and E. Karaduman,"On the padovan p-numbers", Hacettepe Journal of Mathematics and statistics., vol 46,pp. 579-592, 2017.

[4] O. Deveci,"The Jacobsthal-Padovan p-Sequences and their Applications",Proceedings of the Romanian Academy Series A-Mathematics Physics,Technical Sciences Information Science. 3rd ed,vol.20. pp 215-224. 2019.

[5] N. Gogin and A.A. Myllari, "The Fibonacci-Padovan sequence and MacWilliams transform matrices", Programing and Computer Software, published in Programmirovanie., vol 33, pp. 74-79, 2007.

[6] Y. Soykan."Generalized Richard numbers", Int. J. Adv. Appl. Math. and Mech. vol 10. Pp. 38-51.,2023.

[7] G. Cerda-Morales,"New identities for Padovan numbers", Departamento de Matem´atica, Facultad de Ciencias F´ısicas y Matem´aticas, Universidad de Concepci´on, Casilla 160-C, Concepci´on, Chile., 2019.

[8] O. Deveci, Y. Akuzum and E. Karaduman,"The Pell-Padovan p-Sequences and Its Applications", Utilitas Mathematica., vol.98, 327-347, 2015.

[9] S. Ramaswamy,"Properties of Padovan sequence", Turkish Journal of computer and Mathematics Education,2021.

[10] O. Diskay and H. Menken, "On the Quinary Fibonacci-Padovan Sequences, creat math inform, first edition., vol. 32., pp. 41-48., 2023.

[11] D. Kalman, "Generalized Fibonacci numbers by matrix methods", The Fibonacci Quarterly, first edition, vol. 20. Pp. 73-76,1982.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

An In-Depth Analysis of Quantum Key Distribution Protocols and Implementation Challenges in Quantum Communication Networks

Babak Khabiri
Department of Mathematics, Islamic Azad University, Jouybar Branch, Jouybar, Iran

Khosro Jalali
Department of Electronics, National University of Skills (NUS), Tehran, Iran

ABSTRACT

Quantum cryptography, particularly Quantum Key Distribution (QKD), has emerged as one of the most promising applications of quantum mechanics in the field of information security. This paper provides a comprehensive analysis of advanced QKD protocols, including BB84, E91, and entanglement-based protocols. Additionally, it delves into the practical challenges of implementing these protocols in quantum communication networks, such as noise, signal loss, hardware limitations, and the need for quantum repeaters. Furthermore, recent advancements in quantum cryptography and its potential applications in next-generation networks (e.g., 6G and the quantum internet) are discussed. By offering a detailed and specialized review, this paper aims to provide researchers and professionals in the field of information security and quantum computing with a deeper understanding of the challenges and opportunities presented by this emerging technology.

Keywords: Quantum Cryptography, Quantum Key Distribution (QKD), Quantum Entanglement, Quantum Communication Networks, Quantum Internet, Information Security

1 INTRODUCTION

The advent of quantum computing has posed a significant threat to classical cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC). With the development of algorithms like Shor's algorithm, quantum computers have the potential to break these systems in polynomial time [1]. Shor's algorithm, in particular, can efficiently factor large integers and solve the discrete logarithm problem, which are the foundational mathematical problems upon which RSA and ECC rely for security. This capability of quantum computers has made it clear that traditional cryptographic methods, which are secure against classical computers, will not be sufficient in a quantum world. This realization has underscored the urgent need for the development of quantum-resistant cryptographic systems that can withstand the power of quantum computing.

Quantum cryptography, particularly Quantum Key Distribution (QKD), has emerged as a promising solution to this problem. QKD leverages the principles of quantum mechanics to establish a secure communication channel between two parties. Unlike classical cryptographic methods, QKD provides security based on the laws of physics, specifically exploiting phenomena like quantum entanglement and the no-cloning theorem. This makes it resistant to quantum attacks, as any attempt to intercept or measure quantum information will disturb the system and alert the

communicating parties to the presence of an eavesdropper [2]. As quantum computers continue to advance, QKD offers a potential foundation for future-proofing information security by enabling the secure exchange of cryptographic keys that cannot be compromised, even by the most powerful quantum computers.

2. Principles of Quantum Cryptography

Quantum cryptography is grounded in the principles of quantum mechanics, including Heisenberg's uncertainty principle, quantum entanglement, and the no-cloning theorem. These principles ensure that any eavesdropping on quantum systems is detectable [3]. For instance, Heisenberg's uncertainty principle states that it is impossible to measure both the position and momentum of a particle with absolute precision simultaneously, which means that any attempt to measure quantum states inevitably disturbs them. This disturbance makes it easy to detect if someone is trying to intercept the transmission of quantum information. Additionally, quantum entanglement plays a critical role in ensuring the security of quantum communication. When two particles are entangled, their states become so deeply interconnected that a change to one particle will instantly affect the state of the other, regardless of the distance separating them. This phenomenon allows for the detection of any tampering with the system. The no-cloning theorem further reinforces the security of quantum cryptography by stating that it is impossible to create an exact copy of an unknown quantum state, making it impossible for an eavesdropper to replicate and hide their observation of quantum data.

One of the most significant protocols in quantum cryptography is Quantum Key Distribution (QKD), which enables the secure exchange of cryptographic keys between two parties [4]. QKD allows two parties to generate a shared secret key, which can then be used to encrypt and decrypt messages. What makes QKD particularly secure is that any attempt to intercept the key exchange would inevitably disturb the quantum states involved, alerting the parties involved to the presence of eavesdroppers. This feature gives QKD a significant advantage over classical key distribution methods, which can be vulnerable to interception without detection. As a result, QKD has become a cornerstone of modern secure communication systems, particularly in scenarios where privacy and data integrity are paramount. By ensuring that the process of key exchange is immune to interception, QKD makes it possible to establish a level of security that classical encryption methods cannot match, even in the face of sophisticated eavesdropping attempts.

3. Quantum Key Distribution Protocols

This section provides an in-depth analysis of prominent Quantum Key Distribution (QKD) protocols such as BB84, E91, and entanglement-based protocols. The BB84 protocol, introduced by Bennett and Brassard in 1984, is one of the earliest and most widely used QKD protocols [5]. It utilizes the polarization of photons to transmit information, where two sets of polarization states are used to encode the key. In BB84, any eavesdropping attempt is easily detectable because any interception of the photons by a third party disturbs their quantum state, causing errors that can be detected by the communicating parties. This makes the protocol highly effective in ensuring secure communication, as any attempt to measure or tamper with the quantum data will leave traces that can be identified.

The E91 protocol, proposed by Ekert in 1991, takes a different approach by employing quantum entanglement for key distribution, offering a higher level of security [6]. In this protocol, two entangled particles are shared between the sender and receiver, and the quantum states of these particles are measured. The entanglement ensures that the measurement of one particle instantaneously determines the state of the other, regardless of the distance between them. The security of the E91 protocol relies on the violation of Bell's inequalities, which guarantees that any eavesdropping on the quantum channel would disrupt the entanglement and be detectable. This feature provides a higher level of security compared to the BB84 protocol, as it does not only rely on the disturbance of individual quantum states but also on the fundamental properties of quantum mechanics.

In addition to these protocols, entanglement-based protocols, which utilize quantum entanglement in various ways for key distribution, offer significant advantages in terms of security. These protocols take full advantage of quantum mechanical phenomena such as non-locality and the violation of Bell's inequalities to detect eavesdropping and ensure secure key exchange. The combination of entanglement and the no-cloning theorem provides a solid foundation for developing more advanced QKD protocols that can withstand increasingly sophisticated attacks in quantum communication networks.

4. Practical Challenges in Implementing QKD

Despite its numerous advantages, the implementation of Quantum Key Distribution (QKD) systems faces several practical challenges. Noise, signal loss, and hardware limitations are among the primary obstacles to the widespread adoption of QKD [7]. Quantum systems are highly sensitive to external disturbances, which can introduce errors during transmission. For instance, photon detectors may experience inefficiencies, leading to the loss of quantum information, and environmental factors such as temperature fluctuations can affect the coherence of quantum states. Furthermore, the existing hardware for QKD is often expensive and requires precise calibration, which can make deployment in large-scale networks challenging.

Another significant challenge in QKD is the limited distance over which quantum information can be transmitted. As quantum information travels through optical fibers or the atmosphere, it is subject to signal degradation due to loss and scattering, which can severely limit the range of communication. To overcome this limitation, quantum repeaters are needed [8]. These devices, which use quantum entanglement, enable the transmission of quantum information over much longer distances. Quantum repeaters function by breaking down the transmission into smaller segments, entangling particles at each intermediate point, and then using these entanglements to restore the quantum state. This process allows for the extension of the communication range beyond the typical distance limitations of direct quantum communication channels.

The development and deployment of quantum repeaters represent a critical step in overcoming the distance limitations of QKD systems [9]. However, the technology is still in the experimental phase, and significant advancements are required before quantum repeaters can be used effectively in practical applications. Researchers are exploring various approaches, including entanglement swapping and quantum memory, to improve the performance and reliability of quantum repeaters. Once these challenges are addressed, QKD systems could achieve secure communication over global distances, paving the way for large-scale, quantum-secure networks.

5. Future Applications and Prospects

Quantum cryptography holds immense potential in various domains, including secure communications, banking, and national defense. As quantum technologies continue to advance, the integration of quantum cryptography into these fields is expected to become a new standard in information security [10]. In the realm of secure communications, quantum cryptography can provide unbreakable encryption methods that are resistant to attacks from both classical and quantum computers, making it invaluable for protecting sensitive data. In banking, where the security of financial transactions is paramount, quantum cryptography could ensure that money transfers, personal information, and investment strategies are protected from potential breaches. Similarly, in national defense, quantum cryptography has the potential to protect government communications, military strategies, and classified intelligence from adversaries.

With the rapid development of quantum technologies, future research in this field may focus on addressing key challenges such as developing fault-tolerant quantum algorithms. These algorithms would be resilient to errors that arise due to imperfections in quantum hardware, allowing quantum cryptographic systems to operate efficiently and reliably in real-world conditions. Improving quantum hardware will also be crucial, as current quantum devices still face issues such as limited qubit coherence times and high error rates, which hinder their scalability and practicality. Addressing these issues will be essential for realizing the full potential of quantum cryptography.

Looking ahead, next-generation networks, such as 6G and the quantum internet, are areas that could greatly benefit from the integration of quantum cryptography [11]. 6G networks, with their focus on ultra-low latency, high data rates, and massive device connectivity, will require new levels of security to safeguard the immense amount of data transmitted across them. Quantum cryptography could provide the necessary tools to ensure the privacy and integrity of communications in these high-performance networks. The quantum internet, which envisions a global network of quantum devices that can exchange quantum information, could revolutionize how data is transmitted, creating a new era of communication that is inherently secure against any form of eavesdropping. As these technologies evolve, quantum cryptography will likely play a key role in shaping the future of global information security.

6. Conclusion

Quantum cryptography, as one of the most critical future technologies in information security, presents numerous challenges and opportunities for researchers. As the world moves closer to the era of quantum computing, the potential for quantum cryptography to revolutionize how we secure data becomes increasingly evident. However, despite its promising advantages, the practical challenges associated with implementing quantum cryptographic systems remain significant. Issues such as noise, signal loss, and the limitations of current hardware pose hurdles that need to be overcome for widespread adoption. Furthermore, the limited distance over which quantum information can be transmitted and the need for quantum repeaters are technical barriers that require ongoing innovation.

Nonetheless, recent advancements in quantum technologies, including improvements in quantum key distribution protocols and the development of quantum repeaters, promise a more secure future. These innovations bring us closer to overcoming the challenges that have hindered the full realization of quantum cryptography. With the progress being made, it is anticipated that quantum cryptographic systems will become essential in ensuring the security of sensitive information, especially in the face of increasingly sophisticated threats posed by quantum computers.

This paper, through a comprehensive and specialized review, aims to enhance the understanding of quantum cryptography and its pivotal role in the future of digital security. By exploring the underlying principles, key protocols, and ongoing developments in the field, this work seeks to provide a clearer picture of how quantum cryptography can shape the future landscape of information security. As we enter a new era where quantum computing and quantum cryptography converge, understanding and preparing for the challenges and opportunities ahead will be critical to safeguarding digital communications in the years to come.

References:

[1] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2), 303-332.

[2] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7-11.

[3] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145.

[4] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3), 1301.

[5] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7-11.

[6] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6), 661.

[7] Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics*, 8(8), 595-604.

[8] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4), 1012-1236.
[9] Sangouard, N., Simon, C., de Riedmatten, H., & Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1), 33.
[10] Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2), 025002.
[11] Wang, X., Yu, Z., & Zhang, Z. (2021). Quantum internet: A vision for the road ahead. *Science*, 372(6539), eabe5253.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Post-Quantum Cryptography: A Comprehensive Review of Lattice-Based Cryptosystems and Their Resistance to Quantum Attacks

Khosro Jalali

Department of Electronics, National University of Skills (NUS), Tehran, Iran

Babak Khabiri
Department of Mathematics, Islamic Azad University, Jouybar Branch, Jouybar, Iran

Abstract:

As quantum computing advances, the threat to classical cryptographic systems grows exponentially. Post-quantum cryptography (PQC) has emerged as a critical field of study, aiming to develop cryptographic algorithms that can withstand attacks from quantum computers. This paper provides an in-depth review of lattice-based cryptosystems, one of the most promising candidates for post-quantum cryptography. We explore the mathematical foundations of lattice-based cryptography, its security assumptions, and its resistance to quantum attacks. Additionally, we discuss the practical challenges of implementing lattice-based cryptosystems, including key size, computational efficiency, and standardization efforts. Finally, we examine the potential applications of lattice-based cryptography in securing next-generation communication systems, cloud computing, and the Internet of Things (IoT). This paper aims to provide researchers and practitioners with a thorough understanding of lattice-based cryptography and its role in the post-quantum era.

Keywords:
Post-Quantum Cryptography, Lattice-Based Cryptography, Quantum Resistance, Cryptographic Algorithms, Quantum Computing, Information Security.

1. Introduction

The rise of quantum computing poses a significant threat to classical cryptographic systems, particularly those based on integer factorization and discrete logarithms, such as RSA and Elliptic Curve Cryptography (ECC). Shor's algorithm, which can efficiently solve these problems in polynomial time on a quantum computer, has made it clear that existing cryptographic schemes, once considered secure, would be rendered vulnerable to quantum attacks. This has necessitated the development of post-quantum cryptographic algorithms that can resist the power of quantum computing [1]. These new cryptographic algorithms aim to ensure data security even in a future where quantum computers are capable of breaking traditional cryptographic systems.

Among the various approaches to post-quantum cryptography, lattice-based cryptosystems have gained considerable attention due to their strong security guarantees and versatility. Lattice-based cryptography relies on the hardness of problems such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), which are believed to be resistant to attacks from both classical and quantum computers [2]. This makes lattice-based schemes promising candidates for securing data in a world dominated by quantum computing. In addition to their security, lattice-based cryptosystems are highly versatile, supporting a wide range of cryptographic primitives, such as encryption, digital signatures, and fully homomorphic encryption.

This paper focuses on lattice-based cryptography, delving into its mathematical foundations, key problems, and existing constructions. It also explores its potential to secure information in the quantum era, addressing the challenges it faces in terms of performance, efficiency, and implementation. By examining the state of the art in lattice-based cryptosystems, this paper aims to provide a comprehensive overview of how lattice-based cryptography could play a crucial role in post-quantum security and shape the future of secure communication.

2. Mathematical Foundations of Lattice-Based Cryptography

Lattice-based cryptography is built on the hardness of certain mathematical problems in lattice theory, such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem [3]. Lattices are mathematical structures that consist of a regular arrangement of points in space, typically defined by a set of basis vectors. These structures have many interesting properties that are leveraged in cryptographic constructions. The complexity of solving certain problems in lattices, such as finding the shortest vector or solving the LWE problem, forms the foundation of the security of lattice-based cryptosystems.

The Shortest Vector Problem (SVP) involves finding the shortest non-zero vector in a lattice, while the Learning With Errors (LWE) problem is based on the difficulty of distinguishing between noisy linear equations and random ones. Both of these problems are considered hard, even for quantum computers, due to their deep connection to the geometric properties of lattices and the mathematical structure of high-dimensional spaces. These problems have been extensively studied and are believed to be resistant to both classical and quantum attacks, making them a promising foundation for post-quantum cryptography.

This section provides a detailed explanation of the mathematical concepts underlying lattice-based cryptography, starting with lattices themselves. A lattice is typically represented by a set of integer linear combinations of basis vectors, and the challenge of solving certain problems, such as finding the shortest vector, becomes computationally difficult as the dimension of the lattice increases. Basis reduction is a technique used to simplify the lattice structure, making it easier to solve lattice problems. It involves transforming the lattice's basis into a set of vectors that are "shorter" and more closely related, which can help in solving the SVP and LWE problems more efficiently.

We also discuss the security assumptions that make lattice-based cryptography resistant to quantum attacks [4]. The security of lattice-based systems is based on the belief that certain problems, such as SVP and LWE, remain hard even in the presence of quantum algorithms. Unlike classical problems like integer

factorization and discrete logarithms, which are vulnerable to Shor's algorithm, lattice problems are not easily solvable by known quantum algorithms, making them suitable candidates for secure cryptographic protocols in the quantum era. This resistance to quantum attacks, combined with the flexibility of lattice-based cryptosystems to support a wide range of cryptographic applications, positions them as a robust and future-proof solution for securing digital communication in the post-quantum world.

3. Lattice-Based Cryptographic Schemes

This section explores several prominent lattice-based cryptographic schemes, including encryption, digital signatures, and key exchange protocols. These schemes utilize the hardness of lattice problems to provide secure solutions that are resistant to both classical and quantum attacks. Notable examples of lattice-based schemes include the NTRU encryption scheme, the Ring-LWE-based encryption scheme, and the Dilithium signature scheme [5]. Each of these schemes offers different strengths and trade-offs in terms of security, efficiency, and practical implementation.

The NTRU encryption scheme is a well-known lattice-based encryption algorithm that is based on the Ring-LWE problem. It offers efficient encryption and decryption operations, making it suitable for use in resource-constrained environments. One of the key advantages of NTRU is its relatively small key sizes compared to other post-quantum encryption schemes, such as those based on RSA or ECC. However, NTRU's security is dependent on the hardness of the Ring-LWE problem, and while it is resistant to quantum attacks, its security could be compromised by advances in quantum algorithms or implementation vulnerabilities.

The Ring-LWE-based encryption scheme is another widely studied approach, where encryption is based on the hardness of the Learning With Errors problem in a ring structure. This scheme is often used in the construction of fully homomorphic encryption (FHE) systems, allowing for computation on encrypted data. Ring-LWE-based schemes provide strong security guarantees and can be adapted to a variety of cryptographic applications, including encryption and key exchange protocols. However, their efficiency is a key challenge, as the computational overhead for operations on large lattices can be significant. The larger the lattice dimension, the more secure the scheme, but it also results in slower operations.

The Dilithium signature scheme, on the other hand, is a lattice-based digital signature scheme designed for post-quantum security. It is based on the hardness of the Module-LWE problem, which is an extension of the LWE problem in a ring structure. Dilithium offers both strong security guarantees and relatively fast signing and verification operations. Its security is based on the hardness of solving the Shortest Vector Problem (SVP) and the Learning With Errors problem in module lattices. The scheme is particularly well-suited for applications where digital signatures are needed, such as authentication and integrity verification. Despite its efficiency, the larger key and signature sizes compared to classical digital signature schemes could pose challenges for deployment in environments with limited bandwidth.

We also analyze the security, efficiency, and practical implementation of these schemes. While lattice-based cryptosystems offer promising resistance to quantum attacks, their efficiency in terms of

computational resources and bandwidth usage remains a key consideration for real-world applications. For instance, although lattice-based schemes generally have smaller key sizes than some other post-quantum alternatives, their public key sizes can still be larger than traditional RSA and ECC schemes, potentially leading to increased overhead in terms of storage and transmission.

In addition to individual schemes, ongoing efforts by organizations such as NIST are playing a critical role in standardizing lattice-based cryptographic algorithms for post-quantum security [6]. NIST has been conducting a public competition to evaluate and select quantum-resistant cryptographic algorithms, with lattice-based cryptography being one of the most prominent families of algorithms under consideration. The goal is to develop standards that can be adopted globally to ensure the continued security of cryptographic systems in the face of quantum computing advancements. As part of this effort, several lattice-based schemes, including Dilithium, NTRU, and others, are undergoing extensive scrutiny to assess their security, performance, and suitability for real-world deployment.

By exploring these lattice-based cryptographic schemes, we can better understand their potential to secure information in the quantum era. The continuous evolution of these schemes and the ongoing efforts by cryptographic organizations will ultimately determine how effectively lattice-based cryptography can protect against the emerging threats posed by quantum computing.

4. Practical Challenges in Implementing Lattice-Based Cryptography

Despite their strong security guarantees, lattice-based cryptosystems face several practical challenges that need to be addressed for their widespread adoption. One of the primary concerns is the large key size and ciphertext size, which can significantly impact storage and bandwidth requirements. Lattice-based schemes, particularly those based on Ring-LWE or Module-LWE, often require larger key sizes compared to classical cryptographic algorithms such as RSA and ECC. These large key sizes arise from the complexity of the lattice problems and the need to store and transmit larger ciphertexts for secure encryption. As a result, the increased storage and bandwidth requirements can be a barrier to deploying lattice-based cryptosystems in environments with constrained resources, such as embedded devices or low-bandwidth communication channels [7].

In addition to the size-related challenges, computational efficiency is another critical issue for lattice-based cryptosystems. Lattice-based algorithms often require more processing power compared to classical cryptographic algorithms. Operations such as encryption, decryption, and key generation involve complex mathematical computations on large lattices, which can be computationally expensive. For example, key generation in lattice-based schemes involves solving hard problems in high-dimensional spaces, which requires significant computational resources. This inefficiency can lead to slower execution times and higher energy consumption, making it less suitable for real-time applications or devices with limited processing power.

This section examines these challenges in detail and discusses potential solutions to overcome them. One promising approach is the use of optimization techniques that aim to reduce the computational overhead of

lattice-based algorithms. These techniques include methods to reduce the lattice dimension without sacrificing security, as well as improvements in algorithmic efficiency, such as faster key generation and encryption procedures. Researchers have also explored techniques like dimension reduction and basis pruning to make lattice problems easier to solve without compromising security. These methods can help alleviate some of the performance issues associated with lattice-based cryptosystems.

Another potential solution is the use of hardware acceleration to speed up lattice-based operations. Specialized hardware, such as Field-Programmable Gate Arrays (FPGAs) or Graphics Processing Units (GPUs), can be used to accelerate the computationally intensive operations involved in lattice-based cryptography. These hardware platforms are well-suited for parallel processing and can significantly reduce the time required to perform operations on large lattices. By offloading the heavy computational tasks to dedicated hardware, the overall performance of lattice-based cryptosystems can be improved, making them more viable for practical use in various applications.

In summary, while lattice-based cryptosystems offer robust security guarantees against quantum attacks, their practical challenges related to key size, ciphertext size, and computational efficiency must be addressed. Optimization techniques and hardware acceleration present promising solutions that can help overcome these challenges and pave the way for the widespread deployment of lattice-based cryptography in post-quantum secure systems [8].

5. Applications of Lattice-Based Cryptography

Lattice-based cryptography has a wide range of potential applications in securing next-generation communication systems, thanks to its strong security guarantees against quantum attacks and its versatility in supporting various cryptographic primitives. As the world moves toward increasingly complex and interconnected systems, lattice-based cryptography offers a promising solution for securing critical infrastructure in several emerging domains. This section explores some of these applications in detail, highlighting the unique advantages of lattice-based cryptography in each context.

One prominent application of lattice-based cryptography is in cloud computing environments, where protecting sensitive data is a top priority. Cloud computing platforms often store large volumes of user data, including personal information, financial records, and intellectual property. Lattice-based cryptosystems, particularly those that support fully homomorphic encryption (FHE), enable secure computation on encrypted data. This means that data can be processed in the cloud without ever needing to be decrypted, ensuring that sensitive information remains confidential throughout the processing cycle. This feature is particularly valuable in multi-tenant cloud environments, where data from different users may reside on the same infrastructure, and privacy must be maintained. By using lattice-based encryption, cloud providers can offer users enhanced security without compromising performance.

In the context of the Internet of Things (IoT), where billions of interconnected devices collect and share data, lattice-based cryptography can help secure communications between these devices. The IoT is particularly vulnerable to security breaches due to its wide attack surface and the large number of potentially insecure devices. Lattice-based cryptosystems can be used to provide end-to-end encryption between IoT devices, ensuring that data transmitted across potentially insecure networks is protected from eavesdropping and tampering. Additionally, lattice-based cryptography can be applied to secure key exchange protocols

for IoT devices, allowing them to establish trust and communicate securely even in resource-constrained environments. The flexibility and efficiency of lattice-based schemes make them suitable for IoT applications, where low power consumption and fast execution are critical requirements.

Another important application of lattice-based cryptography is in secure multi-party computation (SMC), a technique that allows multiple parties to jointly compute a function while keeping their individual inputs private. This is particularly useful in scenarios where organizations or individuals wish to collaboratively compute results without revealing their private data. Lattice-based cryptosystems provide the foundation for secure SMC protocols, ensuring that participants' data remains confidential throughout the computation process. These protocols have applications in various fields, such as secure voting systems, privacy-preserving data analysis, and confidential business agreements, where parties need to jointly process information without exposing sensitive details.

In addition to these applications, lattice-based cryptography plays a crucial role in the development of quantum-resistant communication protocols, particularly in the context of future 6G networks and beyond [10]. As quantum computing evolves, it threatens the security of current communication systems that rely on traditional cryptographic methods like RSA and ECC. The development of quantum-resistant protocols is therefore essential to ensure the continued security of communication systems. Lattice-based cryptography offers a natural solution, as its security is believed to be resistant to quantum attacks. In the context of 6G networks, which are expected to support ultra-high-speed, low-latency communication for applications such as autonomous vehicles, smart cities, and advanced healthcare, quantum-resistant communication protocols will be necessary to protect sensitive data and maintain the integrity of communications. Lattice-based cryptosystems can provide the foundation for such protocols, enabling the secure transmission of data across next-generation networks that are resistant to quantum threats.

In conclusion, lattice-based cryptography offers unique advantages for securing a wide range of applications in next-generation communication systems. Its ability to provide strong security guarantees against quantum attacks, along with its versatility in supporting a variety of cryptographic operations, makes it an ideal candidate for securing cloud computing, IoT, secure multi-party computation, and the development of quantum-resistant communication protocols for 6G networks and beyond. As the adoption of quantum computing becomes more widespread, lattice-based cryptography is poised to play a key role in ensuring the security and privacy of digital communication in the quantum era.

6. Conclusion

As quantum computing continues to advance, the need for post-quantum cryptographic solutions becomes increasingly urgent. The potential of quantum computers to break widely used cryptographic systems, such as RSA and ECC, has made it clear that existing cryptographic protocols will no longer be sufficient in the quantum era. Lattice-based cryptography, with its strong security guarantees and versatility, emerges as one of the most promising approaches to addressing this challenge. Due to its resistance to quantum attacks and its capability to support a wide range of cryptographic primitives, lattice-based cryptosystems are gaining significant attention as candidates for securing digital communication in the post-quantum world.

This paper has provided a comprehensive review of lattice-based cryptosystems, covering their mathematical foundations, practical challenges, and potential applications. We have explored key problems in lattice theory, such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem, and how these problems underpin the security of lattice-based cryptographic schemes. We have also discussed the significant challenges, including large key sizes, computational inefficiency, and storage demands, that must be overcome for the practical deployment of lattice-based systems. Solutions such as optimization techniques and hardware acceleration have been examined as potential ways to address these challenges.

Moreover, this paper has highlighted several real-world applications of lattice-based cryptography, including its use in cloud computing, the Internet of Things (IoT), secure multi-party computation, and the development of quantum-resistant communication protocols for future networks like 6G. The versatility of lattice-based cryptosystems makes them well-suited for a variety of scenarios, from protecting sensitive data to enabling privacy-preserving computations, positioning them as a foundational component of post-quantum secure infrastructure.

By offering a detailed analysis of the current state of lattice-based cryptography, we aim to contribute to the ongoing efforts to develop and standardize quantum-resistant cryptographic algorithms. These efforts, spearheaded by organizations such as NIST, are crucial in ensuring the long-term security of information systems in the quantum era. As quantum computing continues to evolve, lattice-based cryptography offers a pathway toward safeguarding digital communications and maintaining privacy and integrity in a world where quantum threats are a reality. Through continued research and development, lattice-based cryptosystems will play a pivotal role in shaping the future of secure communication in the post-quantum world.

References:

[1] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2), 303-332.
[2] Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4), 283-424.
[3] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6), 1-40.
[4] Micciancio, D., & Regev, O. (2007). Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*, 37(1), 267-302.
[5] Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. *Journal of the ACM*, 60(6), 1-35.
[6] National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography
[7] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange—A new hope. *USENIX Security Symposium*, 327-343.
[8] Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. *IEEE Symposium on Security and Privacy*, 553-570.
[9] Boneh, D., & Zhandry, M. (2013). Secure signatures and chosen ciphertext security in a quantum

computing world. *CRYPTO*, 361-379.
[10] Zhang, Z., & Wang, X. (2021). Quantum-resistant cryptography for 6G networks. *IEEE Communications Magazine*, 59(6), 62-68.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Numerical Modeling of Degenerate Parabolic Problems in Biological Population Diffusion

Mehdi Alaeiyan

School of Mathematics and Computer Science, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Iran

Omid Nikan [1]

School of Mathematics and Computer Science, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Iran

Abstract

This paper presents a localized meshless algorithm for solving the nonlinear biological population model (NBPM), which describes the dynamics of biological populations and provides useful predictions. The solution is approximated using the local radial basis function method based on the partition of unity (LRBF-PU). The partial differential equation (PDE) is first transformed into a system of ordinary differential equations (ODEs) using radial kernels, and the resulting system is solved using a high-order ODE solver. The approach avoids the need for linearization and addresses matrix ill-conditioning, a common issue in global RBF approximations. Numerical experiments demonstrate the method's superior efficiency and accuracy compared to existing techniques.

Keywords: Nonlinear Biological Population Model; RBF; LRBF-PU; Shape Parameter
AMS Mathematical Subject Classification [2010]: 65M06, 65M70, 35K55.

1 Introduction

Population models significantly enhance our understanding of natural phenomena and biological processes. They help describe dynamics, predict evolution, and assess the impact of environmental changes, such as global climate effects on species like polar bears and loggerhead sea turtles. Mathematically, the diffusion of biological populations in a region $\mathbb{R}^2$ is modeled by the population density $u(\mathbf{x}, t)$, diffusion velocity $v(\mathbf{x}, t)$, and supply rate $\mathcal{F}(\mathbf{x}, t)$. Gurtin and Maccamy [1] derived the nonlinear PDE:

$$u_t = \Delta\Phi(u) + \mathcal{F}(u), \tag{1}$$

with assumptions $\mathcal{F} = \mathcal{F}(u)$ and $v = -k(u)\nabla u$. For $\Phi(u) = u^2$, it reduces to:

$$u_t = \Delta u^2 + \mathcal{F}(u), \tag{2}$$

known as the Nonlinear Biological Population Model (NBPM). Various forms of $\mathcal{F}(u)$ include:

[1] speaker

- Malthusian law: $\mathcal{F} = \mu u$ [1],
- Verhulst law: $\mathcal{F} = \mu u - \gamma u^2$ [2],
- Porous media model: $\mathcal{F} = \mu u^\theta$ [3, 4].

A generalized form is $\mathcal{F}(u) = hu^\alpha(1 - ru^\beta)$, leading to:

$$u_t = \Delta u^2 + hu^\alpha(1 - ru^\beta). \tag{3}$$

Initial and boundary conditions are:

$$u(\mathbf{x}, 0) = f(\mathbf{x}), \quad \mathbf{x} \in \Omega, \tag{4}$$

$$u(\mathbf{x}, t) = g(\mathbf{x}, t), \quad (\mathbf{x}, t) \in \partial\Omega \times [0, T]. \tag{5}$$

Numerical techniques such as Adomian decomposition [5], variational iteration [6], homotopy perturbation [7], and radial basis functions [8] have been used to solve the NBPM. Localized methods like LRBF schemes effectively handle matrix ill-conditioning and improve accuracy and efficiency [9].

2 Numerical Implementation

The LRBF-PU method efficiently reduces computational time while maintaining high accuracy. It offers advantages such as geometrical flexibility for high-dimensional problems, reduced computational cost, and adaptability [10, 11].

Consider a computational domain $\Omega \subseteq \mathbb{R}^d$ covered by scattered points $\Xi = \{\mathbf{x}_1, \ldots, \mathbf{x}_N\}$. Using the RBF interpolation, the approximation takes the form:

$$u(\mathbf{x}) \simeq S(\mathbf{x}) = \sum_{j=1}^{N} \lambda_j \phi_j(\mathbf{x}, \varepsilon), \tag{6}$$

where $\phi_j(\mathbf{x}, \varepsilon)$ is a strictly positive definite (SPD) radial kernel. Imposing interpolation conditions $S(\mathbf{x}_i) = u_i$ yields the linear system:

$$A\lambda = u, \tag{7}$$

with $A_{ij} = \phi(\|\mathbf{x}_i - \mathbf{x}_j\|_2, \varepsilon)$. The interpolation can also be expressed using cardinal basis functions:

$$S(\mathbf{x}) = L(\mathbf{x})u, \quad \text{where} \quad L(\mathbf{x}) = \Phi A^{-1}. \tag{8}$$

For domain Ω, let $\{\Omega_j\}_{j=1}^M$ be overlapping subdomains with Shepard's partition of unity (PU) weights:

$$w_j(\mathbf{x}) = \frac{\varphi_j(\mathbf{x})}{\sum_{k \in I(\mathbf{x})} \varphi_k(\mathbf{x})}. \tag{9}$$

The global PU approximation $\mathcal{P}_u$ is:

$$\mathcal{P}_u(\mathbf{x}) = \sum_{j \in I(\mathbf{x})} w_j(\mathbf{x}) S_j(\mathbf{x}), \tag{10}$$

where S_j are local RBF interpolants. For partial derivatives, applying Leibniz's rule gives:

$$\Delta u(\mathbf{x}) = \sum_{j \in I(\mathbf{x})} \sum_{i \in J(\Omega_j)} \big(l_j \Delta w_j + 2\nabla w_j \cdot \nabla l_j + \Delta l_j w_j\big) u(\mathbf{x}_i). \tag{11}$$

To solve PDEs, collocation nodes are divided into boundary ($\mathcal{B}$) and interior ($\mathcal{I}$) nodes. The system matrix A is split as:

$$A = A_{\mathcal{I}} + A_{\mathcal{B}}, \tag{12}$$

where $A_{\mathcal{I}}$ and $A_{\mathcal{B}}$ correspond to interior and boundary points, respectively. Using differentiation matrices and collocating Eq. (11), the system of ODEs is:

$$\frac{\mathrm{d}U(t)}{\mathrm{d}t} = (\Delta A_{\mathcal{I}})U^2(t) + (\Delta A_{\mathcal{B}})G^2(t) + hU^{\alpha}(t)(1 - rU^{\beta}(t)). \tag{13}$$

The ODE system (13) can be solved using MATLAB's `ode15s` or other time-stepping methods. Stability is ensured by scaling the spatial operator's eigenvalues via the time step δt. Algorithm 1 summarizes the procedure.

Algorithm 1: Full Discretization of the NBPM

Input: $N, M, \delta t, T, \alpha, \beta, h, r$

1 $t_{\text{step}} = [0 : \delta t : T]$
2 Construct $\Delta A_{\mathcal{I}}$, $\Delta A_{\mathcal{B}}$
3 Set RHS: RHS $= \Delta A_{\mathcal{I}} U^2 + \Delta A_{\mathcal{B}} G^2 + hU^{\alpha}(1 - rU^{\beta})$
4 Set initial condition $U_0 = f(x)$
5 Solve: $[t, U] = \text{ode15s}(@(t, U)\text{RHS}, t_{\text{step}}, U_0, \text{options})$
6 Calculate absolute error

3 Numerical results

This section presents a numerical example demonstrating the application of the proposed method. The inverse multiquadric (IMQ) $\phi(r) = \frac{1}{\sqrt{1+\varepsilon^2 r^2}}$ was used as the basis function, and all computations were performed in MATLAB on a PC with 8 GB RAM. The accuracy of the method is evaluated using the error norms L_∞, L_2, and L_{rms}, defined as:

$$L_\infty = \max_{1 \le j \le N-1} |u(\mathbf{x}_j, T) - U(\mathbf{x}_j, T)|,$$

$$L_2 = \left(h_\Omega \sum_{j=1}^{N} \left(u(\mathbf{x}_j, T) - U(\mathbf{x}_j, T)\right)^2 \right)^{1/2},$$

$$L_{\text{rms}} = \left(\frac{1}{N} \sum_{j=1}^{N} \left(u(\mathbf{x}_j, T) - U(\mathbf{x}_j, T)\right)^2 \right)^{1/2},$$

where N is the number of collocation nodes in Ω, $h_\Omega = h_x = h_y$ is the minimum distance between any two nodes, and $u(\mathbf{x}_j, T)$ and $U(\mathbf{x}_j, T)$ represent the analytical and numerical solutions, respectively.

Example 3.1. Let us consider the NBPM when $\alpha = \beta = 1$, $h = 1/5$ and $r = 0$ that has analytic solution given by $u(x, y, t) = \exp(\frac{t}{5})\sqrt{xy}$.

We address this problem using the LRBF-PU method and investigate the impact of varying δt, M, and N on the total simulation time T. Table 1 presents a comparison of the error norms L_2 and L_∞, along with the CPU runtime (in seconds), for the LRBF-PU and MCBDQ methods [12] with $N = 144$, $M = 25$, and $\delta t = 0.0001$, evaluated at different total times T over the domain Ω_1. Table 2 provides a similar comparison of the error norms L_2 and L_∞, as well as the condition number (CN) and CPU runtime, for the LRBF-PU

and LRBF techniques [8] when $\delta t = 0.0001$, $N = 400$, $M = 25$, and $T = 1$ over Ω_1. From Tables 1 and 2, it is evident that the LRBF-PU method is both highly efficient and accurate. Additionally, the coefficient matrix for the LRBF-PU method is observed to be more well-posed compared to the LRBF method. Figure 1 illustrates the numerical solutions and corresponding absolute errors obtained for $N = 625$, $M = 64$, and $\delta t = 0.0001$ at $T \in \{10\}$ over the domain $[0, 3]^2$.

Table 1: Error norms L_2 and L_∞, and the CPU run time of the LRBF-PU and MCBDQ [12] with $N = 144$, $M = 25$ and $\delta t = 0.0001$ on Ω_1.

	MCBDQ [12]			LRBF-PU			
T	L_∞	L_2	CPU	L_∞	L_2	CN	CPU
2	$2.31e-03$	$7.94e-03$	5.87	$1.3420e-05$	$1.2854e-05$	$4.3037e+04$	1.24
5	$4.10e-03$	$1.50e-02$	14.84	$2.3437e-05$	$2.4471e-05$	$4.3069e+04$	1.99
8	$1.13e-02$	$3.06e-02$	23.79	$4.2698e-05$	$4.4541e-05$	$4.3069e+04$	2.69
10	$9.34e-02$	$2.07e-02$	29.60	$6.3697e-05$	$6.6509e-05$	$4.3069e+04$	3.15

Table 2: Error norms L_2 and L_∞, as well as CN and CPU run time of the LRBF-PU and LRBF [8] with $\delta t = 0.0001$, $N = 400$ and $M = 25$.

LRBF [8]				LRBF-PU			
L_∞	L_2	CN	CPU	L_∞	L_2	CN	CPU
$1.215e-05$	$7.643e-05$	$7.732e+13$	1.26577	$2.3497e-06$	$6.1431e-06$	$3.4250e+05$	1.13

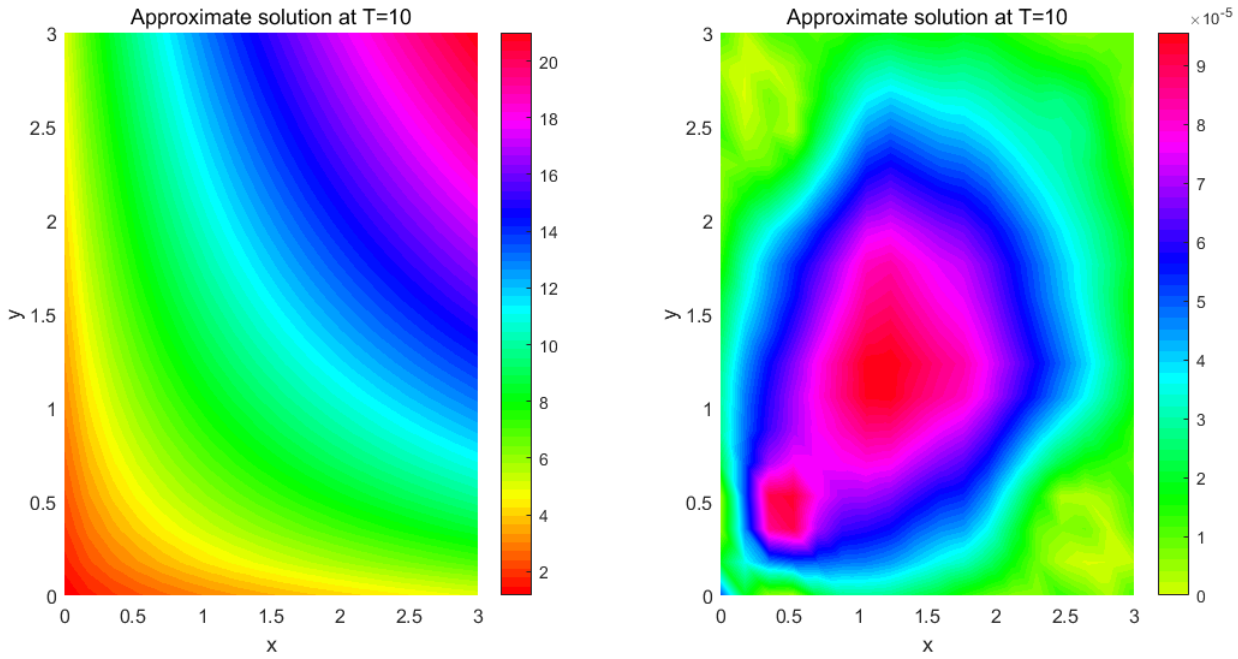


Figure 1: Approximate solutions and corresponding absolute errors at total time $T \in \{10\}$.

References

[1] M. E. Gurtin, R. C. MacCamy, On the diffusion of biological populations, Mathematical biosciences 33 (1-2) (1977) 35–49.

[2] Y.-G. Lu, Hölder estimates of solutions of biological population equations, Applied Mathematics Letters 13 (6) (2000) 123–126.

[3] J. Bear, Dynamics of fluids in porous media. Elsevier, New York (1972).

[4] A. Okubo, et al., Diffusion and ecological problems: mathematical models.

[5] F. Shakeri, M. Dehghan, Numerical solution of a biological population model using He's variational iteration method, Computers & Mathematics with Applications 54 (7-8) (2007) 1197–1209.

[6] M. Zellal, K. Belghaba, An accurate algorithm for solving biological population model by the variational iteration method using He's polynomials, Arab Journal of Basic and Applied Sciences 25 (3) (2018) 142–149.

[7] P. Roul, Application of homotopy perturbation method to biological population model, Applications and Applied Mathematics 10 (2010) 1369–1378.

[8] M. Uddin, H. Ali, M. Taufiq, On the approximation of a nonlinear biological population model using localized radial basis function method, Mathematical and Computational Applications 24 (2) (2019) 54.

[9] R. Cheng, L. Zhang, K.-M. Liew, Modeling of biological population problems using the element-free kp-Ritz method, Applied Mathematics and Computation 227 (2014) 274–290.

[10] A. Safdari-Vaighani, A. Heryudono, E. Larsson, A radial basis function partition of unity collocation method for convection–diffusion equations arising in financial applications, Journal of Scientific Computing 64 (2) (2015) 341–367.

[11] O. Nikan, Z. Avazzadeh, A localisation technique based on radial basis function partition of unity for solving Sobolev equation arising in fluid dynamics, Applied Mathematics and Computation 401 (2021) 126063.

[12] B. K. Singh, A novel approach for numeric study of 2D biological population model, Cogent Mathematics & Statistics 3 (1) (2016) 1261527.

e-mail: alaeiyan@iust.ac.ir
e-mail: omidnikan77@yahoo.com

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A localized kernel-based meshless approach for pricing financial options in fractal transmission systems

Omid Nikan

School of Mathematics and Computer Science, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Iran

Mohammad Navaz Rasoulizadeh[1]

Department of Mathematics, Velayat University, Iranshahr, Iran

Abstract

The option pricing dynamics in fractal transmission systems are described by the time-fractional Black-Scholes equation (TFBSE). This paper introduces an effective local meshless method for the numerical solution of the TFBSE. Initially, a semi-discrete algorithm is developed using an $L1$-type finite difference formula for the temporal variable, achieving an accuracy order of $2-\alpha$ for smooth solutions, where $0 < \alpha \leq 1$ represents the fractional-order derivative. In the second step, a localized radial basis function finite difference (LRBF-FD) approach is employed to construct a fully discrete scheme. The method's unconditional stability and convergence are rigorously examined using the energy norm framework. Exact weight expressions for first- and second-order derivatives are computed using a multiquadric function in the finite difference context. The proposed approach generates linear systems with tridiagonal and diagonal matrices, ensuring computational efficiency. Numerical experiments are conducted to demonstrate the effectiveness and accuracy of the method.

Keywords: Black-Scholes model, Fractional derivatives; Local meshless method; Radial basis function; Finite difference weights

AMS Mathematical Subject Classification [2010]: 35R11; 91G20; 65M70;p 41A30; 65M06

1 Introduction

The growing complexity of financial markets and increasing uncertainty compel investors to seek innovative strategies to adapt to volatile conditions and generate income. Options, among the most traded financial products, are commonly priced using mathematical models governed by partial differential equations (PDEs). The Black-Scholes (B-S) model, introduced by Merton, Black, and Scholes in 1973 [1, 2], describes option pricing using a second-order parabolic PDE. Although the B-S model led to significant advancements in option trading, its assumptions are overly idealistic for real-world scenarios.

To address these limitations, fractional derivatives [3] have been employed to model the memory and hereditary properties of financial systems. Fractional B-S models, such as the finite moment log stable

[1] speaker

(FMLS) model by Carr and Wu [4], and fractional Black-Scholes equations (TFBSE) have been developed to capture fractal dynamics in finance. Studies by Schmelzle [5], Cartea *et al.* [6], and others [7, 8] have introduced analytical and numerical methods for pricing options under fractional models.

This paper focuses on the approximate solution of the TFBSE using efficient local technique based on a radial basis function finite difference (RBF-FD) meshless technique. For this aim, let $C(S,t)$ denote the price of a European-style double-barrier option. The TFBSE is expressed as:

$$\begin{aligned}&\frac{\partial^\alpha C(S,t)}{\partial t^\alpha}+\frac{1}{2}\sigma^2S^2\frac{\partial^2C(S,t)}{\partial S^2}+(r-D)S\frac{\partial C(S,t)}{\partial S}-rC(S,t)=0,\\&C(b_d,t)=p(t),\quad C(b_u,t)=q(t),\quad C(S,T)=v(S),\end{aligned}\tag{1}$$

where $0<\alpha\leq 1$, σ is volatility, r is the risk-free rate, and D is the dividend rate. The operator $\frac{\partial^\alpha}{\partial t^\alpha}$ represents the Riemann-Liouville fractional derivative, which can be reformulated as an initial value problem using $\tau=T-t$:

$${}_0D_\tau^\alpha C(S,T-\tau)=\frac{1}{\Gamma(1-\alpha)}\frac{\mathrm{d}}{\mathrm{d}\tau}\int_0^\tau\frac{C(S,T-\eta)-v(S)}{(\tau-\eta)^\alpha}\,\mathrm{d}\eta.\tag{2}$$

By taking $x=\ln S$ and $v(x,\tau)=C(\exp(x),T-\tau)$, and introducing a source term $g(x,\tau)$, the equation becomes:

$$\frac{\partial^\alpha v(x,\tau)}{\partial\tau^\alpha}=\frac{1}{2}\sigma^2\frac{\partial^2v(x,\tau)}{\partial x^2}+(r-\frac{1}{2}\sigma^2-D)\frac{\partial v(x,\tau)}{\partial x}-rv(x,\tau)+g(x,\tau),\tag{3}$$

$$v(x,0)=v(x),\qquad b_d<x<b_u,\tag{4}$$

$$v(b_d,\tau)=p(\tau),\quad v(b_u,\tau)=q(\tau),\quad 0<\tau<T,\tag{5}$$

where $0<\alpha<1$.

Golbabai *et al.* [15] showed that the fractional derivative $\frac{\partial^\alpha v(x,\tau)}{\partial\tau^\alpha}$ is equivalent to the Caputo fractional derivative:

$${}_0D_\tau^\alpha v(x,\tau)=\frac{\partial^\alpha v(x,\tau)}{\partial\tau^\alpha}=\frac{1}{\Gamma(1-\alpha)}\frac{\mathrm{d}}{\mathrm{d}\tau}\int_0^\tau\frac{v(x,\eta)-v(x,0)}{(\tau-\eta)^\alpha}\,\mathrm{d}\eta={}_0^CD_\tau^\alpha v(x,\tau),\tag{6}$$

for $0<\alpha\leq 1$, where v is continuously time differentiable.

Various numerical approaches for solving the TFBSE have been proposed, including finite difference schemes [9, 10], Monte Carlo methods [11], and collocation techniques [12, 13]. Other works, such as [14, 15], employed global radial basis functions (RBFs) and Chebyshev methods for solution approximation.

2 Numerical Implementation

2.1 Time Discrete Scheme

This section employs a finite difference (FD) algorithm to discretize the time-fractional derivative. Let $\tau_n=n\delta t$, where $0\leq n\leq M$ and $\delta t=\frac{T}{M}$ represents the time step. Using the $L1$ approximation [17], the fractional derivative in Eq. (1) is approximated as:

$$\frac{\partial^\alpha v(x,\tau_{n+1})}{\partial t^\alpha}=\frac{\delta t^{-\alpha}}{\Gamma(2-\alpha)}\left[(v^{n+1}-v^n)+\sum_{k=1}^{n}\lambda_\alpha(k)(v^{n+1-k}-v^{n-k})\right]+\mathcal{O}(\delta t^{2-\alpha}),\tag{7}$$

where $a_0=\frac{\delta t^{-\alpha}}{\Gamma(2-\alpha)}$, $\lambda_\alpha(k)=(k+1)^{1-\alpha}-k^{1-\alpha}$, and $v^0=v(x,\tau=0)$. The convergence rate of $2-\alpha$ holds for smooth solutions [16].

Using Eq. (7) and the θ-weighted method ($0 < \theta \leq \frac{1}{2}$), the semi-discrete scheme for Eq. (1) is formulated as:

$$a_\alpha v^{n+1} - \gamma_1\theta\nabla^2 v^{n+1} - \gamma_2\theta\nabla v^{n+1} + \gamma_3 v^{n+1} = \begin{cases} \gamma_1(1-\theta)\nabla^2 v^n + \gamma_2(1-\theta)\nabla v^n \\ +a_\alpha\big[v^n - \sum_{k=1}^{n}\lambda_\alpha(k)(v^{n+1-k} - v^{n-k})\big] + g^{n+1}, & n \geq 1, \\ a_\alpha v^0 + g^1, & n = 0, \end{cases} \tag{8}$$

where $\gamma_1 = \frac{1}{2}\sigma^2 > 0$, $\gamma_2 = r - D - \gamma_1$, $\gamma_3 = r > 0$, and $g^{n+1} = g(x, \tau_{n+1})$.

Ignoring truncation errors R^{n+1} and letting V^n approximate v^n, the semi-discrete algorithm becomes:

$$a_\alpha V^{n+1} - \gamma_1\theta\nabla^2 V^{n+1} - \gamma_2\theta\nabla V^{n+1} + \gamma_3 V^{n+1} = \begin{cases} \gamma_1(1-\theta)\nabla^2 V^n + \gamma_2(1-\theta)\nabla V^n \\ +a_\alpha\big[V^n - \sum_{k=1}^{n}\lambda_\alpha(k)(V^{n+1-k} - V^{n-k})\big] + g^{n+1}, & n \geq 1, \\ a_\alpha V^0 + g^1, & n = 0. \end{cases} \tag{9}$$

Defining the operator $\mathcal{L}$, we rewrite Eq. (9) as:

$$\mathcal{L}(*) = \begin{cases} [a_\alpha + \gamma_3 - \theta\gamma_2\nabla - \theta\gamma_1\nabla^2](*) & 1 < i < N, \\ (*) & i = 1 \text{ or } i = N, \end{cases} \tag{10}$$

and the right-hand side:

$$b^{n+1} = \begin{cases} \gamma_1(1-\theta)\nabla^2 V^n + \gamma_2(1-\theta)\nabla V^n \\ +a_\alpha\big[V^n - \sum_{k=1}^{n}\lambda_\alpha(k)(V^{n+1-k} - V^{n-k})\big] + g^{n+1}, & n \geq 1, \\ a_\alpha V^0 + g^1, & n = 0. \end{cases} \tag{11}$$

Thus, the semi-discrete system can be expressed as:

$$\mathcal{L}V(x, \tau_{n+1}) = b^{n+1}. \tag{12}$$

2.2 Spatial Discretization

RBF meshfree techniques are classified into global and local approaches. While global methods suffer from ill-conditioning due to dense matrices and shape parameter sensitivity, local techniques overcome these issues by employing only adjacent data points, resulting in sparse matrices and reduced execution time.

The standard RBF interpolation approximates a function $u(\mathbf{x})$ as:

$$u(\mathbf{x}) \simeq S(\mathbf{x}) = \sum_{j=1}^{N} \beta_j \phi_j(\mathbf{x}, c), \tag{13}$$

where β_j are unknown coefficients, $\phi_j(\mathbf{x}, c)$ are RBFs with shape parameter c, and $\|\cdot\|$ denotes the Euclidean norm. The coefficients $\{\beta_j\}$ are determined by enforcing $S(\mathbf{x}_i^c) = u_i^c$, leading to a nonsingular linear system [20, 19].

To improve conditioning, RBF-FD methods localize the collocation using stencils $\Xi^{(i)} \subset \Xi$. A linear operator $\mathbf{L}$ is approximated as:

$$\mathbf{L}V(\mathbf{x}_i) \simeq \sum_{j=1}^{n_s} \omega_j^{(i)} V(\mathbf{x}_j^{(i)}), \tag{14}$$

where $\{\omega_j^{(i)}\}$ are weights calculated using RBFs centered at stencil nodes:

$$\mathbf{L}\phi_k(\mathbf{x}_i, c) = \sum_{j=1}^{n_s} \omega_j^{(i)} \phi_j(\mathbf{x}_k, c), \quad k = 1, \ldots, n_s. \tag{15}$$

Collocating (15) at stencil nodes results in a linear system:

$$\mathbf{\Phi}\boldsymbol{\omega}^{(i)} = [\mathbf{L}\mathbf{\Phi}]^{(i)}, \quad \boldsymbol{\omega}^{(i)} = \mathbf{\Phi}^{-1}[\mathbf{L}\mathbf{\Phi}]^{(i)}, \tag{16}$$

where $\mathbf{\Phi}$ is the interpolation matrix, and $[\mathbf{L}\mathbf{\Phi}]^{(i)}$ contains operator evaluations.

The RBF-FD method efficiently computes weights for differential operators while maintaining sparsity. Table 1 lists weights for the first and second derivatives using stencils with $n_s = 3$ and 5 equispaced nodes.

Table 1: RBF-FD weights for first and second derivatives.

Node	First derivative		Second derivative	
	$n_s = 3$	$n_s = 5$	$n_s = 3$	$n_s = 5$
x_{i-2h}	$\frac{1}{12h}\left(1 + \frac{8h^2}{c^2}\right)$	–	$-\frac{1}{12h^2}\left(1 + \frac{74h^2}{7c^2}\right)$	–
x_{i-h}	$-\frac{1}{2h}\left(1 + \frac{h^2}{2c^2}\right)$	$-\frac{2}{3h}\left(1 + \frac{2h^2}{c^2}\right)$	$\frac{1}{h^2}\left(1 + \frac{h^2}{c^2}\right)$	$\frac{4}{3h^2}\left(1 + \frac{37h^2}{14c^2}\right)$
x_i	0	0	$-\frac{2}{h^2}\left(1 + \frac{h^2}{c^2}\right)$	$-\frac{5}{2h^2}\left(1 + \frac{74h^2}{35c^2}\right)$
x_{i+h}	$\frac{1}{2h}\left(1 + \frac{h^2}{2c^2}\right)$	$\frac{2}{3h}\left(1 + \frac{2h^2}{c^2}\right)$	$\frac{1}{h^2}\left(1 + \frac{h^2}{c^2}\right)$	$\frac{4}{3h^2}\left(1 + \frac{37h^2}{14c^2}\right)$
x_{i+2h}	$-\frac{1}{12h}\left(1 + \frac{8h^2}{c^2}\right)$	–	$-\frac{1}{12h^2}\left(1 + \frac{74h^2}{7c^2}\right)$	–

The full discretization equation for time levels n and $n+1$ is:

$$\sum_{j=1, j\neq i}^{n_s} \zeta_j^{n+1} V^{n+1}(x_j^{(i)}) + \eta_i^{n+1} V^{n+1}(x_i) = \sum_{j=1, j\neq i}^{n_s} \zeta_j^{n} V^{n}(x_j^{(i)}) + \kappa_i^{n} V^{n}(x_i) + F^{n+1}(x_i), \tag{17}$$

where ζ_j, η_i, and κ_i are weight coefficients, and $F^{n+1}(x_i)$ accounts for source terms. This scheme supports backward Euler ($\theta = 1$) and Crank-Nicolson ($\theta = 0.5$) time-stepping methods.

3 Numerical results

This section demonstrates the solution's behavior and evaluates the proposed method's performance in terms of accuracy and convergence.

Example 3.1. Consider the TFBSE for a European option:

$$\begin{aligned}
&\frac{\partial^\alpha C(S,t)}{\partial t^\alpha} + \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 C(S,t)}{\partial S^2} + (r-D)S\frac{\partial C(S,t)}{\partial S} - rC(S,t) = 0, \quad (S,t) \in (b_d, b_u) \times (0,T),\\
&C(0,t) = 0, \quad C(1,t) = 0,\\
&C(S,T) = \max(S - K_1, 0) - 2\max(S - K_2, 0) + \max(S - K_3, 0),
\end{aligned}$$

where $\sigma = 0.5$, $r = 0.1$, $D = 0$, $T = 1$, and strike prices $K_1 = 0.6$, $K_2 = 0.65$, and $K_3 = 0.7$.

Since Example 3.1 lacks an analytical solution, the double-mesh principle is used to compute numerical errors. Table 2 shows L_∞ errors for various N and α values at $T = 1$. The results demonstrate the proposed method's accuracy. Figure 1 illustrates the option values $C(S, 1)$ for $\alpha \in \{0.25, 0.45, 0.75, 1\}$, highlighting the impact of α on the solution.

Table 2: Numerical errors L_∞ for various N and α with $\delta t = 1/200$ at $T = 1$ in Example 3.1.

α	$N = 140$	$N = 280$	$N = 680$	$N = 960$
0.3	5.9970×10^{-3}	4.4017×10^{-3}	3.6622×10^{-3}	1.6704×10^{-3}
0.5	3.7780×10^{-3}	1.1382×10^{-3}	1.0103×10^{-3}	7.8791×10^{-4}
0.7	3.6896×10^{-3}	2.1376×10^{-3}	9.1502×10^{-4}	5.7112×10^{-4}
0.9	8.6626×10^{-4}	5.0567×10^{-4}	1.2252×10^{-4}	1.0192×10^{-4}

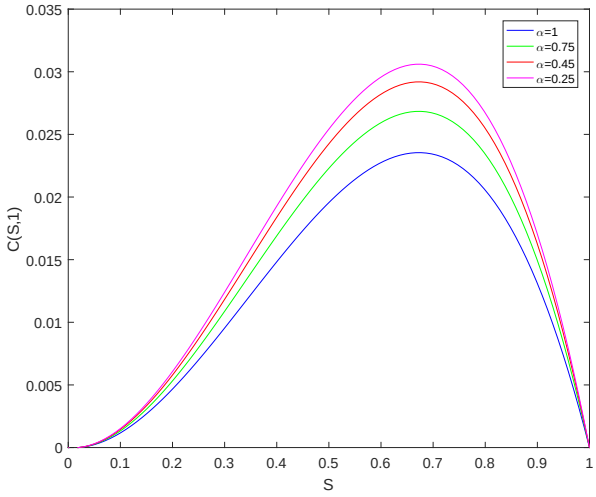


Figure 1: Option prices obtained by the TFBSE at different α in Example 3.1 when $T = 1$.

References

[1] Black, Fischer, and Scholes, Myron. The pricing of options and corporate liabilities. *Journal of Political Economy.* 1973;81(3):637–654.

[2] Merton, Robert C. Theory of rational option pricing. *The Bell Journal of Economics and Management Science.* 1973;:141–183.

[3] Kilbas, Anatoliĭ. *Theory and applications of fractional differential equations.* Elsevier; 2006.

[4] Wyss, Walter. The fractional Black-Scholes equation. *Fractional Calculus and Applied Analysis.* 2000;3(1):51–61.

[5] Schmelzle Martin. *Option pricing formulae using Fourier transform: Theory and application.* Preprint, http://pfadintegral. com. 2010;.

[6] Cartea, Alvaro, and Castillo-Negrete, Diego. Fractional diffusion models of option prices in markets with jumps. *Physica A: Statistical Mechanics and its Applications.* 2007;374(2):749–763.

[7] Chen, Wenting, Xu, Xiang, and Zhu, Song-ping. Analytically pricing European-style options under the modified Black-Scholes equation with a spatial-fractional derivative. *Quarterly of Applied Mathematics.* 2014;72(3):597–611.

[8] Kumar, Sunil, et al. Analytical solution of fractional Black-Scholes European option pricing equation by using Laplace transform. *Journal of Fractional Calculus and Applications.* 2012;2(8):1–9.

[9] Song, Lina, and Wang, Weiguo. Solution of the fractional Black-Scholes option pricing model by finite difference method. *Abstract and Applied Analysis.* 2013;2013 Article ID 194286:1–10.

[10] Chen Wenting, Xu Xiang, Zhu Song-Ping. A predictor–corrector approach for pricing American options under the finite moment log-stable model. *Applied Numerical Mathematics.* 2015;97:15–29.

[11] Li Qing, Zhou Yanli, Zhao Xinquan, Ge Xiangyu. Fractional order stochastic differential equation with application in European option pricing. *Discrete Dynamics in Nature and Society.* 2014; 2014, Article ID 621895:1–12.

[12] Mesgarani H, Beiranvand A, Aghdam Y Esmaeelzade. The impact of the Chebyshev collocation method on solutions of the time-fractional Black–Scholes. *Mathematical Sciences.* 2020;1:1–7.

[13] Roul Pradip. A high accuracy numerical method and its convergence for time-fractional Black-Scholes equation governing European options. *Applied Numerical Mathematics.* 2020;151:472–493.

[14] Zhang Hongmei, Liu Fawang, Turner Ian, Yang Qianqian. Numerical solution of the time fractional Black–Scholes model governing European options. *Computers & Mathematics with Applications.* 2016;71(9):1772–1783.

[15] Golbabai Ahmad, Nikan Omid. A computational method based on the moving least-squares approach for pricing double barrier options in a time-fractional Black–Scholes model. *Computational Economics.* 2020;55(1):119–141.

[16] Zaky, Mahmoud A., Hendy, Ahmed S., and Macías-Díaz, Jorge E. Semi-implicit Galerkin–Legendre spectral schemes for nonlinear time-space fractional diffusion-reaction equations with smooth and nonsmooth solutions. *Journal of Scientific Computing.* 2020;82(1):1–27.

[17] Liu, Fawang, Zhuang, Pinghui, Anh, Vo, Turner, Ian, and Burrage, Kevin. Stability and convergence of the difference methods for the space–time fractional advection–diffusion equation. *Applied Mathematics and Computation.* 2007;191(1):12–20.

[18] Nikan, Omid, Avazzadeh, Zahra, and Machado, J.A. Tenreiro. Numerical investigation of fractional nonlinear sine-Gordon and Klein-Gordon models arising in relativistic quantum mechanics. *Engineering Analysis with Boundary Elements.* 2020;120:223–237.

[19] Buhmann, Martin D. *Radial basis functions: theory and implementations.* Cambridge University Press; 2003.

[20] Wendland, Holger. *Scattered data approximation.* Cambridge University Press; 2004.

[21] Bayona, Victor, Moscoso, Miguel, Carretero, Manuel, and Kindelan, Manuel. RBF-FD formulas and convergence properties. *Journal of Computational Physics.* 2010;229(22):8281–8295.

e-mail: omidnikan77@yahoo.com
e-mail: mn.rasoulizadeh@velayat.ac.ir

نهمین کنفرانس بین‌المللی
ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات
۵ و ۶ دی ۱۴۰۳

مروری جامع بر فناوری بلاکچین: اصول اساسی و پیشینه تاریخی همراه با چالش‌های آینده

مهدی علائیان[۱]
دانشگاه علم و صنعت ایران، دانشکده ریاضی و علوم کامپیوتر، تهران، ایران

چکیده

فناوری بلاکچین یک دفتر کل دیجیتال توزیع‌شده است که کسب‌وکارها، صنایع و تجارت را با حذف نیاز به یک مرجع مرکزی برای ذخیره و کنترل متحول کرده است. بلاکچین بلوک‌های داده‌ای دارای برچسب زمانی و غیرقابل تغییر ارائه می‌دهد که به‌جای اینکه توسط یک نهاد واحد مالکیت شوند، توسط گروهی از گره‌ها یا رایانه‌ها مدیریت می‌شوند، جایی که هر بلوک با استفاده از اصول رمزنگاری ایمن و به هم متصل می‌شود. طبیعت غیرقابل تغییر و غیرمتمرکز بلاکچین اعتماد، مالکیت، هویت و سیستم‌های مالی را بازتعریف کرده است و راه‌حلی امن، سریع، شفاف و شبه‌ناشناس ارائه می‌دهد. این مقاله مروری جامع بر فناوری بلاکچین با تمرکز بر پیشینه تاریخی، اصول اساسی و افزایش ناگهانی محبوبیت این فناوری ارائه می‌دهد. همچنین مقاله الگوریتم‌های مختلف اجماع در فناوری بلاکچین را مورد بحث قرار می‌دهد. در ادامه، مقاله بر حوزه‌های کاربردی مختلف و موارد استفاده آینده‌نگر فناوری بلاکچین با چالش‌ها و مسائل زیرساختی تمرکز می‌کند. علاوه بر این، مقاله برخی موارد استفاده غیرمتعارف از فناوری بلاکچین را نیز ارائه می‌دهد. این مطالعه همچنین مقالات پیشرفته را بررسی کرده تا نمای کلی جامعی از جنبه‌های مختلف فناوری بلاکچین در حوزه‌های متنوع ارائه دهد. مقایسه بین سیستم‌های پایگاه داده سنتی و فناوری بلاکچین ارائه شده و سناریوهای مناسب برای استفاده از راه‌حل‌های مبتنی بر بلاکچین که ممکن است در آن‌ها بهترین عملکرد را داشته باشند یا نداشته باشند، نیز مورد بحث قرار گرفته است.

واژه‌های کلیدی: فناوری بلاکچین، الگوریتم‌های اجماع، دفتر کل توزیع‌شده غیرمتمرکز، تغییرناپذیری، رمزنگاری، شفافیت

۱ مقدمه

فناوری بلاکچین یک دفتر کل دیجیتال توزیع‌شده است که کسب‌وکارها، صنایع و تجارت را با حذف نیاز به یک مرجع مرکزی برای ذخیره و کنترل متحول کرده است. بلاکچین بلوک‌های داده‌ای دارای برچسب زمانی و غیرقابل تغییر ارائه می‌دهد که به‌جای اینکه توسط یک نهاد واحد مالکیت شوند، توسط گروهی از گره‌ها یا رایانه‌ها مدیریت می‌شوند، جایی که هر بلوک با استفاده از اصول رمزنگاری ایمن و به هم متصل می‌شود. طبیعت غیرقابل تغییر و غیرمتمرکز بلاکچین اعتماد، مالکیت، هویت و سیستم‌های مالی را بازتعریف کرده است و راه‌حلی امن، سریع، شفاف و شبه‌ناشناس ارائه می‌دهد.

این مقاله مروری جامع بر فناوری بلاکچین با تمرکز بر پیشینه تاریخی، اصول اساسی و افزایش ناگهانی محبوبیت این فناوری ارائه می‌دهد. همچنین مقاله الگوریتم‌های مختلف اجماع در فناوری بلاکچین را مورد بحث قرار می‌دهد. در ادامه، مقاله بر حوزه‌های کاربردی مختلف و موارد استفاده آینده‌نگر فناوری بلاکچین با چالش‌ها و مسائل زیرساختی تمرکز می‌کند. علاوه بر این، مقاله برخی موارد استفاده غیرمتعارف از فناوری بلاکچین را نیز ارائه می‌دهد. این مطالعه همچنین مقالات پیشرفته را بررسی کرده تا نمای کلی جامعی از جنبه‌های مختلف فناوری بلاکچین در حوزه‌های متنوع ارائه دهد.

مقایسه بین سیستم‌های پایگاه داده سنتی و فناوری بلاکچین ارائه شده و سناریوهای مناسب برای استفاده از راه‌حل‌های مبتنی بر بلاکچین که ممکن است در آن‌ها بهترین عملکرد را داشته باشند یا نداشته باشند، نیز مورد بحث قرارگرفته است. علاوه بر این، مقاله برخی از بدنام‌ترین نقض‌های امنیتی که در گذشته اخیر صنعت بلاکچین را تحت تأثیر قرار داده‌اند، بررسی می‌کند.

[۱] سخنران

۱.۱ نقش بلاکچین در تحول سیستم‌های آموزشی دانشگاهی

بلاکچین در سیستم‌های آموزشی دانشگاهی می‌تواند انقلابی در مدیریت داده‌ها و فرآیندهای آموزشی ایجاد کند. این فناوری امکان ذخیره‌سازی امن و تغییرناپذیر مدارک تحصیلی، گواهینامه‌ها و سوابق آموزشی دانشجویان را فراهم می‌کند، که به جلوگیری از جعل مدارک و افزایش اعتماد میان مؤسسات آموزشی و کارفرمایان کمک می‌کند. همچنین، پروتکل‌های مبتنی بر بلاکچین می‌توانند فرآیند ثبت‌نام و تأیید هویت دانشجویان را تسهیل کنند و نیاز به واسطه‌های متعدد را کاهش دهند. از سوی دیگر، استفاده از قراردادهای هوشمند در سیستم‌های آموزشی می‌تواند به طور خودکار اجرای تعهدات مختلف مانند پرداخت شهریه، ثبت‌نام در دوره‌ها، یا تخصیص منابع آموزشی را مدیریت کند. بلاکچین همچنین می‌تواند در سیستم‌های یادگیری غیرمتمرکز، از جمله به اشتراک‌گذاری منابع و ایجاد انگیزه برای یادگیری مشارکتی، مؤثر باشد. در نهایت، این فناوری می‌تواند تعاملات شفاف و اعتمادآمیز بین دانشجویان، اساتید و دانشگاه‌ها را تقویت کند و از بهره‌وری بیشتر سیستم‌های آموزشی اطمینان حاصل کند.

۲ بررسی فناوری بلاکچین

فناوری بلاکچین یک دفتر کل دیجیتال توزیع‌شده است که کسب‌وکارها، صنایع و تجارت را با حذف نیاز به یک مرجع مرکزی برای ذخیره و کنترل متحول کرده است. بلاکچین بلوک‌های داده‌ای دارای برچسب زمانی و غیرقابل تغییر ارائه می‌دهد که به‌جای اینکه توسط یک نهاد واحد مالکیت شوند، توسط گروهی از گره‌ها یا رایانه‌ها مدیریت می‌شوند، جایی که هر بلوک با استفاده از اصول رمزنگاری ایمن و به هم متصل می‌شود. طبیعت غیرقابل تغییر و غیرمتمرکز بلاکچین اعتماد، مالکیت، هویت و سیستم‌های مالی را بازتعریف کرده است و راه‌حلی امن، سریع، شفاف و شبه‌ناشناس ارائه می‌دهد.

این مقاله مروری جامع بر فناوری بلاکچین با تمرکز بر پیشینه تاریخی، اصول اساسی و افزایش ناگهانی محبوبیت این فناوری ارائه می‌دهد. همچنین مقاله الگوریتم‌های مختلف اجماع در فناوری بلاکچین را مورد بحث قرار می‌دهد. در ادامه، مقاله بر حوزه‌های کاربردی مختلف و موارد استفاده آینده‌نگر فناوری بلاکچین با چالش‌ها و مسائل زیرساختی تمرکز می‌کند. علاوه بر این، مقاله برخی موارد استفاده غیرمتعارف از فناوری بلاکچین را نیز ارائه می‌دهد. این مطالعه همچنین مقالات پیشرفته را بررسی کرده تا نمای کلی جامعی از جنبه‌های مختلف فناوری بلاکچین در حوزه‌های متنوع ارائه دهد.

مقایسه بین سیستم‌های پایگاه داده سنتی و فناوری بلاکچین ارائه شده و سناریوهای مناسب برای استفاده از راه‌حل‌های مبتنی بر بلاکچین که ممکن است در آن‌ها بهترین عملکرد را داشته باشند یا نداشته باشند، نیز مورد بحث قرار گرفته است. علاوه بر این، مقاله برخی از بدنام‌ترین نقض‌های امنیتی که در گذشته اخیر صنعت بلاکچین را تحت تأثیر قرار داده‌اند، بررسی می‌کند.

۳ مفاهیم بلاکچین

۱.۳ اجماع [۲]

مکانیسم‌های اجماع ستون فقرات هر برنامه مبتنی بر بلاکچین را تشکیل می‌دهند. ماهیت غیرمتمرکز بلاکچین نیازمند مجموعه‌ای از قوانین برای شناسایی روشی است که کاربران بتوانند بر روی یک حالت خاص توافق کنند. این مجموعه قوانین توسط مکانیسم‌های اجماع ارائه می‌شود. اولین الگوریتم اجماع، **اثبات کار** [۳]، برای بلاکچین بیت‌کوین معرفی شد [۱]. از آن زمان، چندین الگوریتم اجماع برای پاسخگویی به نیازهای برنامه‌های بلاکچین معرفی شده‌اند. رایج‌ترین روش‌های اجماع در زیر شرح داده شده‌اند.

۱.۱.۳ اثبات کار [۴]

اثبات کار بر اصل یافتن راه‌حلی استوار است که شناسایی آن بسیار دشوار، اما تأیید آن آسان است. اکثر پیاده‌سازی‌های بلاکچین از اثبات کار به‌عنوان مکانیسم اجماع خود استفاده می‌کنند. در این روش، نودهای جدید از طریق حل یک مسئله پیچیده ایجاد می‌شوند. این فرایند به شدت محاسباتی است و به توان محاسباتی بالایی نیاز دارد [۲، ۳، ۴، ۵].

[2] Consensus
[3] Proof of Work
[4] Proof of Work

۲.۱.۳ اثبات سهام [5]

در مکانیسم اجماع اثبات سهام، اعتباردهندگان باید ارز دیجیتال (مانند [6]) خود را به‌عنوان وثیقه قفل کنند. اعتباردهندگان نقشی مشابه ماینرها در اثبات کار دارند. برای بلاکچین اتریوم، حداقل مقدار وثیقه برای تبدیل شدن به یک اعتباردهنده ۳۲ واحد [7] است. در اثبات سهام، اعتباردهندگان به صورت تصادفی برای ایجاد بلوک‌ها و تأیید بلوک‌های دیگر انتخاب می‌شوند. در هر دو حالت، اعتباردهندگان پاداش دریافت می‌کنند [۲، ۳، ۴، ۵].

۳.۱.۳ اثبات سهام نمایندگی‌شده [8]

الگوریتم اجماع اثبات سهام نمایندگی‌شده توسط **دنیل لاریمر** توسعه یافت. این روش تغییری بر روی اثبات سهام سنتی ایجاد می‌کند و سیستمی از انتخابات را برای انتخاب نودهایی که به‌عنوان شاهدان برای تأیید بلوک‌ها عمل می‌کنند، ارائه می‌دهد [۲، ۳، ۴، ۵].

۴.۱.۳ تحمل خطای بیزانسی عملی [9]

الگوریتم تحمل خطای بیزانسی عملی توسط **میگوئل کاسترو** و **باربارا لیسکوف** معرفی شد. این الگوریتم اجماع در پلتفرم‌هایی مانند هایپرلجر فابریک [10] و [11] استفاده می‌شود. تحمل خطای بیزانسی عملی از یک ماشین حالت بیزانسی عملی برای تحمل نودهای مخرب (خطاهای بیزانسی) استفاده می‌کند. نودهای موجود در یک سیستم تحمل خطای بیزانسی عملی با یکدیگر ارتباط برقرار می‌کنند تا همه نودهای صادق را به توافق برسانند [۲، ۳، ۴، ۵].

۵.۱.۳ اثبات فعالیت [12]

اثبات فعالیت ترکیبی از الگوریتم‌های اثبات کار و اثبات سهام است. فرایند استخراج اولیه مشابه اثبات کار است، اما پس از استخراج بلوک، اثبات سهام برای انتخاب گروهی تصادفی از اعتباردهندگان برای تأیید بلوک استخراج‌شده جدید استفاده می‌شود [۲، ۳، ۴، ۵].

۶.۱.۳ اثبات سوزاندن [13]

اثبات سوزاندن یک جایگزین کم‌مصرف برای الگوریتم‌های اثبات کار ارائه می‌دهد. در این روش، قدرت استخراج یک ماینر بر اساس تعداد سکه‌هایی که می‌سوزاند تعیین می‌شود. هرچه تعداد سکه‌های سوزانده شده بیشتر باشد، قدرت استخراج ماینر نیز بیشتر خواهد بود [۲، ۳، ۴، ۵].

۷.۱.۳ اثبات ظرفیت [14]

اثبات ظرفیت حقوق استخراج را با استفاده از فضای اختصاصی هارد دیسک دستگاه‌های ماینینگ تعیین می‌کند. راه‌حل‌های ممکن به‌صورت پیش‌فرض در هارد دیسک ماینرها ذخیره می‌شوند. این الگوریتم شامل دو مرحله پلات‌بندی و استخراج است [۲، ۳، ۴، ۵].

۸.۱.۳ اثبات زمان سپری‌شده [15]

اثبات زمان سپری‌شده بر اساس مفهوم یک سیستم قرعه‌کشی عادلانه است. این الگوریتم از زمان انتظار تصادفی برای تعیین حقوق استخراج استفاده می‌کند. هر نود شرکت‌کننده در سیستم اثبات زمان سپری‌شده منتظر یک زمان تصادفی می‌ماند. اولین نودی که زمان انتظار خود را به پایان برساند، اجازه دارد بلوک جدید را در بلاکچین ثبت کند [۲، ۳، ۴، ۵، ۶].

[5] Proof of Stake
[6] Ethereum
[7] Ethereum
[8] Delegated Proof of Stake
[9] Practical Byzantine Fault Tolerance
[10] Hyperledger Fabric
[11] Zilliqa
[12] Proof of Activity
[13] Proof of Burn
[14] Proof of Capacity
[15] Proof of Elapsed Time

جدول ۱: دسته‌بندی الگوریتم‌های اجماع [۱، ۲، ۳، ۴، ۵].

ردیف	دسته‌بندی	نمونه‌هایی از الگوریتم‌های اجماع
۱	اثبات کار	اثبات کار، اثبات کار معنادار، اثبات کار ترکیبی، اثبات کار تأخیری، اثبات کار زمان
۲	اثبات سهام	اثبات سهام (PoS)، اثبات سهام امن (SPoS)، اثبات سهام نمایندگی‌شده (DPoS)، اثبات سهام زمان (PoST)، اثبات سهام با سود بالا (HiPoS)
۳	تحمل خطای بیزانسی و pBFT	آلباتروس، تحمل خطای بیزانسی غیرهمزمان، بی‌اف‌تری، توافق بیزانسی فدرال، LibraBFT
۴	گراف غیرمدور جهت‌دار (DAG)	بلاک‌فلو، هش‌گراف
۵	محاسبات مورد اعتماد	اثبات زمان سپری‌شده
۶	ترکیبی	اثبات اختیار، اثبات فعالیت
۷	اثبات ظرفیت/فضا	اثبات وجود، اثبات تاریخ، اثبات مکان

جدول ۲: مزایا و معایب الگوریتم‌های اجماع محبوب [۱، ۲، ۳، ۴، ۵].

ردیف	الگوریتم	مزایا	معایب	نمونه‌ها
۱	اثبات کار	امنیت بالا، کاهش حملات انکار سرویس (DoS)	محاسبات فشرده، انرژی‌بر، کند، امکان حمله ٪۵۱	بیت‌کوین، اتریوم
۲	اثبات سهام	بهینه از نظر انرژی، کمتر محاسباتی، سخت برای حمله	مشکل "چیزی در خطر نیست"، احتمال تمرکز، حمله ٪۵۱ با سهام بالا	پیرکوین
۳	اثبات سهام نمایندگی‌شده	بهینه از نظر انرژی، سریع	احتمال تمرکز	بیت‌شیر، EOS
۴	اثبات کار تأخیری	بهینه از نظر انرژی، امنیت بالا	وابسته به زنجیره‌های PoW و PoS	کومودو
۵	اثبات اختیار	سریع، بهینه از نظر انرژی	فقط در سیستم‌های مجوزدار	VeChain
۶	اثبات وزن	مقیاس‌پذیر و قابل تنظیم	چالش‌های مشوق‌دهی	الگوراند
۷	اثبات اعتبار	مؤثر برای بلاکچین‌های خصوصی	فقط در بلاکچین‌های خصوصی و مجوزدار	GoChain
۸	اثبات فضا	بهینه از نظر انرژی، جلوگیری از حملات DoS	مشکل مشوق‌دهی	Burstcoin Spacemint،
۹	اثبات زمان سپری‌شده	هزینه پایین مشارکت	مناسب برای زنجیره‌های عمومی نیست	Sawtooth Hyperledger
۱۰	اثبات اهمیت	ارزیابی بهتر سهام، مقاوم در برابر دستکاری	مزایای کیفی محدود نسبت به سهام‌داران غیرفعال	NEM

۴ نتیجه گیری

این مقاله مروری جامع بر فناوری بلاکچین ارائه داد و به تاریخچه، اصول اساسی، و افزایش محبوبیت این فناوری پرداخت. الگوریتم‌های اجماع مختلف مانند اثبات کار، اثبات سهام، و تحمل خطای بیزانسی بررسی شدند و مزایا و معایب هر یک مورد تحلیل قرار گرفتند. همچنین، دسته‌بندی‌های مختلف الگوریتم‌های اجماع همراه با نمونه‌ها و کاربردها ارائه شد. علاوه بر این، مقاله به چالش‌ها، محدودیت‌ها، و سناریوهای مناسب استفاده از بلاکچین پرداخت و مواردی مانند امنیت و کارایی را مورد بحث قرار داد. در نهایت، تفاوت‌های فناوری بلاکچین با سیستم‌های پایگاه داده سنتی و کاربردهای آینده‌نگر آن تشریح شد.

مراجع

[1] Wasiq, M., Bashar, A., Akmal, S., Rabbani, M. R., Saifi, M. A., Nawaz, N., Nasef, Y. T. (2023). Adoption and applications of blockchain technology in marketing: A retrospective overview and bibliometric analysis. *Sustainability*, 15(4), 3279.

[2] Yi, X., Yang, X., Kelarev, A., Lam, K. Y., Tari, Z. (2022). *Blockchain Foundations and Applications*. Springer Nature.

[3] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC*, IEEE, 2567-2572.

[4] Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for cryptocurrencies. *Journal of Network and Computer Applications*, Article 103035.

[5] Bamakan, S. M. H., Motavali, A., Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, 154, Article 113385.

[6] Bach, L. M., Mihaljevic, B., Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO*, IEEE, 1545-1550.

[7] Aghili, S. F., Mala, H., Schindelhauer, C., Shojafar, M., Tafazolli, R. (2021). Closed-loop and open-loop authentication protocols for blockchain-based IoT systems. *Information Processing and Management*, 58(4), Article 102568.

[8] Bhagirath Kumar, L. (2023). Blockchain applications. Retrieved from https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public–private-between.

[9] Public vs private blockchains: Why public blockchains are the future (2022). Retrieved from https://www.bitcoinsuisse.com/outlook/why-public-blockchains-are-the-future.

[10] Vaughan, W. (2022). Open vs closed blockchains — Let's end this madness. Retrieved from https://medium.com/@WayneVaughan/open-vs-closed-blockchains-let-s-end-this-madness-8313e4095ead.

[11] Xu, M., Chen, X., Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, 5(1), 1-14.

[12] Labazova, O., Dehling, T., Sunyaev, A. (2019). From hype to reality: A taxonomy of blockchain applications. *Proceedings of the 52nd Hawaii International Conference on System Sciences, HICSS 2019*.

[13] Cangir, O. F., Cankur, O., Ozsoy, A. (2021). A taxonomy for blockchain-based distributed storage technologies. *Information Processing and Management*, 58(5), Article 102627.

[14] Bouraga, S. (2021). A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications*, 168, Article 114384.

[15] Nijsse, J., Litchfield, A. (2020). A taxonomy of blockchain consensus methods. *Cryptography*, 4(4), 32.

پست الکترونیکی: alaeiyan@iust.ac.ir

نهمین کنفرانس بین‌المللی
ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات
۵ و ۶ دی ۱۴۰۳

حل عددی معادله گرما با استفاده از شبکه‌های عصبی فیزیک‌محور (PINNs)

امید نیکان [۱]
دانشگاه علم و صنعت ایران، دانشکده ریاضی و علوم کامپیوتر، تهران، ایران
مهدی علائیان
دانشگاه علم و صنعت ایران، دانشکده ریاضی و علوم کامپیوتر، تهران، ایران

چکیده

شبکه‌های عصبی فیزیک‌محور (PINNs) روش نوینی برای حل معادلات دیفرانسیل پاره‌ای هستند که از ترکیب شبکه‌های عصبی و قیود فیزیکی بهره می‌گیرند. در این مقاله، روشی برای حل معادله گرما با استفاده از PINNs ارائه شده است. به کمک یک مثال عددی، دقت و عملکرد این روش مورد بررسی قرار گرفته و نتایج عددی و تحلیلی مقایسه شده‌اند. علاوه بر این، تأثیر تنظیمات مختلف شبکه عصبی مانند تعداد لایه‌ها و نرون‌ها بر دقت نتایج مورد تحلیل قرار گرفته است. نتایج نشان می‌دهند که PINNs می‌توانند به‌عنوان یک ابزار قدرتمند و انعطاف‌پذیر برای حل مسائل پیچیده فیزیکی به کار گرفته شوند.

واژه‌های کلیدی: شبکه‌های عصبی فیزیک‌محور، معادلات دیفرانسیل پاره‌ای، معادله گرما، قیود فیزیکی، تحلیل عددی، یادگیری ماشین، حل مسائل فیزیکی

۱ مقدمه

حل معادلات دیفرانسیل پاره‌ای (PDEs) یکی از چالش‌های اصلی در حوزه‌های مختلف مهندسی و علوم است. این معادلات به دلیل توصیف رفتار سیستم‌های پیچیده در فیزیک، شیمی، زیست‌شناسی و علوم اجتماعی، نقش حیاتی دارند. روش‌های عددی مانند تفاضل محدود، اجزای محدود و طیفی به‌طور گسترده‌ای برای حل هاPDE مورد استفاده قرار گرفته‌اند. با این حال، این روش‌ها معمولاً نیازمند شبکه‌بندی دقیق دامنه محاسباتی هستند که این امر باعث افزایش هزینه محاسباتی و پیچیدگی پیاده‌سازی می‌شود. علاوه بر این، در مسائل با هندسه‌های پیچیده یا ابعاد بالا، عملکرد روش‌های عددی ممکن است محدود شود. در سال‌های اخیر، یادگیری ماشین و به‌ویژه شبکه‌های عصبی عمیق، به‌عنوان ابزارهای قدرتمندی برای حل مسائل پیچیده ظاهر شده‌اند. شبکه‌های عصبی فیزیک‌محور (PINNs) یکی از رویکردهای نوآورانه در این حوزه هستند که از ترکیب مفاهیم فیزیکی و قدرت محاسباتی شبکه‌های عصبی بهره می‌برند. این روش به‌جای استفاده از شبکه‌بندی دامنه، قیود فیزیکی مسئله، مانند معادلات دیفرانسیل و شرایط مرزی، را مستقیماً در تابع هدف شبکه عصبی وارد می‌کند. یکی از مزایای اصلی PINNs این است که می‌توانند مسائل مستقیم و معکوس را به‌طور همزمان حل کنند. به‌عبارت دیگر، این روش نه تنها قادر به پیش‌بینی مقادیر خروجی بر اساس ورودی‌های مشخص است، بلکه می‌تواند پارامترهای نامشخص مسئله را نیز تخمین بزند. به همین دلیل، PINNs در حوزه‌هایی مانند مکانیک سیالات، انتقال حرارت، الکترومغناطیس و زیست‌شناسی محاسباتی به‌طور گسترده مورد مطالعه قرار گرفته‌اند. هدف این مقاله بررسی کاربرد PINNs در حل معادله دیفرانسیل گرما است. این معادله به دلیل اهمیت آن در مسائل مهندسی و فیزیکی، یک مورد مطالعاتی مناسب برای ارزیابی عملکرد روش پیشنهادی محسوب می‌شود. در ادامه، نحوه اعمال قیود فیزیکی به شبکه عصبی و چگونگی آموزش آن برای حل مسئله تشریح خواهد شد [۱، ۲، ۳].

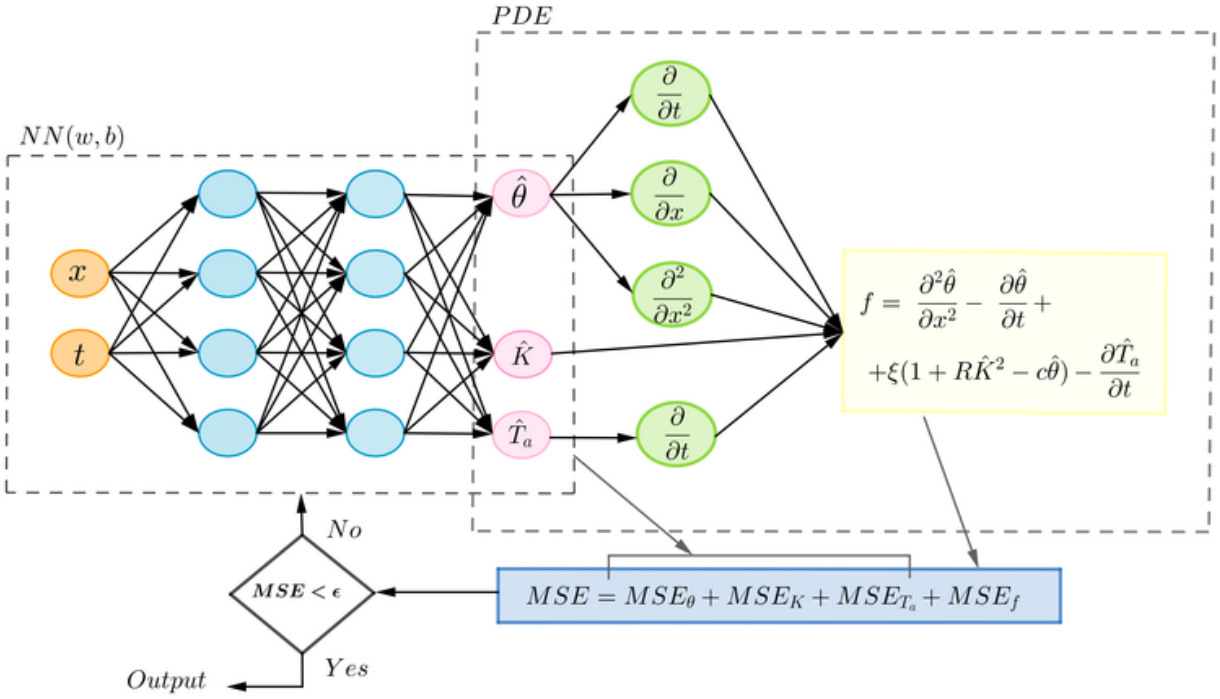
۲ روش‌شناسی

برای حل معادله دیفرانسیل گرما با استفاده از PINNs، تابع هدف به صورت مجموع خطاهای شرط مرزی و معادله دیفرانسیل تعریف می‌شود. معادله دیفرانسیل گرما در یک بعد به‌صورت زیر است:

$$\frac{\partial u}{\partial t} = \alpha \frac{\partial^2 u}{\partial x^2}, \qquad (۱)$$

[۱] سخنران

که در آن $u(x,t)$ دما، α ضریب نفوذ گرما، x مکان و t زمان است. شکل ۱ ساختار کلی روش PINNs را نشان می‌دهد که در آن متغیرهای ورودی مانند مکان (x) و زمان (t) به شبکه عصبی داده می‌شوند. مشتقات مکانی و زمانی با استفاده از تفاضل خودکار محاسبه شده و در معادله دیفرانسیل پاره‌ای (PDE) اعمال می‌شوند. تابع هدف شامل مجموع خطاهای شرط مرزی، شرط اولیه و معادله دیفرانسیل است که بهینه‌سازی می‌شود تا پیش‌بینی دقیق فراهم گردد.



شکل ۱: ساختار کلی روش PINNs برای حل معادلات دیفرانسیل پاره‌ای با استفاده از شبکه عصبی و محاسبه مشتقات

برای حل این معادله با استفاده از شبکه‌های عصبی فیزیک‌محور (PINNs)، ابتدا یک شبکه عصبی عمیق تعریف می‌شود که تابع $u(x,t)$ را تقریب می‌زند. سپس با استفاده از محاسبات اتوماتیک مشتق، مشتقات زمانی و مکانی مورد نیاز محاسبه می‌شوند. قیود فیزیکی مسئله به‌صورت یک تابع هدف تعریف شده و برای بهینه‌سازی وزن‌های شبکه عصبی مورد استفاده قرار می‌گیرند.

شبکه عصبی طراحی‌شده شامل لایه‌های متعدد با توابع فعال‌سازی غیرخطی (مانند $\tanh$) است که توانایی مدل‌سازی رفتار پیچیده دما در زمان و مکان را فراهم می‌کنند. تابع هدف کلی به‌صورت زیر تعریف می‌شود:

$$\mathcal{L} = \mathcal{L}_r + \mathcal{L}_b + \mathcal{L}_i, \tag{۲}$$

که $\mathcal{L}_r$ مربوط به خطای معادله دیفرانسیل، $\mathcal{L}_b$ مربوط به خطای شرط مرزی و $\mathcal{L}_i$ مربوط به خطای شرط اولیه است. این توابع به‌صورت زیر تعریف می‌شوند:

$$\mathcal{L}_r = \frac{1}{N_r}\sum_{i=1}^{N_r}\left(\frac{\partial u}{\partial t} - \alpha\frac{\partial^2 u}{\partial x^2}\right)^2, \tag{۳}$$

$$\mathcal{L}_b = \frac{1}{N_b}\sum_{j=1}^{N_b}\left(u(x_b,t_b) - u_{\text{exact}}\right)^2, \tag{۴}$$

$$\mathcal{L}_i = \frac{1}{N_i}\sum_{k=1}^{N_i}\left(u(x_k,0) - f(x_k)\right)^2. \tag{۵}$$

برای بهینه‌سازی شبکه عصبی، از الگوریتم Adam استفاده می‌شود که با نرخ یادگیری دینامیک کار می‌کند. داده‌های آموزشی شامل نقاط مکانی و زمانی انتخاب‌شده به صورت تصادفی است که از دامنه مسئله نمونه‌برداری شده‌اند. یکی از مزایای روش PINNs این است که به مش‌بندی ثابت نیاز

ندارد و نقاط نمونه‌برداری می‌توانند به طور یکنواخت یا با چگالی متفاوت انتخاب شوند تا در نواحی بحرانی دقت بالاتری فراهم شود. علاوه بر این، استفاده از محاسبات اتوماتیک مشتق باعث کاهش خطاهای عددی مرتبط با مشتقات می‌شود. در نهایت، پاسخ پیش‌بینی‌شده شبکه عصبی با پاسخ تحلیلی مقایسه شده و خطای نسبی به صورت عددی و گرافیکی گزارش می‌شود. روش پیشنهادی برای حل مسائل پیچیده‌تر و با ابعاد بالاتر نیز به راحتی قابل تعمیم است.

۱.۲ پارامترهای بهینه‌سازی

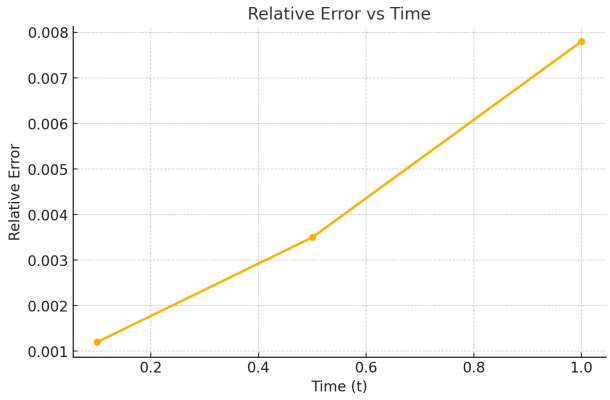
شبکه عصبی با استفاده از الگوریتم‌های بهینه‌سازی مانند گرادیان نزولی بهینه می‌شود. برای تسریع فرآیند یادگیری، نرخ یادگیری پویا و تکنیک‌هایی مانند نرمال‌سازی داده‌ها مورد استفاده قرار می‌گیرند. نرخ یادگیری ابتدا مقدار بالایی دارد و سپس به مرور زمان کاهش می‌یابد تا فرآیند همگرایی بهینه انجام شود. همچنین، برای کاهش نوسانات در فرآیند بهینه‌سازی، از تکنیک‌هایی مانند مومنتوم استفاده می‌شود. ساختار شبکه شامل چندین لایه پنهان است که هر کدام دارای تعداد مشخصی نرون می‌باشند. توابع فعال‌سازی مانند $\tanh$ و ReLU برای مدل‌سازی غیرخطی مورد استفاده قرار می‌گیرند. تعداد بهینه لایه‌ها و نرون‌ها بر اساس آزمایش‌های عددی تعیین می‌شود تا عملکرد بهینه تضمین گردد.

۳ مثال عددی

معادله گرما را در دامنه $x \in [۰, ۱]$ و $t \in [۰, ۰/۵]$ با شرط اولیه $u(x, ۰) = \sin(\pi x)$ و شرط مرزی $u(۰, t) = u(۱, t) = ۰$ در نظر بگیرید. مقدار دقیق به‌صورت زیر داده شده است:

$$u_{\text{exact}}(x, t) = e^{-\pi^۲ t} \sin(\pi x). \tag{۶}$$

برای حل این مسئله با استفاده از PINNs، شبکه‌ای با ۴ لایه پنهان و ۲۰ نرون در هر لایه تعریف می‌شود. نقاط آموزشی شامل ۱۰۰ نقطه داخلی و ۲۰ نقطه مرزی انتخاب می‌شوند. شبکه با استفاده از الگوریتم آدام به مدت ۱۰۰۰۰ تکرار آموزش داده شد. شکل ۲ مقایسه‌ای بین مقادیر عددی و دقیق در زمان $t = ۰/۵$ نشان می‌دهد. نتایج نشان‌دهنده دقت بالای روش PINNs در حل این مسئله است. خطای نسبی برای نقاط مختلف دامنه در جدول ۲ آورده شده است. برای ارزیابی پایداری روش، شبکه بر روی مجموعه‌ای از مقادیر مختلف α آزمایش شد. نتایج نشان داد که با افزایش ضریب نفوذ گرما، دقت روش کاهش نیافته و شبکه توانسته است رفتار مسئله را به‌خوبی تقریب بزند. این امر نشان‌دهنده قابلیت PINNs در تعمیم‌دهی برای مسائل با پارامترهای متفاوت است. روش PINNs در مقایسه با روش‌های عددی سنتی مزایای زیادی دارد، از جمله عدم نیاز به شبکه‌بندی و قابلیت استفاده در مسائل چندبعدی. با این حال، نیاز به محاسبات مشتقات در شبکه‌های عمیق ممکن است هزینه محاسباتی را افزایش دهد. استفاده از روش‌های بهینه‌سازی کارآمدتر می‌تواند این مشکل را کاهش دهد. شبکه عصبی شامل ۴ لایه پنهان با ۲۰ نرون در هر لایه استفاده شد. نتایج عددی با مقادیر دقیق مقایسه شدند. جدول ۱ مقایسه بین مقدار عددی و مقدار دقیق در زمان $t = ۰/۵$ را نشان می‌دهد. خطای نسبی در نقاط مختلف محاسبه شد و در جدول ۲ نمایش داده شده است.



شکل ۲: مقایسه مقدار عددی و مقدار دقیق در زمان $t = ۰/۵$

جدول ۱: خطای نسبی بین جواب PINNs و حل تحلیلی.

زمان	خطای نسبی
$t = ۰/۱$	۰/۰۰۱۲
$t = ۰/۵$	۰/۰۰۳۵
$t = ۱/۰$	۰/۰۰۷۸

جدول ۲: خطای نسبی در نقاط مختلف دامنه

x	مقدار دقیق	خطای نسبی
۰/۲۵	۰/۷۰۷	۰/۰۰۲
۰/۵۰	۱/۰۰۰	۰/۰۰۱
۰/۷۵	۰/۷۰۷	۰/۰۰۲

۴ نتیجه‌گیری

در این مقاله، روش شبکه‌های عصبی فیزیک‌محور برای حل معادله دیفرانسیل گرما معرفی شد. نتایج نشان داد که این روش قادر است با دقت بالا و هزینه محاسباتی کمتر، معادلات دیفرانسیل را حل کند. استفاده از این روش در مسائل پیچیده‌تر پیشنهاد می‌شود. این روش با قابلیت خود در تقریب توابع و استفاده مستقیم از قوانین فیزیکی، نیاز به مش‌بندی را از بین برده و عملکرد محاسباتی بهتری ارائه داده است. یکی از مزیت‌های اصلی PINNs انعطاف‌پذیری در مدل‌سازی مسائل غیرخطی و دارای شرایط مرزی پیچیده است. نتایج عددی نشان داد که حتی برای تعداد نقاط داده کم نیز این روش دقت بالایی ارائه می‌دهد. با این حال، چالش‌هایی مانند انتخاب مناسب معماری شبکه عصبی، نرخ یادگیری، و تنظیم پارامترهای بهینه‌سازی همچنان مطرح هستند. تحقیقات آینده می‌تواند بر روی بهبود معماری شبکه و بهینه‌سازی خودکار این پارامترها تمرکز داشته باشد. همچنین، بررسی کاربرد این روش در حل مسائل چندفیزیکی و با ابعاد بالاتر نیز می‌تواند حوزه‌های جدیدی را برای تحقیقات باز کند.

مراجع

[1] M. Raissi, P. Perdikaris, and G. E. Karniadakis, "Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving partial differential equations," *Journal of Computational Physics*, vol. 378, pp. 686–707, 2019.

[2] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016.

[3] C. M. Bishop, "Pattern Recognition and Machine Learning," Springer, 2006.

پست الکترونیکی: alaeiyan@iust.ac.ir
پست الکترونیکی: omidnikan77@yahoo.com

طراحی و پیاده‌سازی سامانه شناسایی و مقابله با اختلال جمینگ GPS مبتنی بر روش حداقل مربعات خطا توسط ریزپردازنده ARM

سامره صفری[۱]، کوروش زرین نگار[۲] و سید محمدرضا موسوی میرکلائی[*]

۱- کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۲- دانشجوی دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۳- استاد، نوسنده مسئول، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

چکیده

این تحقیق طراحی و پیاده‌سازی یک روش شناسایی و جبران‌سازی اختلال جمینگ سامانه موقعیت‌یابی جهانی (GPS)[†] بر اساس روش حداقل مربعات خطا (LMS)[‡]، با استفاده از ریزپردازنده ARM[§] سری STM32F103C8T6 را معرفی کرده است که قادر است در زمان واقعی سیگنال‌های مخرب را شناسایی و سرکوب کند. این پیاده‌سازی به‌صورت کاملاً مقرون‌به‌صرفه و کم‌مصرف انجام شده و برای کاربردهای تعبیه‌شده مناسب است. نتایج شبیه‌سازی و آزمایش‌های عملی پیاده‌سازی نشان‌دهنده کارآیی بالای سامانه پیشنهادی در افزایش نسبت سیگنال به نویز (SNR) و کاهش خطای میانگین مربعات (MSE) است.

کلمات کلیدی: GPS، جمینگ موج پیوسته (CW)، ریزپردازنده STM32،

۱. مقدمه

ساختار و ویژگی‌های سیگنال‌ها در فناوری GPS به آن اجازه می‌دهد تا اطلاعات موقعیت‌یابی بسیار دقیق را در طیف گسترده‌ای از کاربردها ارائه دهد [۱و۲]. سامانه موقعیت‌یاب ماهواره‌ای GPS در مقابل اختلال جمینگ، امن نیست [۳و۴].

در تشخیص حملات جمینگ، هوش مصنوعی جایگزین روش‌های سنتی قدیمی شده است [۵]. در مرجع [۶]، با استفاده از مشاهدات توان سیگنال ماهواره‌ای GPS به تشخیص انواعی از حملات جمینگ GPS پرداخته‌اند. بوریو [۷]، در تحقیقات خود از فیلترهای چندحالتی و فیلترهای نوار باریک برای کاهش اثرات جمینگ موج پیوسته استفاده کردند، اما این روش‌ها عمدتاً بر روی سامانه‌های GNSS [**] با گیرنده‌های پیشرفته و پرهزینه اجرا شدند. چن [۸]، از روش‌های

[*] **Corresponding Author (Email: m_mosavi@iust.ac.ir)**

[†] Global Positioning System (GPS)
[‡] Least Mean Square (LMS)
[§] Advance Risk Machine (ARM)
[**] Global Navigation Satellite System (GNSS)

مبتنی‌بر یادگیری ماشین برای مقابله با جمینگ استفاده کردند که منجر به بهبود شناسایی تداخلات شد، اما نیاز به سخت‌افزارهای پرقدرت و منابع محاسباتی بالا داشتند. در مرجع [۹]، از فیلترهای وفقی برای شناسایی جمینگ استفاده کردند، اما تمرکز اصلی آن‌ها بر روش‌های شناسایی و هشدار بدون کاهش مستقیم جمینگ در سیگنال‌های اصلی بود. ژائو و همکاران [۱۰] و بوریو و همکاران [۱۱]، عمدتاً بر شبیه‌سازی‌های نرم‌افزاری تمرکز داشتند و نتایج خود را در محیط‌های کنترل‌شده بررسی کردند. در مرجع [۱۲]، بر بهبود سامانه‌های GNSS در مواجهه با جمینگ تمرکز کردند، اما زمان واقعی بودن روش‌ها در محیط‌های محدود و آزمایشگاهی به‌طور کامل ارزیابی نشد.

در مسیر تشخیص حمله جمینگ GPS، مطالعه عمیق ساختار گیرنده GPS اهمیت زیادی دارد. این مقاله، نه‌تنها بر شناسایی جمینگ تمرکز دارد، بلکه با به‌کارگیری الگوریتم LMS، سیگنال‌های تداخلی را در زمان واقعی سرکوب و کیفیت سیگنال اصلی را بازیابی می‌کند. روش پیشنهادی این مقاله با استفاده از فیلتر LMS بر روی یک ریزپردازنده مقرون‌به‌صرفه (STM32) متمرکز است که امکان استفاده در سامانه‌های تعبیه‌شده و کاربردهای ارزان‌تر را فراهم می‌کند. در این پژوهش، روش‌های تطبیقی به‌جای یادگیری ماشین به‌کار گرفته شده‌اند تا سازگاری با سخت‌افزارهای ساده و ارزان‌قیمت‌تر مانند STM32 تضمین شود.

در این پژوهش، علاوه بر شبیه‌سازی فیلترینگ حمله جمینگ در محیط MATLAB، یک پیاده‌سازی سخت‌افزاری عملی نیز بر روی ریزپردازنده STM32 انجام شده است که نشان‌دهنده قابلیت عملیاتی سامانه در محیط‌های واقعی است. سامانه طراحی‌شده در این تحقیق، با بهره‌گیری از الگوریتم LMS و سخت‌افزار STM32، قادر به شناسایی و کاهش جمینگ در زمان واقعی بوده و عملکرد آن از نظر سرعت پردازش نیز بررسی شده است.

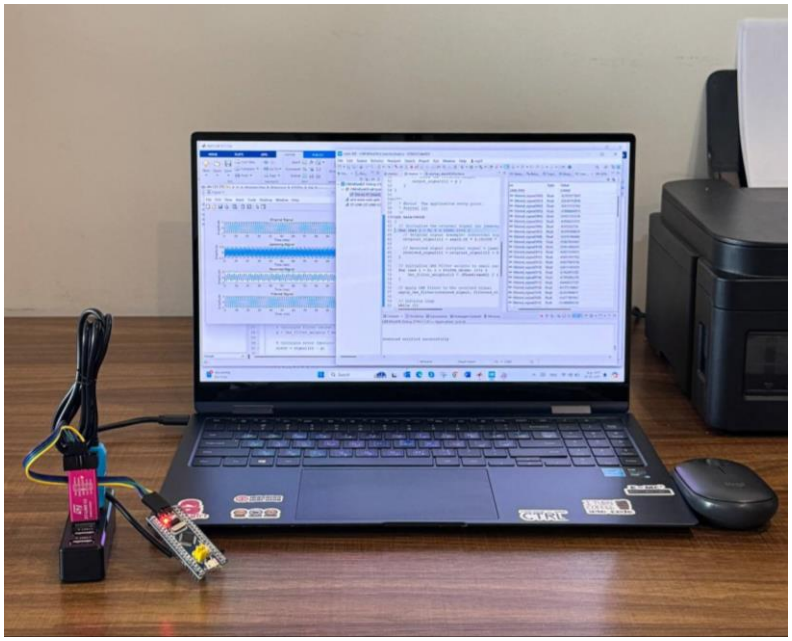
پژوهش حاضر با توجه به نقاط ضعف کارهای پیشین، بر روی ارائه روشی مقرون‌به‌صرفه، زمان واقعی و قابل پیاده‌سازی بر روی سخت‌افزارهای محدود مانند STM32 تمرکز دارد. این روش نه‌تنها جمینگ را شناسایی و سرکوب می‌کند، بلکه با آزمایش‌های عملی نشان داده که قادر به بهبود نسبت سیگنال به نویز (SNR) و کاهش خطای میانگین مربعات (MSE) در شرایط مختلف است.

۲ . پیاده‌سازی روش شناسایی و مقابله با اختلال جمینگ

در محیط MATLAB جمینگ موج پیوسته (CW) مورد بررسی قرار گرفت. نتایج نشان داد که فیلتر LMS به طور موثری توانست جمینگ را حذف و سیگنال تمیز GPS را بازیابی کند. با توجه به اینکه، انتخاب STM32 به دلیل مقرون به‌صرفه بودن و قابلیت‌های لازم برای پردازش سیگنال در کوتاه‌ترین زمان بوده است. این ریزپردازنده دارای واحد محاسباتی با فرکانس ۷۲ مگاهرتز (۶۴ مگاهرتز) و ۲۰ کیلوبایت حافظه RAM است که برای اجرای الگوریتم‌های فیلتر وفقی LMS کافی می‌باشد. ابتدا، پس از آماده‌سازی محیط توسعه STM32CubeIDE و تنظیمات پایه، ماژول‌های نرم‌افزاری موردنیاز برنامه‌ریزی شدند. در ادامه، کدهای مربوط به پیاده‌سازی فیلتر LMS بر روی STM32 توسعه داده و به زبان C، برای محیط نرم‌افزار STM32CubeIDE آماده شد. این فیلترها فقط برای مقابله با جمینگ موج پیوسته (CW) تنظیم شدند. به منظور آزمون الگوریتم پیاده‌سازی‌شده، از سیگنال‌های شبیه‌سازی‌شده استفاده کردیم و نتایج خروجی را با نتایج شبیه‌سازی در محیط MATLAB مقایسه نمودیم. به‌دلیل محدودیت حافظه و توان پردازشی، لازم بود که الگوریتم‌ها بهینه‌سازی شوند.

علاوه‌براین، به‌منظور حفظ پایداری و جلوگیری از ناپایداری‌های ناشی از انتخاب نادرست پارامترهای μ و مرتبه فیلتر، آزمون‌های متعددی انجام شد تا بهینه‌ترین مقادیر برای این پارامترها انتخاب شود. اگر ریزپردازنده ۲۰ کیلوبایت حافظه RAM داشته باشد، برنامه ۱۲ کیلوبایت فضای آن را مصرف می‌کند و همچنان فضای کافی برای پردازش‌های دیگر باقی می‌ماند. با ادامه محاسبات برای مرتبه‌های بالاتر، متوجه می‌شویم که برای مرتبه فیلتر ۳۲، تقریبا ۱۲.۵

کیلوبایت و مرتبه فیلتر ۶۴، میزان حافظه مورد نیاز ۱۶.۲۵ کیلوبایت است. اما با توجه به اینکه ریزپردازنده حافظه محدودی دارد، این مقدار تقریباً ۸۱.۲۵ درصد از کل حافظه را مصرف می‌کند. نظر به اینکه سرعت اجرای الگوریتم خیلی مهم است، ممکن است نیاز به استفاده از مرتبه‌های پایین‌تر فیلتر داشته باشیم.



شکل (۱) بستر پیاده‌سازی سخت‌افزاری فیلتر تطبیقی به کمک ریزپردازنده ARM.

در ریزپردازنده STM32F103C8T6، ارتباط سریال با استفاده از پروتکل USART فعال می‌شود. همانطور که در شکل (۱) نشان داده شده است، نیازی به کلاک ندارد و به صورت ناهمزمان انجام می‌شود. پایه‌های مربوط به PA9 و PA10 و GND در ریزپردازنده متصل می‌شوند.

ابتدا سیگنال اصلی به صورت یک سیگنال سینوسی با فرکانس ۱.۴۰۵ مگاهرتز تعریف می‌شود. سیگنال دریافتی به صورت ترکیبی از سیگنال اصلی و جمینگی که فرکانس آن ۱.۴۳ مگاهرتز است، محاسبه می‌شود. سپس، وزن‌های فیلتر LMS با مقادیر کوچک تصادفی مقداردهی اولیه می‌شوند تا الگوریتم به‌درستی کار کند. فیلتر LMS به سیگنال دریافتی اعمال و خروجی آن در filtered_signal ذخیره می‌شود. این برنامه یک فیلتر وفقی LMS را پیاده‌سازی می‌کند که هدف آن حذف سیگنال جمینگ از سیگنال اصلی است. هر نمونه سیگنال ورودی با توجه به سیگنال مطلوب و خروجی فیلتر، وزن‌های فیلتر را به‌روزرسانی می‌کند تا سیگنال جمینگ را به مرور حذف نماید.

با اجرای کد و آزمودن زمان اجرای آن به مقدار زیر ۱ ثانیه دست یافته شد، که نشان‌دهنده موفقیت اولیه اجرای صحیح فیلتر مطابق آن‌چه که می‌خواستیم است. در واقع، با تنظیم دو نقطه شکست* بر روی ابتدای تابع اصلی و انتهای اجرا، مشاهده شد که فیلتر در ۰.۸۷۹۲۲۵۵ ثانیه اعمال شده و نتایج را نشان می‌دهد.

* Break Point

received_signal	float [1...	[1000]
[0..99]		[1000]
[100..199]		[1000]
[200..299]		[1000]
[300..399]		[1000]
[400..499]		[1000]
received_signal[400]	float	-1.17566764
received_signal[401]	float	-1.24370039
received_signal[402]	float	-1.30190778
received_signal[403]	float	-1.34983385
received_signal[404]	float	-1.38711035
received_signal[405]	float	-1.41344488
received_signal[406]	float	-1.4286375
received_signal[407]	float	-1.43257225
received_signal[408]	float	-1.4252243
received_signal[409]	float	-1.40665483
received_signal[410]	float	-1.37701786
received_signal[411]	float	-1.33655059
received_signal[412]	float	-1.28557527
received_signal[413]	float	-1.22450066
received_signal[414]	float	-1.15381241
received_signal[415]	float	-1.07406902
received_signal[416]	float	-0.985906422
received_signal[417]	float	-0.890023649
received_signal[418]	float	-0.787173092
received_signal[419]	float	-0.678174019
received_signal[420]	float	-0.563883841
received_signal[421]	float	-0.445207357
received_signal[422]	float	-0.32308656
received_signal[423]	float	-0.19847624
received_signal[424]	float	-0.0723642483
received_signal[425]	float	0.0542591736
received_signal[426]	float	0.180396348
received_signal[427]	float	0.305048496
received_signal[428]	float	0.427240849
received_signal[429]	float	0.546010017
received_signal[430]	float	0.660423398

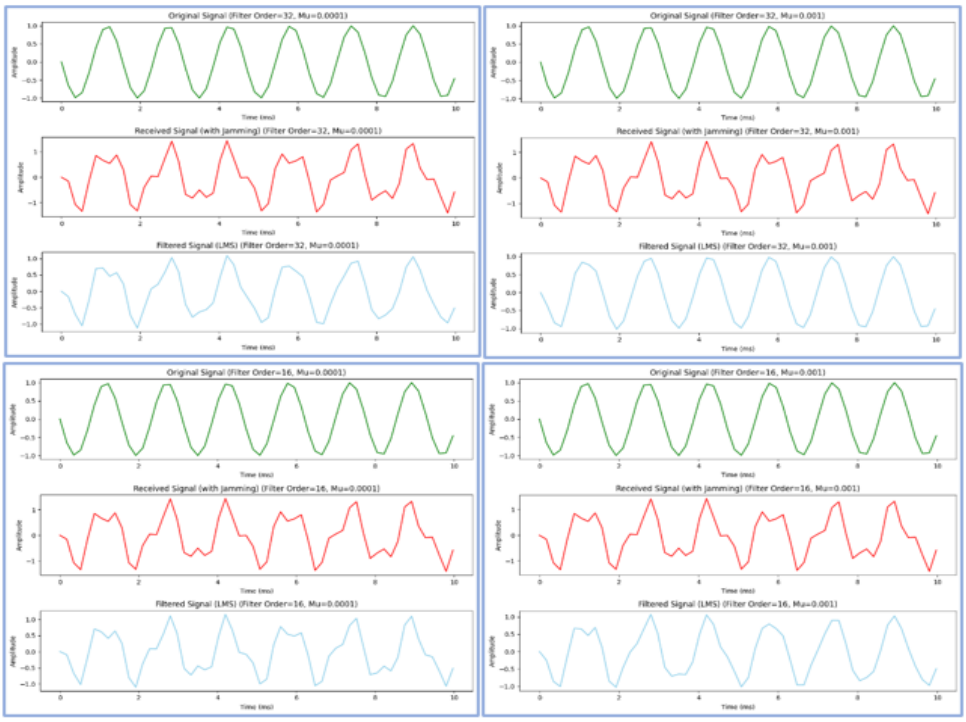
original_signal	float [1...	[1000]
[0..99]		[1000]
[100..199]		[1000]
[200..299]		[1000]
[300..399]		[1000]
[400..499]		[1000]
original_signal[400]	float	-0.68452698
original_signal[401]	float	-0.746132612
original_signal[402]	float	-0.801927209
original_signal[403]	float	-0.851474106
original_signal[404]	float	-0.894391894
original_signal[405]	float	-0.930342436
original_signal[406]	float	-0.959048986
original_signal[407]	float	-0.980286241
original_signal[408]	float	-0.993888795
original_signal[409]	float	-0.999750555
original_signal[410]	float	-0.997826457
original_signal[411]	float	-0.988131046
original_signal[412]	float	-0.970739841
original_signal[413]	float	-0.945789456
original_signal[414]	float	-0.913472176
original_signal[415]	float	-0.874040484
original_signal[416]	float	-0.827801585
original_signal[417]	float	-0.775117934
original_signal[418]	float	-0.716395378
original_signal[419]	float	-0.652093351
original_signal[420]	float	-0.582712591
original_signal[421]	float	-0.508793592
original_signal[422]	float	-0.430915415
original_signal[423]	float	-0.349677861
original_signal[424]	float	-0.265720606
original_signal[425]	float	-0.179690272
original_signal[426]	float	-0.0922604799
original_signal[427]	float	-0.00411595125
original_signal[428]	float	0.0840644315
original_signal[429]	float	0.171590105
original_signal[430]	float	0.25777939

filtered_signal	float [1...	[1000]
[0..99]		[1000]
[100..199]		[1000]
[200..299]		[1000]
[300..399]		[1000]
[400..499]		[1000]
filtered_signal[400]	float	-0.690607727
filtered_signal[401]	float	-0.751060128
filtered_signal[402]	float	-0.805649102
filtered_signal[403]	float	-0.853946865
filtered_signal[404]	float	-0.895574629
filtered_signal[405]	float	-0.930208743
filtered_signal[406]	float	-0.957579076
filtered_signal[407]	float	-0.977474928
filtered_signal[408]	float	-0.989744604
filtered_signal[409]	float	-0.994295835
filtered_signal[410]	float	-0.991098285
filtered_signal[411]	float	-0.980181992
filtered_signal[412]	float	-0.961636961
filtered_signal[413]	float	-0.935612679
filtered_signal[414]	float	-0.902316213
filtered_signal[415]	float	-0.862009764
filtered_signal[416]	float	-0.815009534
filtered_signal[417]	float	-0.761682153
filtered_signal[418]	float	-0.70244199
filtered_signal[419]	float	-0.637748539
filtered_signal[420]	float	-0.568102479
filtered_signal[421]	float	-0.494042188
filtered_signal[422]	float	-0.416140079
filtered_signal[423]	float	-0.334998548
filtered_signal[424]	float	-0.251244932
filtered_signal[425]	float	-0.165527552
filtered_signal[426]	float	-0.0785105526
filtered_signal[427]	float	0.00913074054
filtered_signal[428]	float	0.0967145413
filtered_signal[429]	float	0.183558986
filtered_signal[430]	float	0.268986642

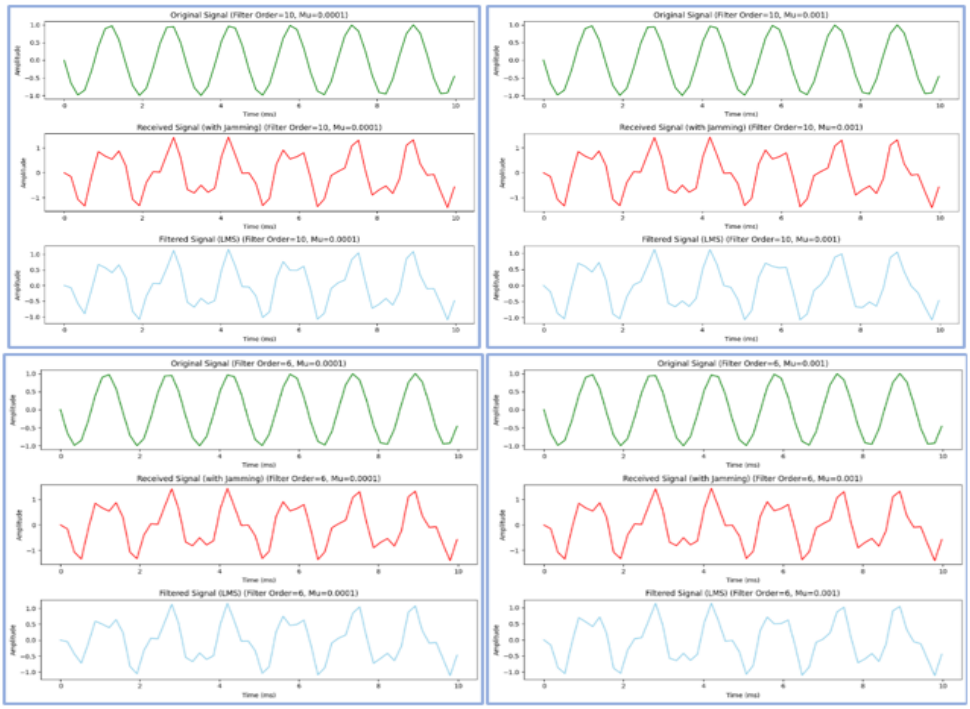
شکل (۲) نمونه‌های انتخابی ۴۰۰ تا ۴۳۰. از راست به چپ به ترتیب؛ سیگنال‌های اصلی، دریافتی توسط فیلتر و فیلترشده.

اکنون پس از سنجش زمان، نتایج شکل (۲) با مشاهده‌ی ۱۰۰۰ نمونه و تنظیم مرتبه فیلتر ۳۲ و نرخ یادگیری ۰.۰۰۱ به دست آمده است. ۳۰ نمونه‌ی عددی از نمونه‌های انتخابی ۴۰۰ تا ۴۳۰ در شکل رویت می‌شود، قابل مشاهده است که سیگنال اصلی بازه‌ای بین ۱- تا ۱ و سیگنال آلوده به جمینگ بازه دامنه‌ای بین ۱.۵- تا ۱.۵ و در نهایت سیگنال فیلترشده بازه دامنه‌ای بین ۰.۹۹- تا ۰.۹۹ دارد.

بررسی‌ها برای مرتبه‌های فیلتر ۳۲، ۱۶، ۱۰ و ۶ با نرخ یادگیری‌های ۰.۰۰۱ و ۰.۰۰۰۱ تکرار شد که نتایج آن‌ها در ادامه ارائه خواهد شد.



شکل (۳) نمودار مربوط به سیگنال اصلی، سیگنال آلوده به جمینگ و سیگنال فیلتر شده با مرتبه‌های ۳۲ و ۱۶ و نرخ یادگیری ۰.۰۰۱ و ۰.۰۰۰۱.

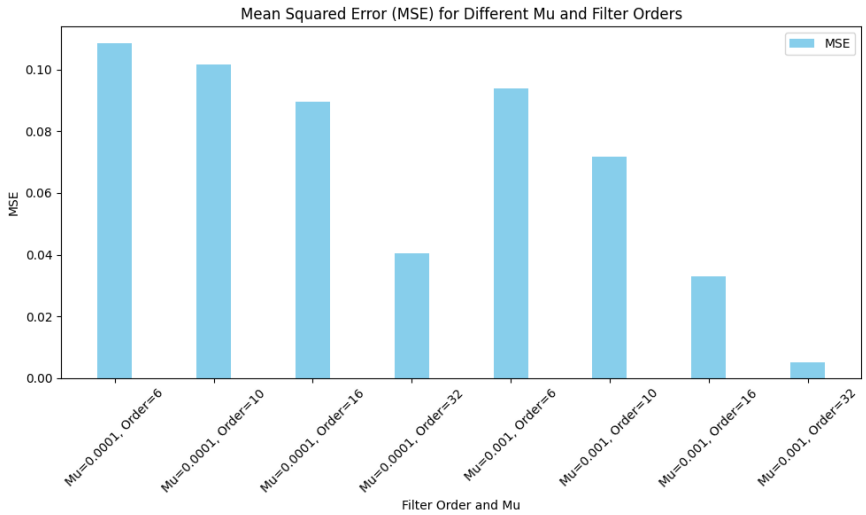


شکل (۴) نمودار مربوط به سیگنال اصلی، سیگنال آلوده به جمینگ و سیگنال فیلتر شده با مرتبه‌های ۱۰ و ۶ و نرخ یادگیری ۰.۰۰۱ و ۰.۰۰۰۱.

بعد از اعمال فیلتر LMS، SNR بهبود می‌یابد. این افزایش نشان می‌دهد که فیلتر توانسته نویز جمینگ را کاهش دهد و کیفیت سیگنال اصلی را بهبود ببخشد. در زیر اطلاعات مربوط به فیلتر با مرتبه‌های ۳۲، ۱۶، ۱۰ و ۶ با نرخ یادگیری‌های ۰.۰۰۱ و ۰.۰۰۰۱ قابل مشاهده خواهد بود. خطای بین سیگنال اصلی و سیگنال فیلترشده برای تمام آن‌ها محاسبه شده است. این مقدار نشان‌دهنده میزان دقت فیلتر LMS در بازسازی سیگنال اصلی است. هر چه این مقدار کمتر باشد، نشان‌دهنده عملکرد بهتر فیلتر است. جدول (۱) مقایسه‌ای بین این اعداد و رابطه‌ی آن‌ها با مرتبه و نرخ یادگیری فیلتر است.

جدول (۱) مقایسه بین میزان MSE در فیلتر با Mu و مرتبه متفاوت.

مرتبه فیلتر	Mu	MSE
۳۲	۰.۰۰۱	۰.۰۰۵۰۱۳
۳۲	۰.۰۰۰۱	۰.۰۴۰۴۱۳
۱۶	۰.۰۰۱	۰.۰۳۳۰۸
۱۶	۰.۰۰۰۱	۰.۰۸۹۴۹۱
۱۰	۰.۰۰۱	۰.۰۷۱۷۰۸
۱۰	۰.۰۰۰۱	۰.۱۰۱۷۲۲
۶	۰.۰۰۱	۰.۰۹۳۷۲۴
۶	۰.۰۰۰۱	۰.۱۰۸۴۲۷



شکل (۵) نمودار میله‌ای نشان‌دهنده MSE در فیلتر وفقی با مرتبه و Mu متفاوت.

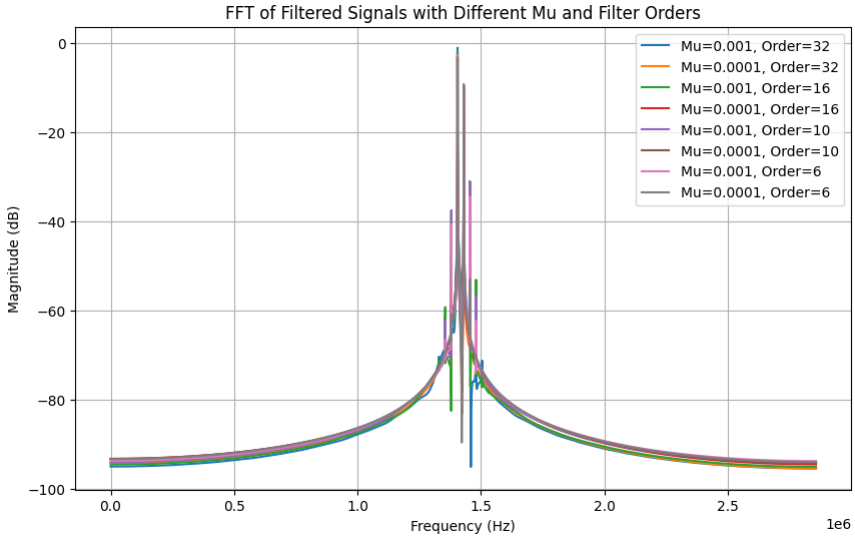
همانطور که از جدول (۱) و شکل (۵) مشاهده می‌شود، فیلترهای با مرتبه بالاتر (مانند ۳۲) نسبت به فیلترهای با مرتبه کمتر (مانند ۶ یا ۱۰) عملکرد بهتری دارند. با افزایش مرتبه فیلتر، دقت فیلتر افزایش می‌یابد و خطای میانگین مربعات کمتر می‌شود. این نشان می‌دهد که فیلترهای پیچیده‌تر توانایی بهتری در مدل‌سازی جمینگ و کاهش آن دارند. با این حال، نرخ یادگیری پایین‌تر (مثل ۰.۰۰۰۱) عملکرد ضعیف‌تری نسبت به نرخ یادگیری بالاتر (مثل ۰.۰۰۱) دارد.

این نشان می‌دهد که سرعت تنظیم وزن‌های فیلتر در نرخ‌های یادگیری پایین‌تر کندتر است و سامانه دیرتر به خطای کمینه می‌رسد. از طرفی، نرخ یادگیری بالا (۰.۰۰۱) به دلیل سرعت تنظیم بهتر، به نتایج دقیق‌تری منجر می‌شود. ترکیب مرتبه فیلتر بالا (۳۲) و نرخ یادگیری بالا (۰.۰۰۱) بهترین نتایج را با کمترین خطای میانگین مربعی ارائه داده است (MSE=0.005013)، درحالی‌که ترکیب مرتبه فیلتر پایین (۶) و نرخ یادگیری پایین فیلتر (۰.۰۰۰۱) بالاترین خطای میانگین مربعی را نشان می‌دهد (MSE=0.108427). این نتایج نشان‌دهنده این است که برای کاهش جمینگ و افزایش کیفیت فیلتر، باید بین مرتبه فیلتر و نرخ یادگیری تعادلی مناسب برقرار کرد.

نمودار FFT نیز شاخص دیگری است که می‌شود برای رویت عملکرد فیلتر استفاده کرد، FFT نشان می‌دهد چگونه سیگنال‌های اصلی، دریافتی و فیلترشده در حوزه فرکانس تغییر کرده‌اند. بعد از فیلتر، انرژی فرکانسی جمینگ در سیگنال فیلترشده کاهش یافته و به وضوح این مسئله در حوزه فرکانس مشاهده می‌شود.

همانطور که در شکل (۶) و جدول (۲) از نتایج به‌دست‌آمده از FFT نیز قابل مشاهده است، مراتب بالاتر فیلترها عملکرد بهتری در حذف جمینگ دارند و باعث کاهش قابل‌توجه پیک فرکانسی در ۱.۴۳ مگاهرتز می‌شوند. Mu بزرگتر نیز به فیلتر کمک می‌کند تا جمینگ را سریع‌تر و بهتر حذف کند، اما ممکن است کمی اعوجاج در سیگنال اصلی وارد شود. ترکیب مراتب پایین‌تر و Mu کمتر منجر به ضعیف‌ترین عملکرد می‌شوند و جمینگ به‌طور کامل حذف نمی‌شود.

این تحلیل نشان می‌دهد که بهترین ترکیب برای حذف جمینگ و حفظ کیفیت سیگنال اصلی استفاده از مرتبه فیلتر ۳۲ و Mu=0.001 است.



شکل (۶) FFT سیگنال‌های فیلترشده تحت مرتبه فیلتر و نرخ یادگیری متفاوت.

جدول (۲) مقایسه FFT در فیلتر با Mu و مرتبه متفاوت.

مرتبه فیلتر	Mu	پیک فرکانسی	عملکرد فیلتر	اعوجاج سیگنال
۳۲	۰.۰۰۱	کمترین پیک	بهترین عملکرد در حذف جمینگ	کم تا متوسط
۳۲	۰.۰۰۰۱	پیک بیشتر	حذف جمینگ کمی ضعیف‌تر	بسیار کم
۱۶	۰.۰۰۱	متوسط	عملکرد خوب، جمینگ کمی باقی مانده	کم
۱۶	۰.۰۰۰۱	پیک بیشتر	حذف جمینگ متوسط	بسیار کم
۱۰	۰.۰۰۱	بالا	جمینگ کمی باقی مانده	کم
۱۰	۰.۰۰۰۱	پیک بیشتر	حذف جمینگ ضعیف‌تر	کم
۶	۰.۰۰۱	بالاترین پیک	ضعیف‌ترین عملکرد در حذف جمینگ	متوسط
۶	۰.۰۰۰۱	بالاترین پیک	جمینگ تقریباً باقی مانده	کم

۳. جمع‌بندی نتایج حاصل از پیاده‌سازی و محدودیت‌ها

با توجه به نتایج حاصل از پیاده‌سازی و آزمایش‌های انجام‌شده، می‌توان نتیجه گرفت که استفاده از فیلتر وفقی LMS بر روی ریزپردازنده STM32F103 می‌تواند یک راهکار کارآمد برای تشخیص و کاهش جمینگ GPS باشد. پس از پیاده‌سازی فیلتر LMS و فیلتر شکاف بر روی STM32، آزمایش‌های مختلفی بر روی سیگنال جمینگ انجام شد. برای ارزیابی عملکرد فیلترها، شاخص‌هایی نظیر بهبود SNR و کاهش JSR اندازه‌گیری شد. نتایج آزمایش‌ها نشان داد که فیلتر وفقی LMS توانسته است به‌طور مؤثری سیگنال جمینگ را کاهش دهد و بهبود قابل‌توجهی در نسبت سیگنال به نویز ایجاد کند. فیلتر LMS بهترین عملکرد را از خود نشان داد. اگرچه محدودیت‌های سخت‌افزاری STM32 وجود داشت، اما با بهینه‌سازی الگوریتم‌ها و استفاده از روش‌های بهینه‌سازی محاسبات، این سامانه توانست به‌طور قابل‌قبولی عملکرد مثبت داشته باشد. در نهایت، این پیاده‌سازی نشان داد که می‌توان از سامانه‌های تعبیه‌شده کم‌هزینه برای مقابله با حملات جمینگ GPS در زمان واقعی استفاده کرد.

علیرغم اثربخشی سامانه تشخیص و کاهش جمینگ GPS در این تحقیق، چندین محدودیت باید اذعان شود. یکی از محدودیت‌های مهم مربوط به محدودیت‌های سخت‌افزاری ریزپردازنده STM32 است. اگرچه این ریزپردازنده مقرون به صرفه و به‌طور گسترده در دسترس است، قدرت پردازش محدود و ظرفیت حافظه آن، پیچیدگی الگوریتم‌های پردازش سیگنال قابل پیاده‌سازی را محدود می‌کند. به‌عنوان مثال، روش‌های پیشرفته‌تر مانند فیلترینگ وفقی و رویکردهای مبتنی‌بر یادگیری ماشین که نشان داده شده است قابلیت‌های تشخیص جمینگ را افزایش می‌دهند، به دلیل این محدودیت‌های سخت‌افزاری نمی‌توانند به‌طور موثر در این بستر اجرا شوند. علاوه‌براین، دامنه روش‌های جمینگ آزمایش

شده در این مطالعه تا حدودی محدود بود. آزمایش‌ها عمدتاً بر جمینگ امواج پیوسته متمرکز بودند که اشکال معمول، اما نسبتاً ساده، تداخل هستند. روش‌های پیچیده‌تر جمینگ، مانند آن‌هایی که شامل پرش فرکانس یا جمینگ فریبنده (فریب) می‌شوند، مورد آزمایش قرار نگرفتند. این روش‌های پیشرفته جمینگ به‌طور فزاینده‌ای رایج می‌شوند و چالش‌های مهمی را برای یکپارچگی سیگنال GPS ایجاد می‌کنند. سامانه فعلی ممکن است به‌طور کامل برای مدیریت این اشکال پیچیده‌تر تداخل، همانطور که در مقالات نشان داده شده است، مجهز نباشد. افزون‌بر آن، محیطی که در آن آزمایش‌ها انجام شد، کنترل شده بود و شرایط پویا و غیرقابل پیش‌بینی را که در استفاده از GPS در شرایط واقعی با آن مواجه می‌شد، به‌طور کامل تکرار نمی‌کرد. این محدودیت بر تعمیم‌پذیری نتایج تأثیر می‌گذارد، زیرا عملکرد سامانه در موقعیت‌های چالش‌برانگیزتر آزمایش نشده باقی می‌ماند.

۴. نتیجه‌گیری

در این مقاله، یک روش مبتنی بر فیلتر وفقی LMS برای مقابله با جمینگ GPS ارائه شد. نتایج شبیه‌سازی نشان دادند که فیلتر LMS توانست SNR سیگنال GPS را به میزان حداقل ۱۶.۳۹ دسی‌بل بهبود بخشد و MSE را تا نزدیک به ۶۰ درصد کاهش دهد که یعنی فیلتر LMS می‌تواند تقریبا به‌طور موثر جمینگ را در موقعیت‌های مختلف کاهش دهد و یکپارچگی سیگنال GPS را حفظ کند. پس از اعتبارسنجی الگوریتم فیلتر در محیط MATLAB، سپس بر روی ریزپردازنده برای آزمون عملکرد پیاده‌سازی شد. سامانه پیاده‌سازی شده بر روی ریزپردازنده ARM از خانواده STM32 قادر به شناسایی و کاهش سیگنال‌های جمینگ موج پیوسته با دقت و کارآیی بالا است. این سامانه توانست به‌طور مؤثر نویزهای ایجاد شده توسط سیگنال‌های جمینگ را در زمان واقعی فیلتر کند و یکپارچگی سیگنال‌های GPS را حتی در شرایط وجود تداخل حفظ کند. از مزایای اصلی این سامانه می‌توان به کم‌هزینه بودن، مصرف توان کم، زمان اجرای پایین و مقیاس‌پذیری آن اشاره کرد که باعث می‌شود در بسیاری از کاربردهای تعبیه‌شده و سامانه‌های IoT قابل استفاده باشد. این پروژه با ارائه روشی عملی برای مقابله با تداخل‌های جمینگ، کمک مهمی به افزایش امنیت سامانه‌های GPS می‌کند.

۵. پیشنهادها برای کار در آینده

در راستای ادامه این پژوهش، پیشنهادهای زیر مطرح می‌شود:

- ✓ **ارتقای کارآیی سامانه در محیط‌های پیچیده‌تر:** آزمایش سامانه در محیط‌های واقعی با جمینگ‌های پیچیده‌تر و ارزیابی عملکرد آن در مواجهه با تداخل‌های چندگانه می‌تواند به بهبود طراحی سامانه منجر شود.
- ✓ **گسترش قابلیت تشخیص برای سایر انواع تداخل‌ها:** علاوه بر جمینگ موج پیوسته، سایر انواع تداخل‌ها مانند جمینگ پالس و فریب نیز می‌توانند مورد بررسی قرار گیرند و قابلیت سامانه در تشخیص و کاهش آن‌ها بهبود یابد.
- ✓ **یکپارچه‌سازی با سامانه‌های GPS پیشرفته‌تر:** گسترش و ادغام سامانه با گیرنده‌های GPS پیشرفته‌تر و بهره‌گیری از الگوریتم‌های بهینه‌سازی جدید می‌تواند کارآیی و دقت بیشتری در مقابله با تداخلات ایجاد کند.
- ✓ **گسترش سامانه به سامانه‌های چندفرکانسی:** با استفاده از گیرنده‌های چندفرکانسی، می‌توان توانایی سامانه را در مواجهه با حملات جمینگ پیچیده‌تر بهبود داد.
- ✓ **بهبود الگوریتم‌های یادگیری ماشین:** استفاده از روش‌های مبتنی‌بر یادگیری ماشین و به‌کارگیری الگوریتم‌های پیشرفته‌تر آن برای بهبود فرآیند شناسایی و تشخیص تداخل‌ها پیشنهاد می‌شود. این روش‌ها می‌توانند موجب افزایش دقت شناسایی و کاهش زمان پاسخ‌دهی شوند.

- ✓ **پیاده‌سازی سخت‌افزاری پیشرفته‌تر:** استفاده از ریزپردازنده‌های با قدرت پردازش بالاتر و بهینه‌سازی سخت‌افزاری می‌تواند عملکرد کلی سامانه را بهبود بخشد.
- ✓ **بررسی سایر روش‌های مقابله با تداخل:** تحقیقات بیشتر روی روش‌های دیگر از جمله استفاده از آنتن‌های شکل‌دهی پرتو و گیرنده‌های با فیلترهای پیشرفته‌تر، می‌تواند موجب افزایش مقاومت سامانه در برابر جمینگ‌های مختلف شود.

ادامه تحقیقات در این حوزه می‌تواند به توسعه سامانه‌های کارآمدتر و قابل‌اعتمادتری برای مقابله با تهدیدات تداخل سیگنال GPS منجر شود که اهمیت بالایی در کاربردهای دفاعی، حمل و نقل و زیرساخت‌های حیاتی دارند.

۶. مراجع

[۱] سید محمدرضا موسوی میرکلائی، "پردازش داده‌ها در گیرنده‌های تک فرکانسه GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۸۹.

[۲] سید محمدرضا موسوی میرکلائی، مریم معاضدی، محمدجواد رضایی و امیر طباطبایی،" مقابله با اختلال در گیرنده‌های GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۴.

[3] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, ‘‘GPS Vulnerability to Spoofing Threats and Overview of Anti-Spoofing Techniques”, International Journal of Navigation and Observation, pp. 1-16, 2012.

[4] D. Borio, C. O'Driscoll, and J. Fortuny, “GNSS Jammers: Effects and Countermeasures”, IEEE Workshop on Satellite Navigation Technologies (Navitech) & European Workshop on GNSS Signals and Signal Processing, pp. 1-7, 2012.

[5] C. Z. Wang, L. W. Kong, J. Jiang, and Y. C. Lai, “Machine Learning-based Approach to GPS Antijamming,” GPS Solutions, vol. 25, no. 3, Jun. 2021.

[6] E. Elezi, G. Çankaya, A. Boyacı and S. Yarkan, "A Detection and Identification Method Based on Signal Power for Different Types of Electronic Jamming Attacks on GPS Signals," IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1-5, 2019.

[7] D. Borio, "A Multi-State Notch Filter for GNSS Jamming Mitigation," IEEE Conference on Localization and GNSS, pp. 1-6, 2014.

[8] Y. R. Chien, "Design of GPS Anti-Jamming Systems using Adaptive Notch Filters," IEEE Systems Journal, vol. 9, no. 2, pp. 451-460, 2015.

[9] D. Li, J. Liu, J. Zhao, G. Wu, and X. Zhao, “An Improved Space-time Joint Anti-Jamming Algorithm based on Variable Step LMS,” Tsinghua Science and Technology, vol. 22, no. 5, pp. 520-528, Sep. 2017.

[10] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, “Protecting GNSS Receivers from Jamming and Interference,” Proceedings of the IEEE, vol. 104, no. 6, pp. 1327-1338, Jun. 2016.

[11] D. Borio and C. Gioia, "Interference Mitigation: Impact on GNSS Timing," GPS Solutions, vol. 25, pp. 1-18, 2021.

[12] H. Elghamrawy, M. Karaim, M. Tamazin, and A. Noureldin, “Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers,” Applied Sciences, vol. 10, no. 12, 2020.

طبقه‌بندی توئیت‌های فارسی براساس هشتگ‌های پرکاربرد با استفاده از شبکه‌های عصبی عمیق

مجید عبدالرزاق‌نژاد [*۱]، هنگامه نخعی [۲].

۱- دانشیار علوم کامپیوتر، دانشکده مهندسی کامپیوتر و صنایع، دانشگاه صنعتی بیرجند.

۲- کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد بیرجند، دانشگاه آزاد اسلامی.

چکیده

امروزه شبکه‌های اجتماعی مجازی نقش بسیار مهمی را در حوادث سیاسی، اجتماعی در کشورها و فرهنگ‌های گوناگون بازی می‌کنند. هشتگ نوعی برچسب است که در شبکه‌های اجتماعی همانند فیس بوک، توئیتر، گوگل پلاس، اینستاگرام و... مورد استفاده قرار می‌گیرد تا هر زمان که نیاز باشد بتوانیم مجموعه‌ای از اطلاعات مختلف در مورد موضوع به خصوصی را در اختیار بگیریم. از طرفی طبقه‌بندی توئیت‌ها یک تکنیک علمی به منظور پیش بینی نوع توئیت‌ها و تشخیص جهت‌گیری معنایی آنها می‌باشند. بر این اساس در این مقاله با هدف طبقه‌بندی چندگانه توئیت‌های فارسی از هشتک‌های پرکاربرد در یادگیری شبکه عصبی عمیق استفاده شده است. در رویکرد پیشنهادی از امبدینگ‌های کلمات تشکیل دهنده برای استخراج امبدینگ‌های هشتگ‌ها استفاده کرده و یک مدل برچسب گذاری چندگانه قبل از اجرای فرایند یادگیری عمیق انجام شده است. این رویکرد برروی یک داده دنیای واقعی که در دو بازه زمانی ۲۲ تا ۲۷ تیرماه ۹۸ و ۸ تا ۱۰ آبانماه ۹۸ اقدام به استخراج ۲۱۲۱۲ توئیت کرده بود پیاده سازی شد. دقت الگوریتم بر روی این داده برابر ۹۲ درصد بدست آمده است.

کلمات کلیدی: طبقه‌بندی، توئیت‌های فارسی، شبکه عصبی کانولوشنال، یادگیری عمیق، امبدینگ، هشتگ.

۱. مقدمه

با ظهور شبکه‌های اجتماعی مجازی، روابط انسان‌ها در اینترنت شکل تازه‌ای به خود گرفته است. رسانه‌های اجتماعی اشکال دیگر ارتباطات کامپیوتر محور را با یکدیگر ادغام کرده و به تبع آن چشم‌انداز رسانه‌ها، شیوه‌های تعامل افراد و تأمین نیازهای کاربران را دگرگون ساخته‌اند. در بستر همیشه در حال تحول رسانه‌های اجتماعی، توئیتر (که اکنون با نام X شناخته می‌شود) به عنوان یک پلت فرم که در آن کاربران افکار، نظرات و تجربیات خود را در زمان واقعی به اشتراک می‌گذارند برجسته است. با میلیون‌ها توئیتی که روزانه تولید می‌شود، حجم انبوه داده‌ها هم فرصت‌ها و هم چالش‌هایی را برای محققان و کسب‌وکارهای مختلف ایجاد می‌کند [۱]. یکی از جذاب‌ترین جنبه‌های داده‌های توئیتر، استفاده از هشتگ‌ها است که به

* **Corresponding author: مجید عبدالرزاق نژاد**
Email: abdolrazzagh@birjandut.ac.ir

عنوان ابزاری قدرتمند برای دسته‌بندی ، کشف محتوا و گسترش علائم تجاری عمل می‌کنند. هشتگ‌ها که اثرگذاری بیشتر از هزاران کلمه در شبکه‌های اجتماعی دارند، نه تنها به سازمان‌دهی توییت‌ها کمک می‌کنند، بلکه نقش مهمی در افزایش دید و دسترسی پست‌ها دارند [۲]. در این زمینه، مفهوم برچسب‌گذاری چندگانه بر اساس تعبیه هشتگ‌های پرکاربرد و جاسازی کلمات توئیت آن‌ها به‌عنوان یک حوزه مهم مطالعه پدیدار می‌شود.

برچسب‌گذاری چندگانه شامل اختصاص بیش از یک برچسب به یک توئیت است که امکان دسته‌بندی دقیق‌تر و جامع‌تر را فراهم می‌کند. این رویکرد به ویژه در گرفتن ماهیت چند وجهی توئیت‌ها، که اغلب موضوعات یا احساسات متعددی را به طور همزمان در بردارند، مفید است [۳]. به عنوان مثال، یک توییت در مورد یک گوشی هوشمند جدید ممکن است شامل هشتگ‌های مرتبط با فناوری، بررسی‌ها و ویژگی‌های خاص آن باشد که جنبه‌های مختلف محتوا را منعکس می‌کند. با استفاده از برچسب‌گذاری‌های متعدد، محققان و کسب‌وکارها می‌توانند بینش عمیق‌تری درباره زمینه و ارتباط توئیت‌ها به دست آورند که منجر به تحلیل‌های دقیق‌تر و معنادارتر می‌شود.

برای پیاده سازی موثر برچسب گذاری‌های چندگانه، درک روابط معنایی بین هشتگ‌ها و کلمات استفاده شده در توئیت‌ها ضروری است. اینجاست که مفهوم امبدینگ مطرح می‌شود. امبدینگ تکنیکی است که در پردازش زبان طبیعی (NLP) برای نمایش کلمات یا عبارات به عنوان برداری عددی در یک فضای برداری پیوسته استفاده می‌شود. این بردارها معنایی، مفهوم و نقش کلمات را می‌گیرند و امکان شناسایی شباهت‌ها و روابط بین آنها را فراهم می‌کنند [۴]. در زمینه توئیتر، امبدینگ را می‌توان هم برای هشتگ‌ها و هم برای کلمات توئیت اعمال کرد و امکان ایجاد نمایش‌های غنی و چند بعدی از توئیت‌ها را فراهم کرد.

هنگامی که امبدینگ گذاری مربوط توئیت‌ها بر اساس هشتگ‌ها و کلمات آن‌ها انجام شدند، گام بعدی طبقه‌بندی آن‌ها در دسته‌های مرتبط است. این مهم باعث می‌شود فرایند مرتب کردن، ایجاد سلسله مراتب مفهومی، جستجو کردن توئیت‌های منتشر شده برای یک محصول یا کسب و کار مشخصی تسهیل گردد [۵]. یادگیری عمیق، زیر مجموعه‌ای از یادگیری ماشین، به عنوان ابزاری قدرتمند برای این کار ظاهر شده است. مدل‌های یادگیری عمیق، مانند شبکه‌های عصبی کانولوشن (CNN) و شبکه‌های عصبی تکراری (RNN)، موفقیت قابل توجهی را در وظایف مختلف NLP از جمله طبقه‌بندی متن نشان داده‌اند [۶]. این مدل‌ها می‌توانند به‌طور خودکار الگوها و ویژگی‌های پیچیده را از مجموعه داده‌های بزرگ بیاموزند، و آنها را برای طبقه‌بندی توئیت‌ها بر اساس چندین برچسب مناسب می‌سازند.

یکی از مؤلفه‌های کلیدی مدل‌های یادگیری عمیق برای طبقه‌بندی توئیت‌ها، استفاده از امبدینگ‌های کلمات از پیش آموزش‌دیده است. این امبدینگ‌ها توسط روش‌هایی مانند Word2Vec، GloVe، و FastText، بر روی مجموعه‌های وسیعی از داده‌های متنی آموزش داده شده‌اند و روابط معنایی بین کلمات را به تصویر می‌کشند. با استفاده از امبدینگ‌های از پیش آموزش‌دیده، مدل‌های یادگیری عمیق می‌توانند از اطلاعات معنایی غنی کدگذاری‌شده در این بردارها بهره‌مند شوند که منجر به بهبود عملکرد در وظایف طبقه‌بندی توئیت‌ها می‌شود. به عبارت دیگر روش‌های طبقه‌بندی متونی که از امبدینگ‌های از پیش آموزش‌دیده استفاده می‌کنند، می‌توانند مفهوم هشتگ‌ها و کلمات توئیت‌ها را بهتر درک کرده و در نتیجه طبقه‌بندی‌های دقیق‌تر و مرتبط‌تری داشته باشند [۷].

حوزه طبقه‌بندی توئیت‌ها و برچسب‌گذاری‌های چندگانه در سال‌های اخیر پیشرفت‌های قابل‌توجهی را تجربه کرده است که ناشی از توسعه مدل‌های یادگیری عمیق پیچیده و تکنیک‌های امبدینگ است. چندین مطالعه استفاده از یادگیری عمیق را برای طبقه‌بندی چند برچسبی مورد بررسی قرار داده‌اند، که در آن توییت‌ها بر اساس محتوای‌شان برچسب‌های متعددی اختصاص می‌دهند. به عنوان مثال، یک مطالعه جامع مروری توسط Tarekegn و همکاران انجام شد [۸]. در این مطالعه مروری کارهای گذشته، معماری‌های مختلف یادگیری عمیق، از جمله شبکه‌های عصبی ترانسفورمرها، رمزگذارهای خودکار، و شبکه‌های کانولوشنال و تکراری را مورد بحث قرار داده و تجزیه و تحلیل مقایسه‌ای از روش‌های موجود را ارائه می‌دهد. مطالعه قابل توجه دیگری توسط مینایی و همکاران [۶] در مورد نوآوری‌های فنی و نقاط قوت بیش از ۱۵۰ مدل

یادگیری عمیق ارائه شد و بینش‌های ارزشمندی را در مورد تکنیک‌های پیشرفته برای طبقه‌بندی توئیت‌ها ارائه کردند. به طور مشابه، مطالعه‌ای توسط Sahoo و همکارانش [۹] نیز انجام شده است. همچنین مقالات تحقیقاتی متعددی وجود دارند که به طور خاص بر روی کاربرد یادگیری عمیق برای طبقه‌بندی توئیت‌ها متمرکز شده‌اند. به عنوان مثال، مطالعه‌ای توسط Krouska و همکاران [۱۰] انجام گرفت که با امبدینگ‌های مختلف از جمله Word2Vec، GloVe و FastText آزمایش کردند و نشان دادند که مدل‌های یادگیری عمیق با استفاده از این امبدینگ‌ها از الگوریتم‌های یادگیری ماشین سنتی بهتر عمل می‌کنند. علاوه بر این، تحقیقات سارا مفتاح و همکاران [۱۱] یک مطالعه درباره اثربخشی تکنیک‌های یادگیری خصمانه در بهبود دقت مدل‌های برچسب‌گذاری برجسته می‌کند، که می‌تواند به وظایف برچسب‌گذاری و طبقه‌بندی توییت‌های متعدد گسترش یابد.

باتوجه به اینکه در تحقیقات انجام شده تمرکز برروی توئیت‌های انگلیسی بوده و تمرکز کمتری برروی برچسب‌گذاری چندگانه توئیت‌های فارسی و طبقه‌بندی آنها انجام گرفته، در این مقاله به دسته‌بندی چندگانه و بلادرنگ توئیت‌های فارسی بر اساس هشتگ‌های پرکاربرد با استفاده از یادگیری عمیق پرداخته‌ایم. در ادامه در بخش دوم به تشریح فازهای روش پیشنهادی و در بخش سوم نیز نحوه جمع آوری توئیت‌های فارسی و پیاده‌سازی روش پیشنهادی و نتایج بدست آمده بیان شده است.

۲- روش پیشنهادی

روش پیشنهادی متشکل از پنج فاز عمده پیش‌پردازش و پاکسازی توئیت‌های فارسی، ایجاد بردار عددی متناظر با هر توئیت یا مدلسازی امبدینگ براساس امبدینگ هر کلمه و هر هشتگ، تراز نمودن هر توئیت با بهترین هشتگ، تنظیم ابرپارامترهای روش پیشنهادی و در نهایت معماری شبکه عصبی عمیق کانولوشن که در ادامه تشریح می‌شوند.

۲-۱ پیش‌پردازش داده‌ها

به منظور پیش‌پردازش و پاکسازی توئیت‌های فارسی جمع آوری شده نخست باید توئیت‌هایی که به زبان فارسی نیستند و بخشی جدایی ناپذیر از داده‌های خام توئیتر هستند از پایگاه داده حذف می‌کنیم. این مهم توسط فراداده‌های نشانگر زبانی تشخیص می‌دهیم. باتوجه به نیاز مدل پیشنهادی به حداقل یک حقیقت مبنا (هشتگ‌های واقعی که توسط کاربران آن توئیت‌ها ایجاد شده‌اند) در هر توئیت، لذا وجود حداقل یک هشتگ الزامی خواهد. از این رو توئیت‌هایی را که دارای حداقل یک هشتگ مرتبط نمی باشند، حذف کردیم. یافت کلمات کلیدی هر توئیت، نرمال‌سازی هر توئیت (حذف کلمات محاوره‌ای که کاربر در توئیت استفاده کرده ولی در دیکشنری‌های رسمی وجود ندارند)، و حذف کلمه توقف، به عنوان بخش‌های مرحله پیش پردازش انجام می‌شوند.

۲-۲ مدلسازی امبدینگ هرکلمه، هر هشتگ

در مدل‌های موجود، امبدینگ‌های هشتگ‌ها براساس کلمات همسایه هشتگ محاسبه می‌شوند، ولی در این پژوهش از امبدینگ‌های کلمات تشکیل دهنده توئیت برای استخراج امبدینگ‌های هشتگ‌ها استفاده کرده‌ایم. لذا در ابتدا با جمع‌آوری تمام توئیت‌های t_h که هشتگ h در آن‌ها ظاهر شده است، یک سند برای هر هشتگ مانند D_h ایجاد می‌شود. شایان ذکر است که تمام هشتگ‌ها و اشارات از سند حذف می‌شوند. H را به عنوان مجموعه تمام هشتگ‌هایی ظاهرشده در مجموعه داده کلی درنظر گرفته، بدین ترتیب برای هر هشتگ h، یک سند D_h به صورت زیر ایجاد می‌کنیم.

$$D_h = \cup \{t_h\} - (\forall h \in H)\{h\} \quad (۱)$$

سپس یک مدل امبدینگ کلمه برای هر سند (متناظر با یک هشتگ) ایجاد می‌کنیم. برای ایجاد این مدل، برای هر کلمه بر اساس استفاده از آن در توئیت‌هایی که حاوی این هشتگ می‌باشند (یعنی برای این هشتگ به سند تعلق دارند)، یک امبدینگ اختصاص داده می‌شود. امبدینگ را با Word2Vec بر اساس skip-gram انجام داده‌ایم. اگر W_h را مجموعه‌ای از کلمات ظاهرشده در D_h در نظر بگیریم. عملیات محاسبه امبدینگ برای تمام کلمات $w \in W_h$ تکرار می‌شود، تا امبدینگ تمام کلماتی که در داخل سند متناظر با هشتگ ظاهر شده‌اند، بدست آید. در نهایت، با استفاده از امبدینگ کلماتی که در توئیت‌های سند حاوی هشتگ ظاهر می‌شوند، امبدینگ V_h براساس میانگین تمام امبدینگ‌های کلمات ظاهر شده در سند برای هر هشتگ محاسبه می‌شود.

$$V_h = \frac{\sum_{w \in W_h} (u_{w,\,h})}{|D_h|} \quad (۲)$$

که در آن $u_{w,\,\mathrm{h}}$ بردار امبدینگ یک کلمه w در W_h و $|D_h|$ طول کلی سند D_h براساس تعداد کلمات (با حفظ کلمات تکراری) می‌باشند. توجه شود که اجرای فرایند فوق برای کلمات تکراری به هرچندبار در سند D_h در نظر گرفته می‌شوند.

۲-۳ تراز نمودن هر توئیت با بهترین هشتگ ممکن

هدف این مرحله اختصاص همتراز ترین هشتگ برای هر توئیت براساس مدلسازی امبدینگ تعریف شده می‌باشد. لذا برای هر توئیت t_i مجموعه کلمات آنرا $word_{t_i}$ فرض می‌کنیم. سپس برای هر هشتگ $h \in H$ ضمن در نظر گرفتن W_h (مجموعه‌ای از کلمات ظاهرشده در D_h) بردار امبدینگ هر کلمه $w_{t_i} \in word_{t_i}$ متناسب با h یعنی $u_{w_{t_i},\,\mathrm{h}}$ برابر با $u_{w,\,\mathrm{h}}$ زمانیکه $w_{t_i} \in W_h$ باشد. حال بااستفاده از امبدینگ کلماتی که در $word_{t_i}$ برای توئیت t_i متناظر با هشتگ h بدست آمده، امبدینگ V_{h,t_i} براساس میانگین زیر محاسبه می‌شود:

$$V_{h,t_i} = \frac{\sum_{w_{t_i} \in word_{t_i}} (u_{w_{t_i},\,h})}{|word_{t_i}|} \quad (۳)$$

میزان تزار هشتگ h برای توئیت t_i با نماد h_{t_i} نمایش می‌دهیم از طریق محاسبه میزان شباهت کسینوسی دو بردار امبدینگ V_{h,t_i} و V_h انجام خواهد شد. از بین تمامی هشتگ‌های H، تعداد k هشتگ که بیشترین h_{t_i} را داشتند بعنوان k هشتگ تراز شده برای توئیت t_i با بردارهای امبدینگ V_h در نظر گرفته خواهند شد.

۲-۴ تنظیم ابرپارامترهای روش پیشنهادی

روش پیشنهادی شامل چهار ابرپارامتر تنظیم فرکانس رخداد مینیمم کلمه، اندازه پرش، تعیین ابعاد بردار عددی امبدینگ و حداکثر تعداد هشتگ‌های ترازشده برای هر توئیت است. به منظور پرهیز از در نظر گرفتن کلمات کم اهمیت، فقط کلماتی که از یک مقدار آستانه مشخص بیشتر در سند آمده‌اند بعنوان فرکانس رخداد مینیمم کلمه انتخاب خواهند شد. این آستانه به صورت تجربی در این پژوهش ۳ تنظیم شده است. همچنین به دلیل استفاده از الگوریتم skip-gram برای امبدینگ (و عدم استفاده از مدل بسته کلمات) و به منظور تعیین ماکزیمم اندازه پنجره skip این پارامتر بصورت تجربی برابر با ۴ مفروض شد. بعبارت دیگر در روش پیشنهادی از skip-4 gram استفاده شده است. از آنجایی که طول

بردار عدد که از امبدینگ‌های Word2Vec استفاده می‌کنند بین ۵۰ تا ۶۰۰ کاربرد بیشتری داشته‌اند در این پژوهش آزمایشاتی براساس طول‌های ۵۰، ۱۰۰، ۲۰۰، ۴۰۰ و ۶۰۰ انجام گرفت که بهترین نتایج برای بردارهای اندازه ۵۰ بدست آمد. لذا سومین ابرپارامتر روش پیشنهادی یعنی تعیین ابعاد بردار، ۵۰ مفروض شد. در نهایت در این پژوهش حداکثر تعداد هشتگ تراز شده برای هر توئیت به منظور برچسب‌گذاری چندگانه توئیت‌ها ۳ مفروض شد.

۲-۵ معماری شبکه عصبی کانولوشن عمیق

در روش پیشنهادی از یک شبکه عصبی کانولوشن عمیق استفاده شده که از یک لایه کانولوشن با ۲۸ نرون و یک لایه max pooling بعد آن استفاده شده است که سایز ورودی را نصف می‌کند. این عمل باعث می‌شود از بیش برازش شبکه جلوگیری شود. سپس از یک لایه Dense با ۳۰ نرون و در انتهای یک لایه Dense با چهار نرون برای کلاس خروجی استفاده شده است. زیرا توئیت‌ها در چهار دسته ورزشی، سیاسی، سینمایی و مذهبی استخراج شده و یادگیری شبکه مذکور می‌بایست براساس این چهار طبقه انجام بگیرد.

۳- آزمایشات و نتیجه‌گیری

به منظور پیاده‌سازی روش پیشنهادی از یک سیستم با پردازشگر INTEL CORE I7 2.6 GHZ -6700K، حافظه رم ۸ گیگابایتی با سیستم عامل ویندوز استفاده شده است. پیاده سازی با زبان پایتون و در محیط برنامه نویسی jupyter notebook انجام داده‌ایم. برای پیاده‌سازی شبکه کانولوشن شبکه عمیق از کتابخانه‌های Keras و TensorFlow و Scikit learn استفاده شده است.

۳-۱ جمع آوری توئیت‌های فارسی

در این پژوهش، برای جمع‌آوری توئیت‌های فارسی از کتابخانه tweepy و توابع جریانی توئیتردر زبان برنامه‌نویسی پایتون که امکان خواندن مداوم توئیت‌های تصادفی را به ما می‌دهد، استفاده کردیم. برای دریافت توییت‌های دسته سیاسی از هشتگ‌های : 'احمدی نژاد'، 'مجلس'، 'ظریف'، 'ارزش پول ملی'، 'برجام'، 'ترامپ'، 'دلار'، 'روحانی'، 'رئیس جمهور' و برای دریافت توییت‌های دسته ورزشی از هشتگ‌های : 'سعید معروف'، 'کیروش'، 'فوتبالیست'، 'والیبال'، 'رونالدو'، 'مسی'، 'پرسپولیس'، 'فوتبال'، 'استقلال' استفاده شد. همچنین برای دریافت توییت‌های دسته سینمایی از هشتگ‌های : 'سینما'، 'گلزار'، 'مهناز افشار'، 'شهاب حسینی'، 'پژمان جمشیدی'، 'سام درخشانی'، 'اکبر عبدی'، 'ترانه علیدوستی'، 'پیمان معادی'، 'نوید محمد زاده'، 'حمید فرخ نژاد'، 'لیلا حاتمی'، 'بهرام رادان'، 'پرویز پرستویی'، 'فیلم'، 'سریال'، 'شبکه'، 'صدا و سیما'، 'نیکی کریمی'، 'جواد عزتی' و در نهایت برای دریافت توییت‌های دسته مذهبی از هشتگ‌های : 'مذهب'، 'اسلام'، 'دعا'، 'پیامبر'، 'حضرت فاطمه'، 'نماز'، 'مهدویت'، 'نیایش'، 'پروردگار'، 'زیارت'، 'عاشورا'، 'امام حسین'، 'حضرت علی' استفاده شد.

داده‌های توییتر برای دو دسته سیاسی و ورزشی با استفاده از هشتگ‌ها و کلمات کلیدی ذکر شده در روزهای ۲۲ تا ۲۷ تیر ماه ۹۸ دریافت شده است. در این مدت ۱۱۸۲۵ توییت دریافت شد که از این بین ۹۱۰۰ تا برای دسته سیاسی و ۲۷۲۵ تا برای دسته ورزشی است که بخشی از داده‌های توئیت که برای این دو دسته بدست آمده در شکل ۱ و ۲ نمایش داده شده است. همچنین داده‌های توییتر برای دو دسته سینمایی و مذهبی با استفاده از هشتگ‌ها و کلمات کلیدی ذکر شده در روزهای ۸ تا ۱۰ آبان ماه ۹۸ دریافت شده است. در این مدت ۹۳۸۷ توییت دریافت شد که از این بین ۴۸۸۲ تا

برای دسته سینمایی و ۴۵۰۵ تا برای دسته مذهبی است که بخشی از داده‌های توئیت این دو دسته نیز در شکل ۳ و ۴ ارائه شده است. بنابراین جهت پیاده‌سازی، داده‌های آموزش و آزمون به صورت زیر در نظر گرفته شده‌اند:

-تعداد کل نمونه‌های آموزش: ۲۱۲۱۲

-تعداد داده‌های آموزش: ۸۰ درصد برابر ۱۶۹۷۰ نمونه

-تعداد داده‌های اعتبارسنجی (٪ ۱۰از داده‌های آموزش): برابر ۱۶۹۷ نمونه

-تعداد داده آزمون: ۲۰ درصد برابر ۴۲۴۲ نمونه

1150021446107877376	@MinoBano مواظب رفتاروگفتارت باش آقای ترامپ با دم شیر بازی نکن
1150021476873060353	@FroghWazhma ر نهایت "پرهیزگار" و نهایت پاک نفس استفاده کردن اکثراً کار کسانی است که توسط وحشیان بلک واتر خریداری شده اند گ هولناک رخ می ده، طبیعت زندگی ه نه خواسته ی یک نوع رنگ #مرگ برای ضعیف #امر_طبیعی است هر #قوی اول #ضعیف شد بعد مرد
1150021491943067648	ایت و بی منطق خوانده، مناقشه‌ای دیپلماتیک میان آمریکا و انگلیس در گرفت که به مجادله لفظی میان دو طرف منتهی شد. به دنبال این جریان
1150021619546501121	ی ده، طبیعت زندگی ه نه خواسته ی یک نوع رنگ #مرگ برای ضعیف #امر_طبیعی است هر #قوی اول #ضعیف شد بعد مرد @kheradoo
1150021646478012416	لبانی در مصاحبه با فاکس نیوز: ▼او از جنبش مقاومت حمایت می‌کند، ▼ پرزیدنت از آنها حمایت می کند▼ دولت از آنها حمایت می کند ●
1150021729177219072	با دلار ۱۳۰۰۰تومن میشخ ۲۴۰ میلیون @sherlock1356
1150021730313916416	@M_khabar_negar @Atre_Yaas313 @springbymahdi ل دلیلش بری یاهنوز درگیری چرامنصوب دیگر رهبری از جنگ گفته
1150021738350153734	تحریم ها علیه ایران تو کنگره یه رای مخالف داشته ، بیانیه علیه خروج از برجام تو مجلس ما پونزده تا..چه مفهومی میتونه داشته باشه #نفوذ
1150021790581833728	@AshkanHaifa @Admiralchandler ما خود روحانی و خامنه ای رو هم به عنوان نمایندمون قبول نداریم ... نصرالله خر کیه ؟
1150021797666050049	و رقم زد، "برخی نهادها" نبودند، بلکه نفش خودت بود! آشنا گفت هنوز اول بازی!! آشنا و بازی با دم شیر(اعلام جنگ با نرمالیزاسیون چهره‌ها)
1150021814543945728	زکراکی از جانب محمدو بوهاری، رییس جمهور نیجریه، به رغم شرایط وخیم سلامتی او و دستور دادگاه مبنی بر آزادی وی، ابراز تاسف کرد
1150021911788818432	@motamedkia دی گوه خوریشونو میکردی الان که قراره گوهی بشی تو باشگاشون توییتاتو پاک میکنی نون حرومزادگی خوب بهت میسازه
1150021955241648129	شارهای ترامپ نظام ایران را پایدارتر می‌کند، فاصله رئیس جمهور آمریکا با اهداف و آرزوهایش در قبال ایران را بسیار زیاد ارزیابی کرد»
1150022001144283136	۱۹۹ و یک سال قبل از مرگ تویاک در زندان نوشته شده بود، ژوئیه ۲۰۱۷ به صد هزار دلار رسیده بود. لامصبا زنده و مرده، پول در میارن
1150022002259963904	دیگه از کانادا و آمریکا هشتگ میزنن که ترامپ تحریم کن، جنگ کن، ما مقاومت میکنیم! ما: ☺ ترامپ: ☺☺ مقاومت: ☺☺☺ جنگ: پشماااام
1150022014041640960	، برای تضمین عبور و مرور آزاد از تنگه هرمز هستیم اما این کار زمان می‌برد. رئیس جمهور ترامپ به وضوح متوجه شد که توافق هسته‌ای
1150022020698181633	ت چهل ساله #سرکوب در ترکیب با #اقتصاد ورشکسته، نهایتا مردم عاصی را به خیابان‌های اعتراض و #انقلاب خواهد کشاند. #کیهان_لندن
1150022064222478337	@MozhdeRestart1 @realDonaldTrump جنگ هفتاد و دو ملت همه را عذر بنه چون ندیدند حقیقت ره افسانه زدند
1150022104106119168	: فراموش کرده‌اید فرار خاوری به کانادا چه آسیبی به آبروی نظام زد؟ آنجا هم با وساطت وزیر ذیربط وقت، متهم از بازداشت رسته بود/الف
1150022120983924736	#Fake_ #Fakenews بررسي رويكرد مجلس و دولت #بريتانيا به #اخبار_جعلي،#اطلاعات_نادرست و #سواد_ديجيتالي در سال 2019
1150022135609348096	شرع، ها این شرع. مشروطه و مشروطه و شرع. ۴۰۰ ساله شرع. کاش عربها و ترکهای همسایه هم کمی مثل ما شرع داشتن. ای بی‌شرع ها
1150022172842319872	در فیس بوک ، ازمردم میخواسته درشرکتش سرمایه گذاری کنند ، یکی و دو سال هم سودی میداده ، بعدش هیچی. شرکتی خود این فرد نداشته
1150022199346171909	گ پشتیبانی می کند و نبرد باز شده است. افزود: "ارتش لیبی، ابزارهای خود را در برابر ترکیه دارد #لیبی #لیبیا #ایران #عربستان_سعودی
1150022206019256321	@Borsa342 @JudicialWatch @realDonaldTrump @restartleader د خارجی همراه با قیام میلیونها ایرانی خواهد شد
1150022328249659392	@coraliiine__ احتمالا باز دلار میخواد بره بالا
1150022434701152256	@Mohsen80550829 @cheraghi110 @ManotoNews @SamShahravi دلیلشو بدونی میفهمی چرا حق نداره ارتش درست کنه
1150022510823522304	رم یک نمونه از چنین اقدامی برای یک متهم مستضعف از گذشته خویش می‌تواند ارائه کند؟ فساد از پیوند قدرت و ثروت ستبر و پایدار می‌شود
1150022531195265027	یشون رییس کمیسیون امنیت ملی مجلس هستن. بنظرم که بالاترین صلاحیت سیاسی این شخص سخنرانی مذهبی در مسجد یک محله ست و بس
1150022577894506503	ون برای روابط بد گذشته و دعواهامون تنگ می شه مثل سربازی که دلش برای میدان جنگ تنگ می شه چون زندگی عادی براش کسل کننده س
1150022588174872576	هم بلاک آنبلاک خلاص, ما تو دنیای واقعی مون انقدر جنگ و جدل داریم اومدیم اینجا پی آرامش, آرامش ات رو بچسب جون جونی @grzngi
1150022615194591232	تحریم ها علیه ایران تو کنگره یه رای مخالف داشته. بیانیه علیه خروج از برجام تو مجلس ما پونزده تا ... چرا واقعا؟ #شفافیت
1150022669741506561	@VOAIran جناب ترامپ ماست خورد مرتیکه مادام الخمر
1150022697369440256	«یک میخ و چند کت» ساخته محسن خان‌جهانی رو ببینید. کسی که میگه که من کتم رو توی میدان شهر آویزون می‌کنم و ملت به من رأی میدن
1150022714587058176	@andishyar1 @AYAyatollahi ویزان اصلاح طلب و خاتمی و میر سبز یه روزم اویزان آخوند روحانی فردا هم شاید اویزان رئیسی
1150022715732111361	کدخدایی: شورای نگهبان به طرح تشدید مجازات اسیدپاشی ایراد گرفته و آنرا برای رفع ابهامات به مجلس برگشت داده است.|ایرنا
1150022725852946433	

شکل ۱- بخشی از توئیت¬های سیاسی

1150034522236489729	@Mahsae19 شون داد ما چهل امتیاز به حریف دادیم آقایان معروف موسوی یه تنه تیمو به فلک عظما دادن موسوی رو دعوت کردن ژاپن واسه تست مقاومت تور والیبال
1150034587453730816	کریم باقری
1150034662259068928	https://t.co/Rxj22oH7PV اعلام آمادگی پرسپولیس برای حضور در جام شهدا
1150034775056539654	اگه کونیمون نمیکنید من یه قیچی به تاج ابروم بزنم شبیه گاندالف شم
1150034845474705411	، مقام پنجم لیگ ملت‌های والیبال، در مجموع به پاداش ۲۰۳ هزار دلاری رسید. . تا این پول رو هم دولتمردان به حساب دستاورد برجام نزاشتن ، فیلم شو بسازید. #گاندو
1150034908049477635	کنین #استقلال منظورمه)بخاطر کوچکترین مسئله به کُل ارکان باشگاه حمله میکنن تا تیم توحاشیه بره! مرسي هوادارا با وجود شما تیم دشمن نمیخواد #حریر_سلطانیفر
1150034941637517312	رونالدو اورجینال
1150034984348069888	خودم با شماره ۸ برای استقلال بازی میکردم
1150035027910156289	https://t.co/WB4EgWJKce لذتی که توی فرمول یک هست تو فوتبال نیست
1150035089956528128	.با نظر و تصمیم کادر فنی، تیم #پرسپولیس دو دیدار دوستانه عصر روز دوشنبه در اردوی ترکیه برگزار خواهد کرد
1150035214682529793	@Rezars1717 اینارو‌بیخیال بازیا تیم ملی والیبال رو نشستی ساعت دوونیم نصف شب نگاه کردی ک چی بشه
1150035281711521792	@varesh_varesh اها!! تاج کبیر اسپا
1150035321008078848	https://t.co/xiGZH50HyL https://t.co/unZx1AnZMN فیلم/ شاهین سرخ شهریار قهرمان مسابقات فوتبال جام همبستگی مهاجرین غرب تهران
1150035350062075904	@MHemmatiBo @sahartolouee .شریفی خیلی حیف شد. فکر می کردم تو پرسپولیس به اوج بر میگردد
1150035382735659009	@mslmkzm1 .مجید حسینی۵.نورافکن۶.قربانی۷.بادو(مصدوم)۸.برزای۹.بویان. *نکته ضروری بگم.تو فوتبال ایده ستون داریم،یعنی خروجی ها از ستون تیم نباشن/ادامه
1150035406840373249	@Zarghami_ez درد و بلاش بخوره تو سر تاج زاده و زیبا کلام
1150035446891732998	@Pashfuckinmaam @Mahsae19 همیشه امتیاز سرویسمون واسه حریفه وقتی توپ هنوز تبدیل به امتیاز نشده خوشحالی میکنیم و همون توپ میخوابه تو زمینمون
1150035505238683648	.کریم باقری مربی تیم #پرسپولیس با حضور در باشگاه قرارداد جدید خود را برای یک سال دیگر با تیم تمدید کرد
1150035645680758785	@rdko0 @peyman3d فوتبال میای ردک خان؟
1150035659463282693	گابیج مربیه؟ یا پورن استار کروات؟
1150035661816307713	آندرس اینیستای کبیر
1150035782012456961	@Moeinmrezaei2 اره با کیروش کار می کرد
1150035827948511232	@sedfarbod مسی
1150035851424030720	https://t.co/Hm2En1Mfez وحید امیری قرارداد دو ساله‌ای را با قهرمان فوتبال ایران امضاء کرد و بار دیگر به جمع سرخپوشان ایران ملحق شد. #پرسپولیس
1150035852241907712	راض به عملکرد مدیران تیمشان، مقابل ساختمان این باشگاه تجمع کردند و علیه #امیرحسین_فتحی، مدیرعامل و #علی_خطیر، معاون ورزشی باشگاه استقلال شعار دادند
1150035971783704577	نی و ابراهیمی و جباروف و نیام به ترتیب خط ستون استقلال بودن.طرف مقابل.جلال و کمال و علیپور و بشار و نعمتی(دو هافبک جلوی اصلیش)حفظ شدن @mslmkzm1
1150036002565758978	مسی جانم
1150036115803516929	سی از هواداران از من ناراحت هستند برابر آنها حرفی برای گفتن ندارم فقط تمام سعی خودم را خواهم کرد تا با عملکرد خوب، دل آنها و همه هواداران را به دست بیاورم
1150036189803622401	.بزودی در تهران جام جهارجانبه شهدا با حضور تیم های فولاد خوزستان، سایپا، صنعت نفت آبادان و پرسپولیس تهران برگزار خواهد شد
1150036208539582464	سی از هواداران از من ناراحت هستند برابر آنها حرفی برای گفتن ندارم فقط تمام سعی خودم را خواهم کرد تا با عملکرد خوب، دل آنها و همه هواداران را به دست بیاورم
1150036242760908802	خدایا بشار عزیزم تو پرسپولیس بمونه به تخمت که کنعانی و فرشاد برگشتن
1150036337661231104	@masoud5020 این خائن الدنگ بر عکس بقیه یکم فوتبال بلده
1150036350751694848	@illaramendi47 -_- آخ آخ هاشمی‌نسب رو بگو :(یه بنده خدایی میگفت من هنوز آرزومه هاشمی‌نسب برگرده با لباس پرسپولیس خداحافظی کنه
1150036368640397312	لیل اینکه در مقایسه با ما همیشه طرف آنها را میگیرند این است که آنها را ضعیف تر میبینند! چون کوردها همیشه در مقابل فارسها تسلیم شده اند! مانند تسلیم قاضی محمد
1150036382078963713	د همراه میخواست، نه همفکر. سمت دیگر برانکو مداوم شانتاژ میشد. تاج از این دعوا حظ میبرد. طلوع کنندگان در وزارت هم البته سهم داشتند در آن فضای لجزده ۳/

شکل ۲- بخشی از توئیت¬های ورزشی

1189247476743716865	یزد – سیما و صدا خبرگزاری ☑ هم اکنون _ پیامبر آتش سوزی در کارخانه موکت مهریز @yazdmajazi یاد #خاتم #نفت
1189247550504742912	ول نیست؟؟مگه شادی نیست؟؟خود پیامبر گفتن اونوقت چرا صدا و سیما ول نمیکنه آخه.تازه یادش افتاده عزاداری کنه.بسّه آقای صدا و سیما
1189247582159151105	) : بزنین شبکه دو خاک بر سر ستایش که با شلوغ بازیاش حواسامون رو پرت کرد و نذاشت به سریال به این خوبی وقعی بنهیم
1189247610663641088	بله، لینکشو جستم و دیدم. چیزی که برام سال بود[جدی از تحلیل] این بود که این فیلم الان اومده رو پرده، شما دیده بودین یا؟؟؟ @smto
1189247652594176001	سریال پدر کدومه؟ خداروشکر مامان من نمیبینه @TOUGHGUY3484
1189247657342066690	تبلیغی هواداران مجاهدین در شهرهای میهن به‌مناسبت ۷ آبان سالروز کوروش کبیر / نه شاه، نه شیخ - مرگ بر ارتجاع، مرگ بر استبداد فیلم
1189247711549280261	. . . شمام یکی در میون فیلم از لِنگاک سیخ و لخت زن اجنبی میاد لای توییت ها؟ آخر این دوتا لِنگ شرف و آبرومنو میبره
1189247729366716424	نفری داره خواهش میکنه، سریال ستایش رو پخش کنین و بریم که ستایش 1 و 2 و3 رو از شنبه ،هر شب از آیفیلم ببینیم باز☹ #ستایش
1189247747397947393	من خودم چون میدونم اخرش چی میشه اصلا نگاه نمیکنم نه ستایش بلکه هیچ سریال ایرانی رو نگاه نمیکنم @tafti_ir
1189247763315339265	مصرف کردن را طی میکنند. این حس در سینما به شدت تاثیر متفاوتی داره و مشابه Enter the void @MrSoheail
1189247773847310336	اتفاقا منم تو فیلم دیدم 😂 ورزشاشونم بدآموزی داره @farshad_j_p
1189247792717414401	من یه سؤال دارم تو فیلم مغزهای کوچک زنگ زده مگر مرتکب قتل ناموسی نشدن؟ چرا اون توقیف نشد؟ چون آخرش دختره زنده موند؟
1189247833658068995	و میهیزین خانه پدری سرنوشت گام بلند تو سینمای خفه ماست. قیاص مع الفارق نکنیم @AGHANAZEM @Mitra91240086
1189247839513255938	خوشی های مردم خار داره همش از بدبختی ها فیلم میسازین #ستایش
1189247911407902720	، چندجا مردا بد خراب کرد امشب ب ستایش گفت «ما مردا قولمون تا وقتی قولِ ک خرمون از پل نگذشته باشه، قول ب عیال نصفِ قولم نیست
1189247924661817345	کارشناسی دعوت می کنن. #ابوبکربغدادی اگر ریش هاش رو می زد می تونست به جای #نجاح_محمدعلی تحلیلگر شبکه #بی_بی_سی باشه
1189247968009949186	اره سریال کره ای منم یه مدت پایه بودم، آهنگهای اینا که همه مسخره میکنن اینجا هم 😂😂😂 @GolrokhalizadeH
1189247969536757760	! این سریال جدیده که بازیگراش لنز میذارنم که انگار تمرکزش رو موضوع شوگر مامیه. و رقابت شوگر مامیا

شکل ۳- بخشی از توئیت¬های سینمایی

1189247666120736768	@A_simple_gal یوسف پیامبر 😚
1189247666531770368	@ermiya1214 ک هیچ یک از اهل بیت دلیل و روایت و یا حتی یک نقل تاریخی از اهل بیت نداریم که باید مجلس عزاداری برگزار کرد
1189247676476542977	@gharib_toos1995 @niloomatin @PiiiSelena @nane_sarma_ دعا کن دعا
1189247691819233282	از کسکش بودن برادران شیعی همین بس که برای امام حسین(ع)، مراسم چهلم هم میگیرن ولی برا پیامبر اکرم(ص) حتی مراسم سوم هم نمیگیرن
1189247705966620672	یان او را روح پروردگار بابلیان او را مورد تائید مردوک مسلمانان او را ذوالقرنین و فرستاده خدا و مردم جهان اورا بنیانگذار حقوق بشر میخوانند
1189247732239785984	@AR7_67 زیارت قبول التماس دعا
1189247744516472835	@dw_persian و مرد در افغانستان و در جهان. ما خورد و کلان همه یک انسان هستیم درجهان. ما کافر و مسلمان ندارم بس است کشتار
1189247753651507200	@Subterfugitive گفتم. چون شکر خدایان همه سلسله های ایرانی قبل و بعد از اسلام چماق دستشون بود برای تحمیل دین یا عقیده
1189247779291332608	واهد به دعاهای انسان‌ها گوش دهد باید تمام انسان‌ها با سرعت محو شوند چرا که آن‌ها به طور دائم برای دفع شر هم دیگر دعا می‌کنند. #براندازم
1189247792662962176	@tanasoli 😂😂😂😂 ! نماز حاجت چاره گشاست
1189247799659028486	@amin_asadii چه سعادتی التماس دعا
1189247831179255808	روز جهانی فلسفه: حدیث جعل می‌کنیم و می‌گوییم قبل از اسلام هیچ خبری نبوده، نه خیر، خیلی خبر بوده. ما #کوروش داریم و منشور حقوق بشر
1189247890792833024	@NrmSjd .. نه امام نه پیامبر و نه کتاب خاصی فقط این ۳تا: گفتار نیک کردار نیک پندار نیک همین ۳تارو انجام بدی میشی ک آریایی اصیل
1189247923630026752	@hp_babak جوری که کوروش خیلی باگ تاریخی داره داریوش و خشایار و هخامنشیان بسیار مستند و واقعیه. نه توهمه نه غرب پرستی
1189247979003232256	@fatima1361626 @sm_1361 @Jedaaal ر ان شاءالله که فقط تصور من باشه شما هم سلامت و موفق و مؤید باشید
1189248035752153088	له مذهب بالا تا ته کوچه شك تا هواي خنك استفنا تا شب خيس محبت رفتم من به ديدار كسي رفتم در آن سر عشق چيزها ديدم در روي سهراب
1189248061157134336	د؟؟ یعنی پیامبر هم شوگر مامی زده بود؟؟ نتیجه گیری:ازدواج سنت پیامبر است، درصورت شوگر مامی زدن «احسن» است. #جدی_نگیرید
1189248063929487361	رو شیره مالیدن ! اونم تو این روزها که بحث چند زنی داغه ! من طرفدار مهریه نیستم ولی اینم شد بهانه ؟ امام رضا بنده خدا رو چرا این وسط

شکل ۴- بخشی از توئیت¬های مذهبی

۳-۲ نتایج و ارزیابی

پس از پیش‌پردازش توئیت‌ها که بخشی از داده‌های پیش پردازش شده در شکل‌های ۵ الی ۸ نمایش داده شده، اقدام به تولید امبدینگ توئیت‌ها و هشتگ‌ها در نهایت تراز نمودن حداقل سه هشتگ به هر توئیت می‌نماییم. تقسیم‌بندی داده‌ها هم برای فرایند تولید امبدینگ‌ها به روش Word2Vec بر اساس skip-gram و هم برای شبکه عصبی کانولوشن عمیق براساس ۸۰ درصد آموزش، ۱۰ درصد اعتبارسنجی و ۲۰ درصد آزمون بوده است. در گام بعدی باید هر توئیت به فضای بردار انتقال داده شود. بدین صورت که یک فضای بردار متشکل از کلمات تمام توئیت‌ها داریم. در فضای بردار مربوط به هر توئیت، کلماتی که در آن توئیت استفاده شده‌اند مقدار ۱ و کلماتی که استفاده نشده¬اند برابر ۰ هستند. از این فضای برداری برای هر توئیت به عنوان ورودی یادگیری عمیق استفاده می‌شود.

تعداد مراحل تکرار الگوریتم برابر ۳۰ در نظر گرفته شده است. دقت الگوریتم روی داده‌های تست برابر ۹۹.۷ درصد است. همچنین شکل ۹، ماتریس درهم ریختگی برای مدل آموزش دیده شده و شکل ۱۰ معیارهای precision، recall و f1-score برای هر یک از کلاس‌ها (۰ کلاس ورزشی، ۱ کلاس سیاسی، ۲ کلاس سینمایی، ۳ کلاس مذهبی) نمایش داده است.

	ID	Text
0	1150021446107877376	...مواظب رفتاروگفتارت باش آقای ترامپ با دم شیر ب
1	1150021476873060353	...مسله استفاده جنسی از زنان در تمام کشور ها وجو
2	1150021491943067648	... یکی از ترفندهای مرسوم آبی های به اصطلاح مخالف
3	1150021619546501121	...آرزوی ترامپ برای سفیر انگلیس پس از افشای اینک
4	1150021646478012416	...یکی از ترفندهای مرسوم آبی های به اصطلاح مخالف
5	1150021729177219072	...رودی جولیانی وکیل رئیس جمهور آمریکا از آلبانی
6	1150021730313916416	با دلار ۱۳۰۰۰تومن میشخ ۲۴۰ میلیون
7	1150021738350153734	...خوب بادبزن جیگر حالا که شدی عاقل الدوله هنو
8	1150021790581833728	...تحریم ها علیه ایران تو کنگره به رای مخالف داشت
9	1150021797666050049	...ما خود روحانی و خامنه ای رو هم به عنوان نمای
10	1150021814543945728	...محمدعلی نجفی بنا به خواست برخی نهادها و علی رغ
11	1150021911788818432	...عبداللهی موسی دبیر انجمن آکادمیک جنبش اسلامی ن
12	1150021955241648129	...خبردلار خایه مال بنی وجود نجس امثال تو که وقت

شکل ۵- بخشی از توئیت¬های سیاسی پس از پیش پردازش

	ID	Text
0	1150034522236489729	... قشنگ فعل ریدمان رو صرف کردن آنالیز بازی نشون
1	1150034587453730816	کریم باقری
2	1150034662259068928	اعلام آمادگی پرسپولیس برای حضور در جام شهدا
3	1150034775056539654	...اگه کونیمون نمیکنید من به قیچی به تاج ابروم بز
4	1150034845474705411	...تیم ملی والیبال ایران با کسب مقام پنجم لیگ ملت
5	1150034908049477635	...توباشگاه اُلنگ همه جورحاشیه و اختلاف هست بدون ك
6	1150034941637517312	رونالدو اورجینال
7	1150034984348069888	خودم با شماره ۸ برای استقلال بازی میکردم
8	1150035027910156289	لذتی که توی فرمول یک هست تو فوتبال نیست
9	1150035089956528128	... با نظر و تصمیم کادر فنی تیم پرسپولیس دو دیدار
10	1150035214682529793	...اینارویبخیال بازیا تیم ملی والیبال رو نشستی س
11	1150035281711521792	اهاا تاج کبیر اسیا
12	1150035321008078848	...فیلم شاهین سرخ شهریار قهرمان مسابقات فوتبال جا

شکل ۶- بخشی از توئیت¬های ورزشی پس از پیش پردازش

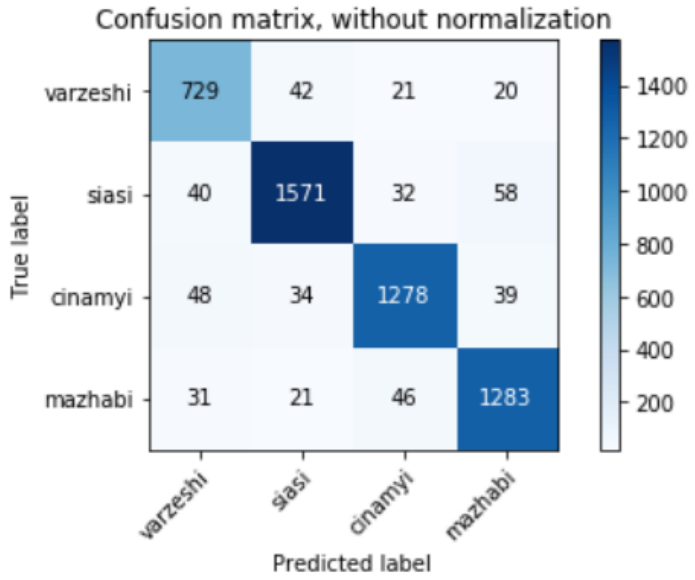
	ID	Text
0	1189247476743716865	...آتش سوزی در کارخانه موکت مهریز هم اکنون خبر
1	1189247550504742912	...بابا مگه فردا اول ربیع الاول نیستمگه شادی نیست
2	1189247582159151105	...بزنین شبکه دو خاک بر سر ستایش که با شلوغ بازیا
3	1189247610663641088	...]بله اینکتو جستم و دیدم چیزی که برام سال بود
4	1189247652594176001	سریال پدر کدومه خداروشکر مامان من نمیبینه
5	1189247657342066690	...فعالیتهای تبلیغی هواداران مجاهدین در شهرهای می
6	1189247711549280261	...شمام یکی در میون فیلم از اینگای سیخ و لخت زن ا
7	1189247729366716424	... خب الان دیگه وقتشه که باز شبکه آیفیلم به صدای
8	1189247747397947393	...من خودم چون میدونم اخرش چی میشه اصلا نگاه نمی
9	1189247763315339265	...و مشابه میافته و بیننده تجربه مشابهی با کا
10	1189247773847310336	اتفاقا منم تو فیلم دیدم ورزشاشونم بدآموزی داره
11	1189247792717414401	...من یه سؤال دارم تو فیلم مغزهای کوچک زنگ زده مگ
12	1189247833658068995	...بهروز شعیبی بسیار فیلمساز منحصر به فردیه اما

شکل ۷- بخشی از توئیت‌های سینمایی پس از پیش پردازش

	ID	Text
0	1189247666120736768	یوسف پیامبر
1	1189247666531770368	...به جز گریه و عزاداری برای امام حسین ع برای هی
2	1189247676476542977	دعا کن دعا
3	1189247691819233282	...از کسکش بودن برادران شیعی همین بس که برای امام
4	1189247705966620672	...در بسیاری از کشورهای دنیا مردم کوروش‌کبیر را ا
5	1189247732239785984	زیارت قبول التماس دعا
6	1189247744516472835	...مردم آمریکا شما در کشور اسلامی جانس ندارد بیخ
7	1189247753651507200	...آقا جان از نظر ازادی عقیده و بیان گفتم چون شک
8	1189247779291332608	...اگر خدا بخواهد به دعاهای انسان‌ها گوش دهد باید
9	1189247792662962176	نماز حاجت چاره گشاست
10	1189247799659028486	چه سعادتی التماس دعا
11	1189247831179255808	...دکتر دینانی در روز جهانی فلسفه حدیث جعل می‌کنی
12	1189247890792833024	...آریایی بودن چیز خاصی نمیخواد نه امام نه پیامب

شکل ۸- بخشی از توئیت‌های مذهبی پس از پیش پردازش

```
Confusion matrix, without normalization
[[ 729   42   21   20]
 [  40 1571   32   58]
 [  48   34 1278   39]
 [  31   21   46 1283]]
```



شکل ۹- ماتریس درهم ریختگی

	precision	recall	f1-score	support
0	0.86	0.90	0.88	812
1	0.94	0.92	0.93	1701
2	0.93	0.91	0.92	1399
3	0.92	0.93	0.92	1381
accuracy			0.92	5293
macro avg	0.91	0.92	0.91	5293
weighted avg	0.92	0.92	0.92	5293

شکل ۱۰- معیارهای precision، recall **و** f1-score

همچنین نتایج الگوریتم پیشنهادی با سه الگوریتم SVM، k-نزدیک‌ترین همسایه و درخت تصمیم مقایسه شد که به ترتیب دقت داده‌های آزمون برای SVM معادل ۷۴٪، k-نزدیکترین همسایه برابر با ۶۸٪، برای درخت تصمیم برابر با ۷۲٪ در مقابل دقت ۹۲٪ روش پیشنهادی بود.

۴- نتیجه و جمع بندی

در پژوهش باتوجه به اهمیت برچسب گذاری چندگانه توئیت‌های فارسی این مهم بااستفاده از امبدینگ هشتگ‌ها و کلمات توئیت‌ها به روش Word2Vec بر اساس skip-gram و تراز نمودن نزدیکترین ۳ هشتگ برای هر توئیت انجام

گرفت. سپس با ایجاد یک فضای برداری برای توئیت‌های پیش پردازش شده اقدام پیاده سازی یک شبکه عصبی کانولوشن عمیق جهت طبقه بندی آنها شد. اگرچه عملکرد روش پیشنهادی بسیار بهتر از عملکرد ۳ روش پایه مانند SVM، k-نزدیک‌ترین همسایه و درخت تصمیم بود ولی لازم است در ادامه تحقیق روش پیشنهادی را با سایر روش‌های بهبود یافته که در مقالات اخیر به چاپ رسیده‌اند نیز مقایسه شود. افزایش تعداد دسته‌ها و هشتگ‌ها و توئیت‌های جمع آوری شده و استفاده از روش‌های یادگیری تقویتی می‌توانند بعنوان پیشنهادات آتی پیش روی این پژوهش باشند.

مراجع

[۱] J. Burgess and N. K. Baym, *Twitter: A biography*. NYU Press, 2022.

[۲] N. Kumar, L. Qiu, and S. Kumar, "A hashtag is worth a thousand words: An empirical investigation of social media strategies in trademarking hashtags," *Information Systems Research* ,vol. 33, no. 4, pp. 1403-1427, 2022.

[۳] X. Liu *et al.*, "Developing multi-labelled corpus of twitter short texts: a semi-automatic method," *Systems*, vol. 11, no. 8, p. 390, 2023.

[۴] S. Selva Birunda and R. Kanniga Devi, "A review on word embedding techniques for text classification," *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020*, pp. 267-281, 2021.

[۵] M. D. Samad, N. D. Khounviengxay, and M. A. Witherow, "Effect of text processing steps on twitter sentiment classification using word embedding," *arXiv preprint arXiv:2007.13027*, 2020.

[۶] S. Minaee, N. Kalchbrenner, E. Cambria, N. Nikzad, M. Chenaghlu, and J. Gao, "Deep learning--based text classification: a comprehensive review," *ACM computing surveys (CSUR)*, vol ,۵۴ .no. 3, pp. 1-40, 2021.

[۷] E. M. Dharma, F. L. Gaol, H. Warnars, and B. Soewito, "The accuracy comparison among word2vec, glove, and fasttext towards convolution neural network (cnn) text classification," *J Theor Appl Inf Technol*, vol. 100, no. 2, p.۲۰۲۲ ,۳۱ .

[۸] A. N. Tarekegn, M. Ullah, and F. A. Cheikh, "Deep learning for multi-label learning: A comprehensive survey," *arXiv preprint arXiv:2401.16549*, 2024.

[۹] C. Sahoo, M. Wankhade, and B. K. Singh, "Sentiment analysis using deep learning techniques: a comprehensive review," *International Journal of Multimedia Information Retrieval*, vol. 12, no. 2, p. 41, 2023.

[۱۰] A. Krouska, C. Troussas, and M. Virvou, "Deep learning for twitter sentiment analysis: the effect of pre-trained word embedding," *Machine Learning Paradigms: Advances in Deep Learning-based Technological Applications*, pp. 111-124, 2020.

[۱۱] S. Meftah, N. Semmar, and F. Sadat, "A neural network model for part-of-speech tagging of social media texts," in *LREC 2018-Eleventh International Conference on Language Resources and Evaluation*, 2018 .

مجموعه‌های ۲-احاطه‌گری همبند و چندجمله‌ای‌های ۲-احاطه‌گری همبند در گراف‌های دوستی

حامد محمودزاده [*۱]، سعید محمدیان سمنانی [۲]

۱- گروه ریاضیات، دانشکده ریاضی و آمار و علوم کامپیوتر، دانشگاه سمنان، سمنان، ایران

۲- گروه ریاضیات، دانشکده ریاضی و آمار و علوم کامپیوتر، دانشگاه سمنان، سمنان، ایران

چکیده

فرض کنید $G = (V, E)$ یک گراف ساده باشد. مجموعه $D \subseteq V$ یک مجموعه ۲-احاطه‌گری همبند G است، اگر هر رأس از $V - D$ حداقل به دو رأس در D متصل باشد و $G[D]$ نیز همبند باشد. عدد ۲-احاطه‌گری همبند گراف G با $\gamma_2^c(G)$ نشان داده می‌شود و برابر با کوچک‌ترین اندازه مجموعه‌های ۲-احاطه‌گری همبند گراف G است.

در این مقاله، تعداد مجموعه‌های ۲-احاطه‌گری همبند در گراف G شمارش می‌شود. برای این منظور، چندجمله‌ای تعریف شده که تعداد مجموعه‌های ۲-احاطه‌گری همبند در گراف G را نشان می‌دهد. این چندجمله‌ای با نام چندجمله‌ای ۲-احاطه‌گری همبند شناخته می‌شود. در پایان برخی خواص این چندجمله‌ای مطالعه شده و برای برخی خانواده‌های گراف‌ها، از جمله گراف‌های دوستی F_n این چندجمله‌ای محاسبه شده است.

کلمات کلیدی: ۲-احاطه‌گری همبند، چند جمله‌ای‌های ۲-احاطه‌گری همبند و گراف‌های دوستی

۱. مقدمه

نظریه گراف به عنوان یکی از شاخه‌های قدرتمند و کاربردی ریاضیات گسسته، به بررسی روابط و ساختارهای بین اشیاء مختلف می‌پردازد. در این نظریه، گراف‌ها به صورت مجموعه‌ای از رئوس (نقاط) و یال‌ها (خطوطی که این نقاط را به هم متصل می‌کنند) تعریف می‌شوند. در طی سالیان اخیر، مفاهیم مختلفی در نظریه گراف به‌وجود آمده است که هر کدام به منظور تحلیل دقیق‌تر این ساختارها و کاربردهای آنها در علوم مختلف از جمله شبکه‌های کامپیوتری، تحلیل شبکه‌های اجتماعی، زیست‌شناسی و حتی علوم مهندسی و اقتصادی به کار گرفته شده‌اند.

یکی از این مفاهیم مهم، مجموعه‌های احاطه‌گر است. مجموعه احاطه‌گر، مجموعه‌ای از رئوس یک گراف است که همه رئوس دیگر یا عضو این مجموعه هستند و یا حداقل به یک رأس از این مجموعه متصل می‌باشند. این مفهوم، نه تنها در تحلیل‌های تئوری گراف اهمیت دارد، بلکه در کاربردهای عملی نظیر بهینه‌سازی شبکه‌ها، طراحی شبکه‌های ارتباطی، و حتی در علوم زیستی به کار گرفته می‌شود. در این راستا، مجموعه‌های ۲-احاطه‌گری همبند به عنوان تعمیمی از مفهوم

* **Email: hamedmahmudzade@gmail.com**

احاطه‌گری معرفی شده است. در این نوع احاطه‌گری، نه تنها مجموعه احاطه‌گر باید بتواند تمام رئوس را احاطه کند، بلکه زیرگراف ناشی از این مجموعه نیز باید همبند باشد، یعنی بین هر جفت از رئوس مجموعه یک مسیر وجود داشته باشد.

چندجمله‌ای‌های ۲-احاطه‌گری همبند به عنوان ابزارهای ریاضی، برای توصیف دقیق‌تر و محاسباتی این نوع احاطه‌گری به کار می‌روند. این چندجمله‌ای‌ها به ما امکان می‌دهند تا ویژگی‌های کلی گراف‌ها و رفتار آنها در مواجهه با تغییرات مختلف را مدل‌سازی کنیم. مطالعه این چندجمله‌ای‌ها نه تنها از لحاظ تئوری اهمیت دارد، بلکه کاربردهای مهمی در شبیه‌سازی و طراحی سیستم‌های پیچیده دارد.

در گراف $G = (V, E)$، یک زیرمجموعه $D \subseteq V$ مجموعه ۲-احاطه‌گری همبند است اگر هر رأس از $V - D$ حداقل به دو رأس در D متصل باشد و زیرگراف القاشده $G[D]$ همبند باشد. عدد ۲-احاطه‌گری همبند گراف G، با $\gamma_2^c(G)$ نمایش داده می‌شود و برابر با کمترین اندازه مجموعه‌های ۲-احاطه‌گری همبند در G است [۵,۴,۱].

چندجمله‌ای ۲-احاطه‌گری همبند گراف G به صورت $D_2^c(G, x) = \sum_{i=\gamma_2^c(G)}^{|V(G)|} d_2^c(G, i)x^i$ تعریف می‌شود، که $d_2^c(G, i)$ نشان‌دهنده تعداد مجموعه‌های ۲-احاطه‌گری همبند با اندازه i است [۶,۳,۲]. این چندجمله‌ای خواص متعددی دارد که در مقالات پیشین بررسی شده‌اند.

در این مقاله، برخی ویژگی‌های چندجمله‌ای ۲-احاطه‌گری همبند برای خانواده‌های خاصی از گراف‌ها بررسی می‌شود. تمرکز ما بر روی گراف‌های خاصی از جمله گراف‌های دوستی F_n است، که با افزودن یک رأس مرکزی به یک چرخه و اتصال آن به تمام رئوس چرخه ساخته می‌شوند. این گراف‌ها به دلیل ساختار منحصربه‌فرد و کاربردهای گسترده در نظریه گراف، توجه زیادی را به خود جلب کرده‌اند[۳].

در ادامه، چندجمله‌ای ۲-احاطه‌گری همبند برای این گراف‌ها محاسبه شده و ارتباط آن با سایر پارامترهای گرافی بررسی شده است. نتایج به‌دست‌آمده نشان‌دهنده الگوهای جالب در ساختار گراف‌های دوستی است که می‌تواند زمینه‌ای برای تحقیقات بیشتر باشد. همچنین، نتایج این تحقیق می‌تواند به درک بهتری از خواص پیچیده گراف‌ها در مسائل دنیای واقعی کمک کند.

مجموعه‌های ۲-*احاطه‌گری همبند* زیرمجموعه‌ای از رئوس گراف هستند که دو ویژگی کلیدی دارند:

۱) هر رأس که در این مجموعه نیست، حداقل با دو رأس از این مجموعه مجاور است.

۲) زیرگراف القا شده توسط این مجموعه همبند است، یعنی بین هر دو رأس در این مجموعه مسیری وجود دارد.

به عبارت دیگر، علاوه بر شرط ۲-احاطه‌گری، شرط همبند بودن نیز برای این نوع مجموعه احاطه‌گر برقرار است، که موجب می‌شود تمامی رئوس احاطه‌گر به صورت یکپارچه و بدون انقطاع با یکدیگر در ارتباط باشند.

این مفهوم ترکیبی از ۲-*احاطه‌گری* و *همبندی* است و در کاربردهایی مانند شبکه‌های ارتباطی و بهینه‌سازی منابع استفاده می‌شود، جایی که نیاز به پوشش کامل شبکه و همبندی پایدار اهمیت دارد.

۲.مجموعه های ۲-احاطه‌گری همبند گراف دوستی F_n

در این بخش ابتدا مجموعه‌های ۲-احاطه‌گری همبند گراف F_1، F_2 و F_3 را مورد بررسی قرار داده و سپس برای F_n این مجموعه‌ها را پیدا می‌کنیم.

گراف F_1 یک گراف دوستی است که از ادغام یک مثلث C_3 در یک رأس مشترک تشکیل شده است. این گراف دارای ۳ رأس است که با یکدیگر مجاور هستند. حال برای یافتن مجموعه‌های ۲-احاطه‌گر همبند، ابتدا تعریف را مرور می‌کنیم:

تعریف مجموعه ۲-احاطه‌گر همبند: مجموعه‌ای از رئوس است که هر رأس گراف یا در این مجموعه قرار دارد، یا توسط حداقل دو رأس از این مجموعه احاطه شده و زیرگراف القایی این مجموعه، همبند باقی بماند.

گراف F_1 و رئوس آن:

- رئوس گراف F_1 را با v_1, v_2 و v_3 برچسب گذاری می‌کنیم.
- در این گراف، هر رأس با دو رأس دیگر مجاور است.

یافتن مجموعه‌های ۲-احاطه‌گر همبند:

۱. **مجموعه کامل رئوس:** اگر $D = \{v_1, v_2, v_3\}$ باشد، تمام رئوس گراف در D قرار دارند و به صورت خودکار ۲-احاطه‌گر همبند محسوب می‌شود، زیرا هر رأس توسط رئوس دیگر احاطه شده است و زیرگراف القایی همبند است.

۲. **مجموعه شامل ۲ رأس** :فرض کنید مجموعه D شامل دو رأس از رأس‌های v_1, v_2, v_3 باشد. هر ترکیب از دو رأس مثلاً $D = \{v_1, v_2\}$ یک مجموعه ۲-احاطه‌گر همبند است، زیرا رأس سوم مثلاً v_3 توسط دو رأس v_1 و v_2 احاطه می‌شود و زیرگراف القایی از رئوس D همبند است.

بنابراین، مجموعه‌های ۲-احاطه‌گر همبند برای F_1 به صورت زیر هستند:

- $\{v_1, v_2, v_3\}$
- هر ترکیب دو رأسی مانند $\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}$

گراف F_2 یک گراف دوستی است که از دو مثلث C_3 تشکیل شده و این دو مثلث در یک رأس مشترک (رأس مرکزی v_5) ادغام شده‌اند. این گراف دارای ۵ رأس است و هر رأس با حداقل دو رأس دیگر مجاور است.

برای یافتن مجموعه‌های ۲-احاطه‌گر همبند برای F_2 :

۱. **مجموعه کامل رئوس:** اگر مجموعه D شامل همه ۵ رأس گراف باشد، این مجموعه به صورت خودکار ۲-احاطه‌گر همبند است، زیرا هر رأس احاطه شده و زیرگراف القایی همبند خواهد بود.

۲. **مجموعه‌های شامل ۳ رأس:** هر ترکیب از ۳ رأس شامل رأس مرکزی طوری انتخاب شود که دو رأس دیگر توسط این ۳ رأس احاطه شوند نیز یک مجموعه ۲-احاطه‌گر همبند است. برای مثال، اگر $D = \{v_1, v_3, v_5\}$ باشد، سایر رئوس گراف توسط این مجموعه احاطه می‌شوند و زیرگراف القایی همبند است.

بنابراین مجموعه‌های ۲-احاطه‌گر همبند برای F_2 شامل موارد زیر می‌شوند:

- $\{v_1, v_2, v_3, v_4, v_5\}$
- هر ترکیب ۳ رأسی مانند $\{v_2, v_4, v_5\}, \{v_1, v_4, v_5\}$، که سایر رئوس را احاطه کنند.

شمارش مجموعه‌های ۲-احاطه‌گر همبند برای F_3 :

گراف F_3 یک گراف دوستی است که از سه مثلث C_3 تشکیل شده و این سه مثلث در یک رأس مشترک (رأس مرکزی) ادغام شده‌اند. این گراف دارای ۷ رأس است و هر رأس با حداقل دو رأس دیگر مجاور است.

برای یافتن مجموعه‌های ۲-احاطه‌گر همبند برای F_3:

- **رأس مرکزی** باید همیشه در مجموعه باشد. بدون رأس مرکزی، مجموعه نمی‌تواند همبند باشد.
- **انتخاب رئوس از هر مثلث:** در F_3، سه مثلث داریم. از هر مثلث باید حداقل یک رأس دیگر را برای تضمین احاطه‌گری انتخاب کنیم. این انتخاب‌ها به شکل زیر است:
  - در هر مثلث، می‌توانیم یکی از دو رأس غیر مرکزی را انتخاب کنیم. برای هر مثلث دو انتخاب داریم.
  - پس تعداد کل انتخاب‌های ممکن برای سه مثلث برابر است با ۸=۲×۲×۲.

در نتیجه مجموعه‌های ۲-احاطه‌گر همبند در F_3 شامل رأس مرکزی و یکی از دو رأس دیگر از هر مثلث است. تعداد کل مجموعه‌های ممکن برابر با ۸ مجموعه است.

برای گراف دوستی F_n با n مثلث: گراف دوستی F_n شامل n مثلث است که همگی دارای یک رأس مرکزی مشترک (v_{2n+1}) هستند. این گراف‌ها دارای $2n+1$ رأس و $3n$ یال هستند.

- برای هر مثلث همچنان دو انتخاب وجود دارد (یکی از دو رأس غیر مرکزی).
- پس تعداد کل مجموعه‌های ۲-احاطه‌گر همبند برای F_n برابر است با 2^n.

گام‌های بدست آوردن مجموعه‌های ۲-احاطه‌گر همبند:

۱. **انتخاب رأس مرکزی:** برای حفظ همبندی باید رأس مرکزی (که در تمام مثلث‌ها مشترک است) در مجموعه D باشد.

۲. **انتخاب رئوس دیگر:** برای هر مثلث می‌توان یک یا دو رأس به مجموعه اضافه کرد تا شرط ۲-احاطه‌گری تأمین شود.

- **استدلال ترکیبیاتی:** در گراف‌های بزرگ‌تر، با افزایش تعداد مثلث‌ها یعنی افزایش n، تعداد ترکیبات ممکن برای انتخاب رئوس در مجموعه D افزایش می‌یابد، اما شرط‌های همبندی و ۲-احاطه‌گری همچنان برقرار می‌ماند. به این ترتیب می‌توان برای هر گراف F_n مشابه روندی که در F_3 انجام شد، مجموعه‌های ۲-احاطه‌گر همبند را پیدا کرد.

۳. عدد ۲-احاطه‌گری همبند گراف دوستی F_n

برای تعیین عدد ۲-احاطه‌گری همبند گراف دوستی F_n، قضیه زیر را به طور دقیق بیان می‌کنیم:

قضیه۱.

برای هر $n \geq 1$، عدد ۲-احاطه‌گری همبند گراف دوستی F_n برابر با $\gamma_2^c(F_n) = n+1$ است.

اثبات.

گراف دوستی F_n از یک رأس مرکزی v_{2n+1} و n مثلث تشکیل شده است، به‌گونه‌ای که هر مثلث شامل رأس مرکزی و دو رأس دیگر است.

گام ۱: ساخت مجموعه ۲-احاطه‌گر

ابتدا رئوس گراف را $v_1, v_2, \dots, v_{2n+1}$ می‌نامیم. واضح است که ببینیم مجموعه $\{v_1, v_3, \dots, v_{2n-1}, v_{2n+1}\}$ یک مجموعه ۲-احاطه‌گر است. زیرا:

- هر رأس v_i یا در مجموعه است یا توسط حداقل دو رأس دیگر در همسایگی آن پوشش داده می‌شود.

پس $\gamma_2^c(F_n) \leq n+1$.

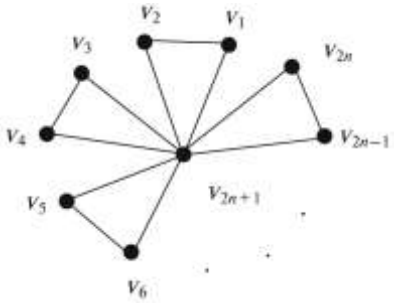
گام ۲: نشان دادن کران پایین

حال فرض کنید D یک مجموعه ۲-احاطه‌گر همبند با اندازه $|D| \leq n$ باشد. باید اثبات کنیم چنین مجموعه‌ای وجود ندارد.

- حالت ۱: اگر رأس مرکزی v_{2n+1} در D باشد، آنگاه برخی از رئوس $V(F_n)$ نمی‌توانند توسط دو رأس مجاور احاطه شوند.
- حالت ۲: اگر v_{2n+1} در D نباشد، طبق شکل(۱) و تعریف ۲-احاطه‌گری، نمی‌توان مجموعه‌ای یافت که تمامی رئوس را احاطه کند.

بنابراین، برای اینکه تمامی رئوس پوشش داده شوند و مجموعه همبند باشد، باید $|D| \geq n + 1$ باشد.

نتیجه می‌گیریم که $\gamma_2^c(F_n) = n + 1$



شکل ۱ – گراف دوستی F_n برچسب گذاری شده

۴.چندجمله‌ای‌های ۲-احاطه‌گری همبند گراف دوستی F_n

در این بخش ابتدا چندجمله‌ای ۲-احاطه‌گری همبند گراف F_1 را پیدا کرده و سپس برای F_n این چندجمله‌ای را به‌دست می‌آوریم.

قضیه ۲. برای گراف F_1 داریم:

$$D_2^C(F_1, x) = \sum_{i=2}^{3} d_2^c(F_1, i)x^i = x^3 + 3x^2 \qquad (1)$$

اثبات.

F_1 معادل C_3 است که چرخه‌ای با مرتبه ۳ می‌باشد. از آنجا که $\gamma_2^c(F_1) = 2$ و داریم:

$d_2^c(F_1, 2) = 3$ و $d_2^c(F_1, 3) = 1$

بنابراین، طبق تعریف، چندجمله‌ای ۲-احاطه‌گری همبند برای گراف F_1 را می‌توان به صورت زیر محاسبه کرد:

$$D_2^C(F_1, x) = \sum_{i=2}^{3} d_2^c(F_1, i)x^i = x^3 + 3x^2$$

قضیه زیر را که در اثبات قضیه ۴ به آن نیاز داریم نیز بیان می‌کنیم

قضیه ۳.

برای هر $n \geq 3$،

$$D_2(C_n, x) = \sum_{i=0}^{n} \left[\binom{n-i}{i} + \binom{n-i-1}{i-1} \right] x^{n-i} \qquad (2)$$

اثبات. فرض کنید رأس‌های چرخه C_n با $v_1, v_2, \dots, v_n$ برچسب‌گذاری شده‌اند. با حذف یال v_1v_n، مسیر P_n با رأس‌های $v_1, v_2, \dots, v_n$ را در نظر می‌گیریم. حال، مجموعه D را به عنوان یک مجموعه ۲-احاطه‌گر از P_n فرض می‌کنیم. برای شمارش مجموعه‌های ۲-احاطه‌گر، دو حالت را بررسی می‌کنیم:

حالت ۱: اگر $v_1, v_n \in D$، تمام حالات ممکن برای انتخاب رأس‌های مجموعه $\{v_2, v_3, \dots, v_{n-1}\}$ در D بررسی می‌شود. در این حالت، تعداد مجموعه‌های ۲-احاطه‌گر $d_2(C_n, i) = \binom{n-i-1}{i-1}$ برای مسیر P_n به دست می‌آید، که در آن $0 \le i \le n$ است.

حالت ۲: رأس v_{n+1} را با اضافه کردن یال v_nv_{n+1} به مسیر P_n اضافه می‌کنیم. با توجه به تعریف مجموعه ۲-احاطه‌گر، v_1 و v_{n+1} باید در D باشند. بنابراین، با استدلال مشابه حالت ۱ برای مسیر P_{n-1}، تعداد مجموعه‌های ۲-احاطه‌گر $d_2(C_n, i) = \binom{n-i}{i}$ برای $0 \le i \le n$ به دست می‌آید [۳,۵,۶].

در نتیجه با در نظر گرفتن هر دو حالت و تعریف چندجمله‌ای ۲-احاطه‌گری چرخه C_n، نتیجه نهایی حاصل می‌شود.

برای یافتن چندجمله‌ای دقیق ۲-احاطه‌گری همبند در گراف دوستی F_n، نیاز داریم که علاوه بر ۲-احاطه‌گر بودن، همبندی مجموعه ۲-احاطه‌گر را نیز لحاظ کنیم. یعنی هر مجموعه ۲-احاطه‌گر همبند باید به گونه‌ای انتخاب شود که اتصال بین رأس‌های آن حفظ شود.

قضیه ۴.

برای هر $n \ge 2$، چندجمله‌ای ۲-احاطه‌گری همبند F_n به‌صورت زیر محاسبه می‌شود:

$$D_2^C(F_n, x) = x^{2n+1} + (2n+1)x^{2n} + \sum_{i=0}^{n-2}\binom{n}{i}2^{n-i}x^{(n+1)+i}. \quad (3)$$

اثبات. موارد زیر اثبات را کامل می‌کند:

۱. حضور رأس مرکزی v_{2n+1}: رأس v_{2n+1} باید در هر مجموعه ۲-احاطه‌گر همبند حضور داشته باشد، زیرا این رأس به تمامی زیرگراف‌های مثلثی متصل است و نقش کلیدی در تضمین همبندی مجموعه ۲-احاطه‌گر ایفا می‌کند.

۲. شرایط هر مثلث :طبق اصل لانه کبوتری، در هر مجموعه ۲-احاطه‌گر همبند، باید حداقل یک رأس از هر مثلث انتخاب شود. به این ترتیب، می‌توانیم مطمئن شویم که تمامی رأس‌های مثلثی به یکدیگر و به رأس مرکزی متصل هستند و همبندی حفظ می‌شود.

۳. تعداد حالات برای هر مقدار i: برای هر i با استفاده از ترکیب‌بندی و اصل لانه کبوتری، تعداد حالات ممکن به صورت $\binom{n}{i}2^{n-i}$ برای حفظ همبندی محاسبه می‌شود.

۴. حالات خاص:
   - برای $i = 2n$، تعداد مجموعه‌های ۲-احاطه‌گر همبند $2n + 1$ است.
   - برای $i = 2n + 1$، تنها یک مجموعه ۲-احاطه‌گر همبند وجود دارد.

بنابراین، چندجمله‌ای نهایی ۲-احاطه‌گری همبند به صورت زیر نتیجه می‌شود و همبندی مجموعه‌ها در هر مرحله تضمین می‌شود.

$$D_2^C(F_n, x) = x^{2n+1} + (2n+1)x^{2n} + \sum_{i=0}^{n-2}\binom{n}{i}2^{n-i}x^{(n+1)+i} \quad (3)$$

۵. نتیجه‌گیری

نتیجه‌ی زیر مشابه رابطه (۳) در قضیه (۴)، با تغییرات زیر بازنویسی می‌شود.

نتیجه ۱.

برای هر $n \geq ۲$، چندجمله‌ای ۲-احاطه‌گری همبند $D_۲^C(F_n, x)$ به صورت زیر محاسبه می‌شود:

$$D_۲^C(F_n, x) = x^{۲n+۱} + \sum_{i=۱}^{n-۱}\left[\binom{۲n-i}{i} + \binom{۲n-i-۱}{i-۱} + \binom{n}{i-۱}\right] x^{(۲n+۱)-i} + ۲^n x^{(n+۱)} \quad (۴)$$

اثبات.

۱. حضور رأس مرکزی $v_{۲n+۱}$: طبق ساختار F_n، رأس مرکزی $v_{۲n+۱}$ باید در هر مجموعه ۲-احاطه‌گر همبند وجود داشته باشد. این شرط به ما اطمینان می‌دهد که همبند بودن مجموعه ۲-احاطه‌گری حفظ می‌شود.

۲. تعداد مجموعه‌های ۲-احاطه‌گر همبند با تعداد رأس‌های مشخص:

- برای $i = n + ۱$، تعداد مجموعه‌های ۲-احاطه‌گر همبند برابر با ۲^n است.
- برای $i = ۲n + ۱$، تنها یک مجموعه ۲-احاطه‌گر همبند وجود دارد.
- برای $n + ۲ \leq i \leq ۲n - ۱$، با در نظر گرفتن همبندی، گراف F_n را به عنوان چرخه $C_{۲n}$ می‌توان در نظر گرفت که در آن برخی یال‌ها حذف شده‌اند. با استفاده از روش اثبات قضیه ۳ و استقراء، تعداد مجموعه‌های ۲-احاطه‌گر همبند به دست می‌آید.

بنابراین، با در نظر گرفتن این شرایط و تعداد مجموعه‌های ممکن، چندجمله‌ای $D_۲^C(F_n, x)$ مطابق فرمول (۲) نتیجه می‌شود.

مراجع

[۱] S. Alikhani, Y.H. Peng, Dominating Sets and Domination Polynomial of Certain Graphs, submitted.propagation using the extended finite element method," *International journal for numerical methods in engineering*, vol.٦٣,pp.٧٦٠-٧٨٨, ٢٠٠٥.

[۲] S P.C. Priyanka Nair, T. Anitha Baby, V.M. Arul Flower Mary, ٢-Dominating sets and ٢- Domination Polynomials of Paths, Journal of Shanghai Jiaotong University ١٦(٢٠٢٠),٤٢-٥١.

[۳] P.C. Priyanka Nair, T. Anitha Baby, ٢-Dominating sets and ٢-Domination Polynomials of Cycles, Adalya Journal, ٩(١١)(٢٠٢٠), ١٨٢-١٩٤.

[٤] S. Alikhani, Dominating Sets and domination Polynomials of Graphs, Ph.D.Thesis, University Putra Malaysia, March ٢٠٠٩.

[٥] S. Alikhani and Y. Peng, “Dominating sets and domination polynomial of cycles,” Global J. Pure Appl.Math. ٤,١٥١–١٦١(٢٠٠٨).

[٦] F. Movahedi and M. H. Akhbari and S. Alikhani , “The Number of ٢-dominating Sets, and ٢-domination Polynomial of a Graph Dominating sets and domination polynomial of cycles,” Lobachevskii Journal of Mathematics. *Vol. ٤٢, No. ٤, pp. ٧٥١–٧٥٩, ٢٠٢١.*

رابطه ی بین مساله های موقعیت عمومی و موقعیت عمومی یال

راضیه اباذری [۱]، غلامحسن شیردل[۲].

۱- دانشجوی کارشناسی ارشد، ریاضی کاربردی دانشگاه قم r7_abazari@yahoo.com

۲- استاد، گروه علوم کامپیوتر دانشگاه قم shirdel81math@gmail.com

چکیده

مساله های موقعیت عمومی و موقعیت عمومی یال به ترتیب به یک ویژگی مهم در راس ها و یال های گراف می پردازند. این دو مساله در مطالعات متعددی به صورت جداگانه مورد بررسی قرار گرفته اند ولی تا کنون ارتباطی بین آن ها برقرار نشده است. در این مقاله با استفاده از ارتباط بین رنگ آمیزی راسی و یالی، دو مقاله ی ذکر شده به هم مرتبط می شوند.

کلمات کلیدی: نظریه گراف، م ساله ی موقعیت عمومی، م ساله ی موقعیت عمومی یال، گراف یالی. رنگ آمیزی گراف

۱. مقدمه

موقعیت عمومی یک حالت خاص و مهم در ریاضیات است و زمانی رخ می دهد که هیچ زیرمجموعه از اشیاء به طور خطی وابسته نباشند. این مفهوم به ویژه در هندسه و جبرخطی اهمیت دارد.

در هندسه گسسته مساله هیچ سه نقطه در خط در یک شبکه ی $n\times n$ برای پیدا کردن نقاطی استفاده می شود که هیچ سه نقطه ای روی یک ردیف یا ستون قرار نگیرد. مساله ی انتخاب زیرمجموعه ی موقعیت عمومی به بررسی این مساله در صفحه ی مختصات می پردازد که در آن هیچ سه نقطه ای نباید هم خط باشد یعنی روی یک خط قرار داشته باشد.

در نظریه گراف مساله موقعیت عمومی برای مدلسازی مسائلی استفاده می شود که دقیقا یک رابطه ی دوتایی روی مسیرها در گراف مدنظر است نه بیشتر. تا سال ها مطالعات صورت گرفته فقط به نسخه ی راسی آن می پرداخت. در سال های اخیر نسخه ی یالی از آن نیز مورد مطالعه قرار گرفته است. در مقاله پیش رو به دنبال یافتن ارتباطی بین این دو مساله

هستیم. با توجه به اینکه این دو مساله از لحاظ تعریف متفاوت می باشند و به ظاهر ارتباطی باهم ندارند با استفاده از گراف یالی می توان میان آن ها رابطه برقرار کرد.

۲. مساله ی موقعیت عمومی

مساله های هیچ سه نقطه در خط و انتخاب زیرمجموعه ی موقعیت عمومی منجر به تعریف مساله ی مشابهی در نظریه ی گراف شد این مساله در [1] معرفی شده است که در ادامه به آن اشاره می کنیم. اگر $G = (V(G).E(G))$ یک گراف باشد، هدف مساله موقعیت عمومی، پیدا کردن بزرگترین مجموعه از راس ها $S \subseteq V(G)$ می باشد و gp-set نامیده می شود، به طوری که هیچ راسی از S در کوتاهترین مسیر ممکن بین دو راس دیگر از S قرار نگیرد به عبارت دیگر هیچ کوتاهترین مسیری از G شامل سه راس از S نباشد. عدد موقعیت عمومی گراف G، gp(G) ، اندازه ی مجموعه ی gp-set است. در این مقاله مساله ی موقعیت عمومی (راسی) به اختصار gpp نامیده می شود.

۳. مساله ی موقعیت عمومی یال

نسخه ی یال از gpp در [2] معرفی شده است. این مساله در این مقاله به اختصار egpp نامگذاری شده که در ادامه بیان می شود. یک زیر مجموعه S از یال های گراف G موقعیت عمومی یال نامیده می شود، اگر هیچ کوتاهترین مسیری از G وجود نداشته باشد که شامل سه یال از S باشد. بیشترین اندازه ی مجموعه موقعیت عمومی یال، gp_e-set گراف نامیده می شود.

۴. گراف یالی

در [3] گراف یالی تعریف شده است به این صورت که گراف یالی بدست آمده از یک گراف G، گرافی است با مجموعه راس های E(G) که در آن دو راس به هم متصل می شوند اگر و فقط اگر در G یال های مجاور باشند.

خصوصیات یک گراف G که تنها به هم‌جواری بین یال‌ها وابسته است، می‌تواند به خصوصیات معادل در L(G) که به هم‌جواری بین راس ها وابسته باشد، تبدیل شود. به عنوان مثال، یک تطابق در G مجموعه‌ای از یال‌هاست که هیچ دو یالی مجاور نیستند و معادل با مجموعه‌ای از راس ها در L(G) است که هیچ دو راسی مجاور نباشند، یعنی یک مجموعه مستقل.

در [4] هر رنگ آمیزی یالی از گراف G یک رنگ آمیزی راسی از L(G) آن است، و برعکس. مخصوصا

$$\chi(G) = \chi'(L(G))$$

گراف G همبند است اگر و فقط اگر L(G) همبند باشد. یعنی اگر مسیری در G وجود داشته باشد آن مسیر در L(G) هم هست.

۶. نتیجه‌گیری

gpp و egpp هردو مورد بحث روی مسیرهای گراف G هستند. در ساختار L(G) مسیرهای G حفظ می شوند. علاوه براین در egpp یک ویژگی هم جواری یال ها مدنظر است می تواند به خصوصیات معادل در L(G) آن با هم جواری بین راس ها تبدیل شود که L(G) همان gpp گراف خواهد بود. به این نتیجه می رسیم که مساله gpp در یک گراف G، می تواند به مساله egpp گراف L(G) تبدیل شود.

۷. مراجع

[1] P. Manuel, S. Klavˇzar, A general position problem in graph theory, Bull. Aust. Math. Soc. 98 (2018) 177–187.

[2] P. Manuel R. Prabha S. Klavˇzar, Edge General Position Problem, (2021)

[3] J. A. Bondy and U. S. R. Murty, "GRAPH THEORY WITH APPLICATIONS," Depart,nent· of Combinatorics and Optimization, University of Waterloo, Ontario, Canada, p 11, 1976.

[4] R. Diestel, " GRAPH THEORY ,"ch 5, p 124, 2024 .[Online].Available: https://diestel-graph-theory.com/basic.html

نهمین کنفرانس بین‌المللی
ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات
۵ و ۶ دی ۱۴۰۳

تعمیر و نگهداری پیشگیرانه با استفاده از الگوریتم یادگیری تقویتی کیو

فاطمه حسن‌تبار درزی[۱]
عضو هیأت علمی گروه آمار، دانشگاه سیستان و بلوچستان، زاهدان، ایران

چکیده

برای تعمیر و نگهداری پیشگیرانه بر اساس یادگیری تقویتی که در این مقاله پیشنهاد شده است، دو پیکربندی مختلف سری و موازی برای یک سیستم دو مؤلفه‌ای در نظر گرفته شده است. هدف یافتن اقدامات بهینه نگهداری در یک افق زمانی با حداقل‌سازی هزینه‌ها است. توزیع وایبل برای مدل کردن فرسایش هر یک از مؤلفه‌های سیستم در نظر گرفته شده است. عمل تعمیر و نگهداری پیشگیرانه بهینه برای هر مؤلفه با مدل کردن مسئله به عنوان فرآیند تصمیم مارکوف و حل آن با استفاده از الگوریتم یادگیری–کیو انجام شده است. در انتها با استفاده از شبیه‌سازی نشان داده شده است چگونه می‌توان از یادگیری تقویتی برای عملیات تعمیر و نگهداری بهینه استفاده کرد.

واژه‌های کلیدی: الگوهای تعمیر و نگهداری پیشگیرانه، توزیع وایبل، یادگیری تقویتی، الگوریتم کیو–لرنینگ.

[2010]: 13D45, 39B42

۱ مقدمه

سیستم‌های صنعتی به طور کلی به دلیل استفاده و قرارگرفتن در معرض عوامل محیطی، دچارتخریب می‌گردند. این تخریب در نهایت منجر به خرابی سیستم شده و در نتیجه مشکلات ایمنی، آسیب به تجهیزات، مشکلات کیفیت و در دسترس نبودن غیرمنتظره دستگاه را به وجود می‌آورد. در دهه‌های گذشته تعمیر و نگهداری [۲] بعد از خرابی سیستم در نظر گرفته می‌شد که در خیلی از موارد کار تشخیص و تعمیر سخت و غیرممکن می‌گردید. به طور سنتی عملیات تعمیر و نگهداری به دو دسته تعمیر و نگهداری اصلاحی [۳] (CM) و تعمیر و نگهداری پیشگیرانه [۴] (PM) دسته‌بندی می‌شوند [۱]. در تعمیر و نگهداری اصلاحی، قطعه خراب، تعویض می‌گردد در صورتیکه در نوع پیشگیرانه مجموعه عواملی که ریسک خرابی را کاهش دهد در نظر گرفته می‌شود.

در دنیای امروز، بهینه‌سازی استراتژی‌های تعمیر و نگهداری سیستم‌ها به‌ویژه در صنایع پیچیده و حیاتی از اهمیت بالایی برخوردار است. یادگیری تقویتی [۵] (RL) به‌عنوان یک روش نوین در حل مشکلات تصمیم‌گیری‌های پیچیده، نقش مهمی در بهبود کارایی و کاهش هزینه‌های تعمیر و نگهداری ایفا می‌کند. RL زیر شاخه‌ای از یادگیری ماشین در هوش مصنوعی می‌باشد که با یادگیری از تکرار تعامل با محیط سر و کار دارد [۳]. یوسفی و همکاران [۵] از الگوریتم یادگیری–کیو در RL برای تعمیر و نگهداری مبتنی بر شرایط استفاده کردند. مطالعات دیگری که در زمینه الگوهای تعمیر و نگهداری مبتنی بر شرایط وجود دارد می توان به رافی و همکاران [۹]، چن و همکاران [۷] و گوبر و همکاران [۸] اشاره کرد. با اینکه الگوهای تعمیر و نگهداری سیستم‌ها با توجه به پیشرفت بشر در صنایع پیچیده مدت‌ها است مورد توجه قرارگرفته است اما استفاده از روش‌های یادگیری تقویتی اخیراً مورد توجه قرارگرفته است و توانسته تأثیرات شگرفی در این زمینه ایجاد کند. استفاده از RL در الگوهای تعمیر و نگهداری سیستم‌ها را می‌توان در کارهای [۴] ، [۶] و [۲] بررسی کرد.

[۱] سخنران

[2] Maintenance
[3] Corrective Maintenance
[4] Preventive Maintenance
[5] Reinforcement Learning

این مقاله، به بررسی بهینه‌سازی استراتژی‌های تعمیر و نگهداری سیستم‌های دو مؤلفه‌ای با استفاده از RL می‌پردازد. مدل پیشنهادی با استفاده از الگوریتم یادگیری کیو [۶] به شبیه‌سازی تصمیمات مختلف در شرایط مختلف سیستم پرداخته است. هدف مدل، کاهش هزینه‌های کلی نگهداری و زمان توقف سیستم با تعیین سیاست‌های بهینه برای تعمیرات پیشگیرانه است. در مدل پیشنهادی، سیستم به طور مستمر از تجربیات خود یاد می‌گیرد تا تصمیمات بهتری در آینده اتخاذ کند. بطور خلاصه، مسئله تعمیر و نگهداری سیستم‌ها با فرایند مارکف مدل می‌گردد و سعی در حل آن با استفاده از RL شده است. در واقع مدل پیشنهادی می‌تواند بهترین تصمیم در هر لحظه را با مدل کردن فضای حالتی که برای سیستم رخ می‌دهد و همچنین مجموعه عوامل پیدا کند.

در ادامه در بخش ۲ مدل‌های یادگیری–کیو در RL توضیح داده می‌شوند. سپس مدل‌های تعمیر و نگهداری، به‌عنوان یک فرایند تصمیم‌گیری مارکف در بخش ۳ مدل می‌گردد تا با استفاده از روش‌های RL بتوان بهترین تصمیم را در هر بازرسی اتخاذ نمود. در انتها در بخش ۴ نتایج مطالعات و شبیه‌سازی برای یک سیستم دو مؤلفه‌ای با پیکربندی مختلف ارائه شده است.

۲ یادگیری کیو

در یادگیری تقویتی فرایند تصمیم‌گیری عامل، با کمک فرایند مارکوف تعریف می‌شود. شرط خاصیت مارکوف عبارتند از:

$$Pr(S_{t+1}|S_t, S_{t-1}, \ldots, S_1) = Pr(S_{t+1}|S_t). \quad (1)$$

طبق رابطه‌ی (۱) فرایندی تصادفی دارای خاصیت مارکوف است، اگر هر حالت فقط به حالت قبل از خودش وابسته باشد. اگر به فرایند مارکوف، عمل و پاداش دریافتی از آن عمل اضافه شود، فرایند تصمیم مارکوف به وجود می‌آید. رابطه‌ی (۲) فرایند تصمیم مارکوف را نشان می‌دهد.

$$Pr(S_{t+1}, r_t|S_t, \ldots, S_1, a_t, \ldots, a_1) = Pr(S_{t+1}, r_t|S_t, a_t) \quad (2)$$

طبق رابطه‌ی (۲) احتمال‌رفتن به حالت S_{t+1} و دریافت پاداش r_t فقط به حالت و عمل قبل بستگی دارد. چندگانه (S, A, P, R, γ) فرایند تصمیم مارکوف است که در آن، S مجموعه‌ی تمام حالت‌های محیط است و فضای حالت نامیده می‌شود. A مجموعه‌ی تمام عمل‌هایی است که عامل می‌تواند در محیط انجام دهد، به این مجموعه فضای عمل گویند. P تابع توزیع تغییر حالت محیط را مشخص می‌کند. R تابعی است از $R : S \times A \longrightarrow R$ و پاداش است که عامل بعد از انجام هر عمل دریافت می‌کند. $\gamma \in [0, 1]$ فاکتور تخفیف است که به منظور همگرا شدن سری پاداش تجمعی استفاده می‌شود. زیربنای یادگیری تقویتی، مبتنی بر پاداش دریافتی از محیط است. پاداش یک عدد اسکالر هست و مشخص می‌کند که عمل عامل در حالت t چقدر خوب بوده است. مجموع پاداش‌های دریافتی در آینده یعنی از حالت t به بعد و با G_t نشان داده می‌شود که در رابطه‌ی (۳) آورده شده است. به G_t بازده و یا پاداش تجمعی گویند. پاداش تجمعی یک دید بلند مدت به عامل می‌دهد. عامل باید به سمت سیاستی حرکت کند تا پاداش تجمعی خود را بیشینه سازد.

$$G_t = r_t + \gamma r_{t+1} + \gamma^2 r_{t+2} + \cdots + \gamma^k r_{t+k}, \quad (3)$$

در رابطه‌ی فوق، r_t ، پاداش دریافتی از محیط بعد از انجام عمل a_t است.

تابع کیو (تابع ارزش حالت –عمل)، میانگین مجموع پاداش‌هایی که عامل با شروع از حالت s و با انجام عمل a می‌تواند در آینده به دست می‌آورد را برمی‌گرداند. به عبارتی این تابع مشخص می‌کند، عامل با انجام عمل a در حالت s انتظار دارد در آینده چه میزان پاداش به دست آورد. تعریف تابع کیو در ادامه آورده شده است.

$$Q(s_t, a_t) = E\big[\sum_{k=0}^{\infty} \gamma^k r_{t+k} | s = s_t, a = a_t\big]. \quad (4)$$

با استفاده از رابطه‌ی بلمن می‌توان تابع کیو را به‌صورت بازگشتی بصورت زیر بازنویسی کرد؛

$$Q(s_t, a_t) = E[r_t + \gamma Q(s_{t+1}, a_{t+1})], \quad (5)$$

[6] Q-Learning

که r_t پاداش بدست آمده در مرحله‌ی tام و $Q(s_{t+1}, a_{t+1})$ تابع کیو برای حالت و عمل مرحله‌ی بعد است. در الگوریتم یادگیری کیو برای بهبود و بروزرسانی تابع کیو بصورت زیر عمل می‌گردد.

$$Q_{t+1}(s_t, a_t) = Q_t(s_t, a_t) + \alpha_t(s_t, a_t)(r_t + \gamma \max_a Q_t(s_{t+1}, a') - Q_t(s_t, a_t)) \quad (۶)$$

که α نرخ یادگیری الگوریتم را مشخص می‌کند. تصمیم عامل در الگوریتم یادگیری-کیو مطابق $\pi(S_t) = \max_a Q_t(s_t, a)$ بدست می‌آید که $\pi(\cdot)$ سیاست عامل نامیده می‌شود. سیاست در هر حالت مشخص می‌کند کدام عمل انتخاب گردد. تصمیم عامل، عملی است که بالاترین مقدار تابع کیو را داشته باشد. البته در فرایند یادگیری برای اکتشاف بیشتر، گاهی عملی به صورت تصادفی انتخاب می‌گردد.

۳ بیان مسئله تعمیر و نگهداری سیستم‌ها با استفاده از فرایند تصمیم‌گیری مارکف

فرایند تصمیم‌گیری مارکوف برای مدل‌بندی وضعیت فرسایش سیستم‌ها در مسئله تعمیر و نگهداری استفاده می‌گردد. در واقع با استفاده از الگوریتم یادگیری تقویتی می‌توان برنامه‌ریزی پویایی برای تعمیر و نگهداری سیستم‌هایی که در طول زمان دچار خرابی می‌شوند انجام داد. یادگیری تقویتی، مجموعه الگوریتم‌هایی است که بر مبنای پاداش دادن به رفتارهای مطلوب سعی در یافتن بهترین عمل برمی‌آید. عامل و محیط دو جزء اصلی روش‌های یادگیری تقویتی هستند. فرایند یادگیری تقویتی با شناسایی وضعیت سیستم و ارسال آن به عامل توسط محیط شروع می‌شود و براساس دانشی که توسط عامل به دست می‌آید، عملی انجام می‌دهد سپس بر اساس عملی که عامل انتخاب می‌کند محیط پاداش و حالت بعدی را محاسبه می‌کند و عامل با اطلاعات برگردانده شده توسط محیط دانش را به روز می‌کند و اخرین اقدام را ارزیابی می‌کند. این رویه به طور مکرر در یک حلقه تا زمانی که محیط به حالت پایانی برسد ادامه می‌یابد. کل فرایند به عنوان یک فرایند تصمیم‌گیری مارکف مدل‌سازی می‌شود که می‌تواند مشکل یادگیری از تعاملات برای دستیابی به یک هدف را حل کند و می‌تواند یک سیستم دینامیکی تصادفی را توصیف کند.

همان‌طور که بیان کردیم مؤلفه‌های سیستم معمولاً با گذشت زمان دچار تخریب می‌گردد و نیازمند یکسری عملیات تعمیر و نگهداری هستند. در الگوهای نگهداری پیشگیرانه، یک سیستم پیش از آنکه دچار شکست گردد، بر اساس شیوه‌ای معین تعویض شده یا مورد بررسی و تعمیر قرار می‌گیرد. فرضیه‌های زیر، برای مدل تعمیر و نگهداری پیشگیرانه یک سیستم در نظر گرفته می‌شود:

- توزیع وایبل برای طول‌عمر سیستم در نظر گرفته می‌شود، بطوریکه:

$$F_T(t) = ۱ - e^{-(\frac{t}{\eta})^\beta}, \quad t \geq ۰.$$

برای حل مسئله PM با استفاده از الگوریتم‌های RL باید این مسئله بصورت یک فرایند مارکف بیان شود. لذا داریم:

۱. فضای حالت سیستم بصورت $S = \{۱, ۲, ۳\}$ تعریف می گردد و نشان دهنده وضعیت مؤلفه سیستم می‌باشد و سه حالت سالم، فرسوده و تخریب شده برای هر مؤلفه در نظر گرفته شده است. به عبارتی

$$S = \begin{cases} ۱ & if \quad X_i(t) \quad be \quad Healthy \\ ۲ & if \quad X_i(t) \quad be \quad Degredaed \\ ۳ & if \quad X_i(t) \quad be \quad failed \end{cases}$$

۲. فضای عمل بصورت $A = \{a_۱, a_۲\}$ می باشد که $a_i, i = ۱, ۲$ها شامل هیچ کاری انجام نشود، تعمیر می‌باشد.

$$A = \begin{cases} ۰ & Do \quad Nothing \\ ۱ & Repaire \end{cases}$$

۳. برای بیان احتمال انتقال وضعیت‌های سیستم فرض می‌شود که سطح تخریب مؤلفه‌های سیستم نتواند در وضعیت اولیه بماند. لذا مؤلفه‌ای که در وضعیت سالم است می‌تواند به هریک از وضعیت‌های ۲ یا ۳ منتقل شود. به منظور یافتن احتمال انتقال به هر یک از وضعیت‌ها، سیستم نباید خرابی سختی را تجربه کند چون خرابی سخت موجب انتقال مستقیم مؤلفه به وضعیت ۳ و باقی ماندن در آن شرایط می‌گردد.

۴. تابع پاداش بر اساس منفی تابع هزینه تعریف می‌گردد. که C_{PM} هزینه تعمیر و نگهداری پیشگیرانه، C_{CM} هزینه تعمیر و نگهداری اصلاحی و C_ρ هزینه جریمه برای خرابی است. متغیر تصادفی باینری ω برای نمایش وضعیت خرابی مؤلفه در نظر گرفته شده است.

$$\begin{aligned} C_t &= \sum_{i=۱}^{n}(C_{PM}\sigma_{i۱} + C_{CM}\sigma_{i۲}) + C_\rho\omega \\ R_t &= -C_t. \end{aligned}$$

هدف از استفاده از یادگیری تقویتی و فرایند مارکف برای مشکل تعمیر و نگهداری، ارائه بهترین سیاست تعمیر و نگهداری است که حداقل هزینه را داشته باشد. چگونگی تعمیر و نگهداری بهینه با یافتن بهترین Q–مقدار برای هر حالت از سیستم تعیین می‌شود، که نشان می‌دهد چه اقدامات نگهداری باید برای هر حالت تخریب در هر زمان بازرسی اجرا شود.

۴ شبیه‌سازی و نتایج

برای تعمیر و نگهداری پیشگیرانه بر اساس یادگیری تقویتی که در این مقاله پیشنهاد شده است، دو پیکربندی مختلف سری و موازی برای یک سیستم در نظر گرفته شده است. در سیستم سری با n جزء، اگر جزء i خراب شود، کل سیستم از کار می افتد. در حالیکه در سیستم موازی، تمام n جزء باید از کار بیفتند تا سیستم از کار بیفتد. بنابراین از سیستمی با دو مؤلفه، با دو شکل سری و موازی برای نشان دادن روش پیشنهادی استفاده می‌شود. هر جزء در طول زمان فرسوده می‌شود و می‌تواند به صورت جداگانه در سیستم جایگزین یا تعمیر شود. همچنین بازه‌های بازرسی ثابت (به عنوان مثال ماه، هفته و ...) در نظر گرفته شده است. هدف یافتن اقدامات تعمیر و نگهداری بهینه برای یک افق زمانی مشخص است.

پارامترهای تابع هزینه $C_{PM} = ۵۰, C_{CM} = ۵۰۰$ و $C_f = ۱۰۰۰$ در نظر گرفته شد. همچنین پارامترهای RL در مدل کیو–لرنینگ با مقادیر $\alpha = ۰/۱, \gamma = ۰/۹$، و $\epsilon = ۰/۱$ تنظیم گردیده است.

تخریب یا تعمیر هر یک از مؤلفه مستقل از دیگری در نظر گرفته شده است و احتمال انتقال بین وضعیت‌ها بر اساس تابع توزیع وایبل $F_T(t) = ۱ - e^{-(\frac{t}{\eta})^\beta}$ محاسبه شده است. پارامتر توزیع وایبل برای گذار از حالت سالم به حالت فرسوده $(\beta = ۲, \eta = ۱۰۰۰)$، و برای گذار از حالت فرسوده به تخریب کامل $(\beta = ۱/۵, \eta = ۵۰۰)$ با بازه زمانی $t = ۱۰۰$ در نظر گرفته شده است. همچنین احتمال باقی‌ماندن در وضعیت فعلی با استفاده از رابطه $P(Stay) = ۱ - P(Transition)$ محاسبه می‌گردد. ماتریس انتقال احتمال در بصورت زیر بدست آمده است؛

$$P_{ij} = \begin{pmatrix} ۰/۹۰۴۸ & ۰/۰۹۵۲ & ۰/۰۰۰۰ \\ ۰/۰۰۰۰ & ۰/۸۶۶۰ & ۰/۱۳۴۰ \\ ۰/۰۰۰۰ & ۰/۰۰۰۰ & ۱/۰۰۰۰ \end{pmatrix}$$

در جدول ۱ با توجه به اینکه سیستم از دو مؤلفه تشکیل شده است مجموعه اقدامات ممکن از فضای عمل را نشان می‌دهد. که ۰ نشان دهنده هیچ اقدامی انجام نگردد و ۱ نشان دهنده تعمیر سیستم می‌باشد. که باید دید با توجه به وضعیت سیستم و نوع پیکربندی RL چه روش نگهداری را پیشنهاد می‌دهد.

جدول ۱: مجموعه عمل‌ها در سیستم‌های با دو مؤلفه

شماره	عمل انجام شده برای مؤلفه۱	عمل انجام شده برای مؤلفه۲	زوج مرتب عمل انجام شده
۱	هیچ اقدامی	هیچ اقدامی	$(۰, ۰)$
۲	تعمیر	هیچ اقدامی	$(۱, ۰)$
۳	هیچ اقدامی	تعمیر	$(۰, ۱)$
۴	تعمیر	تعمیر	$(۱, ۱)$

جدول۲ با توجه به اینکه مؤلفه‌های سیستم موازی یا سری هستند الگوهای تعمیر و نگهداری بهینه را با استفاده از روش یادگیری–کیو پیشنهاد می‌دهد. همان‌طور که از جدول پیدا است، زمانیکه سیستم در خطر شکست نیست مدل پیشنهادی عمل هیچ اقدامی و زمانیکه سیستم در خطر است مدل پسشنهادی تعمیر را برای مؤلفه‌ها پیشنهاد می‌دهد. که نوع اقدامات در پیکربندی سری و موازی با یکدیگر متفاوت است. با توجه به اینکه در پیکربندی سری فرسوده بودن یک مؤلفه تهدید شکست مؤلفه و در نتیجه شکست سیستم را در پی خواهد داشت روش یادگیری–کیو پیشنهاد تعویض قطعه را می‌دهد.

Table 2: Add caption

Scenario number	Scenario of state	State number	Optimal action number	
			in parallel component	in series component
1	Healthy-Healthy	(1, 1)	(0, 0)	(0, 0)
2	Degraded-Healthy	(2, 1)	(0, 0)	(1, 0)
3	Failed-Healthy	(3, 1)	(1, 0)	(1, 0)
4	Healthy-Degraded	(1, 2)	(0, 0)	(0, 1)
5	Degraded-Degraded	(2, 2)	(0, 0)	(0, 1)
6	Failed-Degraded	(3, 2)	(1, 0)	(1, 1)
7	Healthy-Failed	(1, 3)	(0, 1)	(0, 1)
8	Degraded-Failed	(2, 3)	(0, 1)	(0, 1)
9	Failed-Failed	(3, 3)	(1, 0)	(1, 1)

۵ نتیجه‌گیری

در این مقاله، یک سیستم ساده با دو پیکربندی موازی و متوالی برای تعمیر و نگهداری پیشگیرانه در نظر گرفته شده است. از مدل یادگیری-کیو در بهینه سازی تصمیم‌گیری عمل تعمیر و نگهداری استفاده شد. روش پیشنهادی در پیکربندیهای مختلف خوب عمل کرده و می‌تواند برای مدل‌های پیچیده‌تری نیز استفاده گردد.

مراجع

[1] Rausand, M. and Hoyland, A., 2003. System reliability theory: models, statistical methods, and applications (Vol. 396). John Wiley & Sons.

[2] Adsule, A., Kulkarni, M. and Tewari, A., 2020. Reinforcement learning for optimal policy learning in condition-based maintenance. IET Collaborative Intelligent Manufacturing, 2(4), pp.182-188.

[3] Yousefi, N., Tsianikas, S. and Coit, D.W., 2022. Dynamic maintenance model for a repairable multi-component system using deep reinforcement learning. Quality Engineering, 34(1), pp.16-35.

[4] Huang, J., Chang, Q. and Arinez, J., 2020. Deep reinforcement learning based preventive maintenance policy for serial production lines. Expert Systems with Applications, 160, p.113701.

[5] Yousefi, N., Tsianikas, S. and Coit, D.W., 2020. Reinforcement learning for dynamic condition-based maintenance of a system with individually repairable components. Quality Engineering, 32(3), pp.388-408.

[6] Zhang, N. and Si, W., 2020. Deep reinforcement learning for condition-based maintenance planning of multi-component systems under dependent competing risks. Reliability Engineering & System Safety, 203, p.107094.

[7] Chen N, Ye ZS, Xiang Y, Zhang L. Condition-based maintenance using the inverse Gaussian degradation model. European Journal of Operational Research. 2015 May 16;243(1):190-9.

[8] Gruber A, Yanovski S, Ben-Gal I. Condition-based maintenance via simulation and a targeted Bayesian network metamodel. Quality Engineering. 2013 Oct 1;25(4):370-84.

[9] Rafiee K, Feng Q, Coit DW. Condition-based maintenance for repairable deteriorating systems subject to a generalized mixed shock model. IEEE Transactions on Reliability. 2015 Aug 20;64(4):1164-74.

پست الکترونیکی: Hasantabar_f@math.usb.ac.ir

بررسی و تحلیل تکنیک های دسته بندی ترافیک های رمزنگاری شده در بستر شبکه با استفاده از مدل های یادگیری عمیق

امید پاک شکاراسطلخی[1*]، رضا ابراهیمی آتانی[2]، مهران علیدوست نیا[3]

۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر نرم افزار دانشگاه گیلان [1]

۲- دانشیار گروه مهندسی کامپیوتر دانشگاه گیلان [2]

۳- استادیار دانشکده مهندسی و علوم کامپیوتر دانشگاه شهید بهشتی تهران [3]

چکیده

دسته‌بندی ترافیک رمزگذاری شده به فرآیند شناسایی و دسته‌بندی ترافیک شبکه‌ای اشاره دارد که با استفاده از پروتکل‌های مختلف مانند SSL/TLS، SSH، IPsec و غیره رمزگذاری شده است. این دسته‌بندی برای درک ماهیت فعالیت شبکه، شناسایی تهدیدات امنیتی بالقوه و اطمینان از انطباق با مقررات حفاظت از داده ضروری است. یکی از دلایل اصلی نیاز به دسته‌بندی ترافیک رمزگذاری شده افزایش برنامه‌ها و سرویس‌های رمزگذاری شده است. بسیاری از برنامه‌ها و خدمات محبوب، از جمله مرورگرهای وب، برنامه‌های پیام‌رسانی و سرویس‌های مبتنی بر ابر، به‌طور پیش‌فرض از رمزگذاری برای محافظت از داده‌ها و ارتباطات کاربر استفاده می‌کنند. در نتیجه، بخش قابل توجهی از ترافیک شبکه در حال حاضر رمزگذاری شده است و این امر دسته‌بندی و مشاهده ماهیت ترافیک عبوری را برای اپراتورهای شبکه چالش‌برانگیز می‌کند. برای مقابله با این چالش، اپراتورهای شبکه و متخصصان امنیتی روش‌ها و ابزارهای مختلفی را برای دسته‌بندی ترافیک رمزگذاری شده توسعه داده‌اند. از میان این روش‌ها، مدل‌های یادگیری عمیق به‌عنوان یک رویکرد امیدوارکننده برای دسته‌بندی ترافیک رمزگذاری‌شده ظاهر شده‌اند. هدف از این مقاله مروری، بررسی و تحلیل تکنیک هایی است که از مدل‌های یادگیری عمیق به‌منظور دسته‌بندی ترافیک رمزگذاری شده شبکه استفاده نموده‌اند. در انتها ضمن ارزیابی کیفیت دسته بندی مدل های بررسی شده موضوعات تحقیقاتی باز این حوزه ارایه می گردد.

کلمات کلیدی: دسته‌بندی ترافیک رمزگذاری‌شده شبکه، ترافیک رمزگذاری‌شده، یادگیری عمیق، یادگیری ماشین، تحلیل شبکه، پایش ترافیک.

۱. مقدمه

دسته‌بندی ترافیک شبکه فرآیند شناسایی برنامه‌ها یا فعالیت‌های خاص و تطبیق آنها با ترافیک شبکه است. این وظیفه برای مدیریت و امنیت شبکه ضروری است [۱]. دسته‌بندی ترافیک شبکه اخیراً به‌دلیل پیشرفت در فناوری رایج شده است. رشد روزافزون تقاضای ترافیک اینترنت پرسرعت، نیاز به چنین وظیفه‌ای را افزایش داده است [۲]. در مدیریت شبکه، دسته‌بندی ترافیک شبکه، موجب شناسایی انواع مختلف برنامه‌های کاربردی شبکه می‌شود و تخصیص مناسب منابع شبکه

[1] Omid.pakshekar.est@gmail.com
[2] rebrahimi@guilan.ac.ir
[3] alidoostnia@sbu.ac.ir

را امکان‌پذیر می‌کند [۳]. همچنین مدیریت کارآمد منابع شبکه را تسهیل کرده و در ایمن‌سازی شبکه ضروری است [۴]. علاوه بر این دسته‌بندی دقیق ترافیک شبکه، تضمین‌کننده کیفیت خدمات[1] (QoS) است. امروزه روش‌های رمزنگاری مختلفی از جمله HTTPS، SSH، SSL و برنامه‌هایی مانند Tor و TrueCrypt در دسترس هستند. این روش‌ها در رمزگذاری ترافیک اینترنت برای محافظت از حریم خصوصی کاربران استفاده می‌شوند [۵]. بنابراین، نیاز به دسته‌بندی ترافیک شبکه که توسط این برنامه‌ها ایجاد می‌شوند، وجود دارد. این دسته‌بندی، از بدافزارها جلوگیری کرده و تشخیص نفوذ شبکه[2] را به حداکثر می‌رساند. همچنین دسته‌بندی ترافیک به ارائه‌دهندگان خدمات اینترنتی[3] (ISP) در انجام فرآیند عیب‌یابی شبکه کمک می‌کند [۶]. در این راستا، سیستمی که بتواند دسته داده‌های ترافیک شبکه را پیش‌بینی کند، با استفاده از الگوهای پنهان موجود در بسته‌های ارسالی، مانند پروتکل‌های امنیتی خاص، همچون HTTPS که از رمزگذاری استفاده می‌کنند، پیشنهاد می‌شود. با استفاده از این سیستم پهنای باند موجود بهینه می‌شود و عملکرد شبکه افزایش می‌یابد. این موضوع می‌تواند به‌طور قابل توجهی بر تجربه کاربر تأثیر بگذارد [۲].

متداول‌ترین رویکردهای مورد استفاده در دسته‌بندی ترافیک شبکه، دسته‌بندی ترافیک شبکه مبتنی بر بازرسی بسته‌های عمیق[4] (DPI)، روش‌های آماری، بازخوردهای رفتاری و دسته‌بندی مبتنی بر پورت[5] است [۷]. شایان ذکر است که روش دسته‌بندی مبتنی بر پورت اخیراً دقت پایینی را نشان داده‌اند که به استفاده غیرسیستماتیک پورت یا پنهان‌سازی پورت نسبت داده می‌شود. در مورد روش مبتنی بر DPI، نمی‌توان از آن در دسته‌بندی ترافیک شبکه رمزگذاری‌شده استفاده کرد؛ زیرا می‌تواند حریم خصوصی کاربران را نقض کند.

از این رو محققان ترجیح داده‌اند از روش‌های آماری و رفتاری استفاده کنند. این روش‌ها شامل مهندسی ویژگی‌ها به‌صورت دستی است و ویژگی‌هایی که با جریان ترافیک خام مرتبط هستند، در دسته‌بندی ترافیک شبکه استخراج و اعمال می‌شوند [۲, ۸]. این روش‌ها دارای نقطه ضعف هستند؛ زیرا برای اجرا به یک متخصص در زمینه شبکه نیاز دارند که دانش زیادی داشته باشد. این متخصص باید از ویژگی‌های آماری ترافیک شبکه مبتنی بر جریان آگاهی داشته باشد، زیرا این ویژگی‌ها باید در طراحی مدل دسته‌بندی در نظر گرفته شوند [۲].

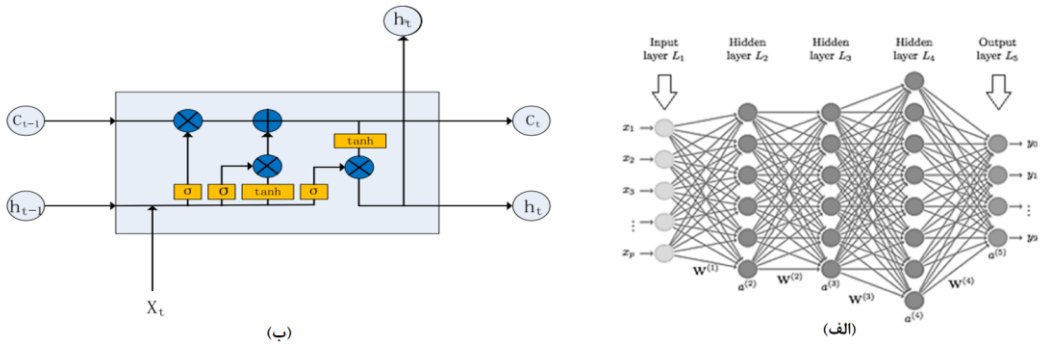
با توسعه فناوری‌های جدید، روش‌های یادگیری ماشین و روش‌های یادگیری عمیق در دسته‌بندی ترافیک شبکه، مورد استفاده و مطالعه قرار گرفته‌اند [۹]. الگوریتم‌های یادگیری ماشین و یادگیری عمیق دسته‌بندی ترافیک شبکه را با استفاده از مدل‌های آموزشی از روی دسته‌های شناخته‌شده امکان‌پذیر می‌سازند. این مدل‌ها می توانند به‌طور خودکار ترافیک جدید را شناسایی و دسته‌بندی کنند. دسته‌بندی ترافیک با استفاده از یادگیری عمیق روشی است که از مدل‌های شبکه عصبی عمیق برای دسته‌بندی خودکار ترافیک شبکه استفاده می‌کند. رویکرد یادگیری ماشین می‌تواند ترافیک برنامه‌های کاربردی ناشناخته یا رمزگذاری شده خاصی را شناسایی کند، اما بر دانش قبلی متکی است. رویکرد یادگیری عمیق، نیازی به استخراج دستی ویژگی‌های ترافیک ندارد و می‌تواند به‌طور خودکار رابطه نگاشت بین ترافیک شبکه و برچسب‌های مربوطه را ایجاد کند، بنابراین وابستگی به دانش قبلی را حذف می‌کند و نسبت به روش‌های یادگیری ماشین ترجیح داده می‌شود [۱۰]. بر همین اساس، گزارش حاضر روش‌های دسته‌بندی ترافیک رمزگذاری شده شبکه را مبتنی بر روش‌های یادگیری عمیق مورد بررسی و مطالعه قرار داده است.

[1] Quality of Service (QoS)
[2] Network intrusion detection
[3] Internet service provider (ISP)
[4] Deep packet inspection-based (DPI)
[5] Port-based classification

۲. یادگیری عمیق

از سال ۲۰۰۶، یادگیری عمیق به‌عنوان حوزه جدیدی از مطالعات یادگیری ماشین ظاهر شده است [۱۱, ۱۲]. الگوریتم‌های یادگیری عمیق، مانند مغز انسان، با تکرار یک کار، تجربه کسب می‌کنند و هوشمندتر می‌شوند [۱۳]. مدل‌های یادگیری عمیق، مانند شبکه‌های عصبی عمیق[1](DNN) ، شبکه‌های عصبی پیچشی[2] (CNN) و شبکه‌های عصبی بازگشتی[3] (RNN)، در حوزه‌های مختلف تحقیقاتی، مانند دسته‌بندی تصویر [۱۴]، پیشرفت‌های قابل توجهی را به‌دست آورده‌اند. در مقایسه با دسته‌بندهای آماری معمولی، مدل‌های یادگیری عمیق برای تبدیل ویژگی‌های ورودی به برچسب‌های کلاس بهتر عمل می‌کنند [۱۳]. مدل‌های یادگیری عمیق نیازی به استخراج دستی ویژگی‌های ترافیک شبکه ندارند و می‌توانند به طور خودکار رابطه نگاشت بین ترافیک شبکه و برچسب‌های مربوطه را ایجاد کنند، به این ترتیب، وابستگی به دانش قبلی حذف می‌شود [۱۰]. دسته‌بندی ترافیک یادگیری عمیق روشی است که از مدل‌های شبکه عصبی عمیق برای دسته‌بندی خودکار ترافیک شبکه استفاده می‌کند [۱۵]. در این راستا از روش‌های مختلفی استفاده شده است که در ادامه بیان خواهند گردید.

مدل شبکه عصبی عمیق: همانطور که در شکل ۱ (الف) نشان داده شده است، ساختار شبکه عصبی عمیق را می‌توان به‌عنوان نوع خاصی از شبکه عصبی با لایه‌های پنهان زیادی در نظر گرفت. شبکه‌های عصبی عمیق بیش از یک لایه پنهان[4] دارند. لایه‌های شبکه عمیق نیز از گره‌ها یا نورون‌ها تشکیل شده است که مانند مغز انسان مکانی برای انجام محاسبات است. در یک گره، ورودی داده در یک وزن ضرب می شود. هر چه این وزن بیشتر باشد، تأثیر آن داده ورودی بیشتر است. سپس مجموع داده‌های ضرب شده محاسبه می‌شود. در نهایت، برای رسیدن به خروجی، مقدار مجموع از یک تابع فعال‌ساز[5] عبور می‌کند و خروجی تولید می‌شود [۱۶].



شکل ۱ (الف) شبکه عصبی عمیق [۱۳]، (ب) ساختار مدل LSTM [۱۵]

مدل شبکه عصبی پیچشی: ساخت شبکه‌هایCNN، از ساختار بینایی بیولوژیکی الهام گرفته شده است [۱۷]. از این رو، شبکه‌های عصبی پیچشی عملکرد بهتری را در یادگیری ویژگی‌های محلی اعمال می‌کنند [۱۸]. CNNها در زمینه‌های مختلف از جمله پردازش زبان طبیعی [۱۹] و بینایی ماشین [۲۰] سرآمد بوده‌اند. CNNها همچنین در سال‌های اخیر عملکرد فوق العاده‌ای در ترافیک رمزگذاری شده نشان داده‌اند [۲۱]. شبکه‌های عصبی پیچشی، از پرکاربردترین روش‌های یادگیری عمیق هستند. یک لایه ورودی، یک لایه خروجی و تعدادی لایه پنهان یک شبکه عصبی پیچشی را تشکیل می‌دهد. لایه‌های پیچش، ادغام[6]و کاملاً متصل[7] سه نوع لایه اصلی هستند که یک شبکه عصبی پیچشی را تشکیل می‌دهند. به‌طور کلی، شبکه‌های عصبی پیچشی، شبکه‌های عصبی لایه‌ای هستند که در آنها چندین لایه کاملاً متصل پس از سازماندهی

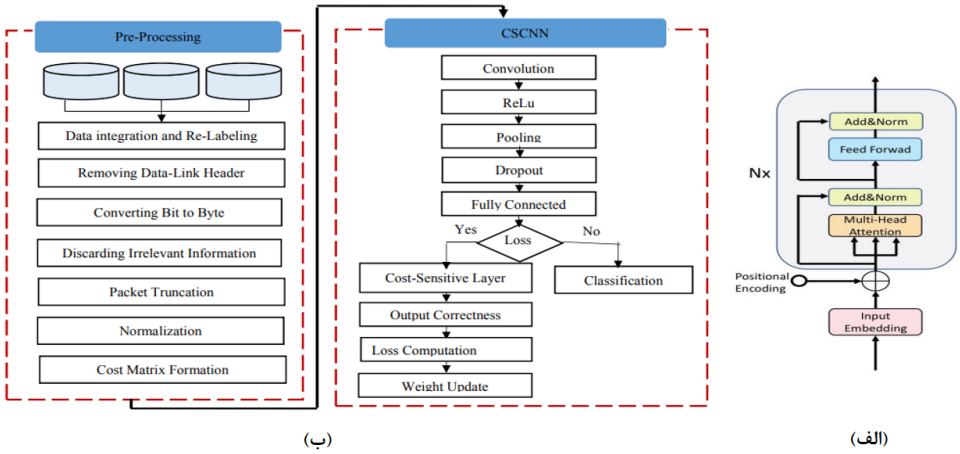
[1] Deep neural network (DNN)
[2] Convolutional neural network (CNN)
[3] Recurrent neural network (RNN)
[4] Hidden layer
[5] Activation layer
[6] Pooling
[7] Fully connected

لایه‌های پیچش و ادغام به‌طور متناوب ساخته می‌شوند [۱۳]. عملکرد فوق العاده‌ای در ترافیک رمزگذاری شده نشان داده‌اند [۲۱]. یک لایه ورودی، یک لایه خروجی و تعدادی لایه پنهان یک شبکه عصبی پیچشی را تشکیل می‌دهد. لایه‌های پیچش، ادغام و کاملاً متصل سه نوع لایه اصلی هستند که یک شبکه عصبی پیچشی را تشکیل می‌دهند. به‌طور کلی، شبکه‌های عصبی پیچشی، شبکه‌های عصبی لایه‌ای هستند که در آنها چندین لایه کاملاً متصل پس از سازماندهی لایه‌های پیچش و ادغام به‌طور متناوب ساخته می‌شوند [۱۳].

مدل حافظه کوتاه مدت طولانی: حافظه کوتاه مدت طولانی [1](LSTM)، نوعی از شبکه عصبی بازگشتی هستند که می‌توانند وابستگی‌های طولانی مدت را یاد بگیرند. ساختار مدل LSTM در شکل ۱ (ب) نشان داده شده است. LSTM می‌تواند مسئله ناپدید شدن گرادیان را حل کند و ثابت شده است که نتایج تشخیص قابل قبولی در تحلیل سری‌های زمانی به دست می‌آورد. به همین دلیل، LSTM می‌تواند برای تحلیل ترافیک شبکه استفاده شود، زیرا داده‌های ترافیک شبکه، داده‌هایی با وابستگی بالا به زمان هستند [۲۲]. ساختار LSTM از چهار لایه شامل سلول حافظه، گیت ورودی، گیت خروجی و گیت فراموشی تشکیل شده است. سلول حافظه مقادیر را برای بازه‌های زمانی دلخواه نگه می‌دارد و سه گیت دیگر جریان اطلاعات را به داخل و خارج از سلول تنظیم می‌کنند. گیت فراموشی تصمیم می‌گیرد که چه اطلاعاتی از حالت قبلی سلول حذف شود. گیت ورودی تصمیم می‌گیرد که چه اطلاعات جدیدی در حالت فعلی سلول ذخیره شود. گیت خروجی تصمیم می‌گیرد که چه اطلاعاتی از حالت فعلی سلول به‌عنوان خروجی ارائه شود [۲۳]

حافظه کوتاه مدت طولانی: مدل حافظه کوتاه‌مدت طولانی دوطرفه[2] (Bi-LSTM)، توسعه‌ای از مدل LSTM است که توالی‌های ورودی را در دو جهت رو به‌جلو و عقب پردازش می‌کند و به شبکه اجازه می‌دهد تا اطلاعاتی را از گذشته و آینده بگیرد. این معماری به‌ویژه برای کارهایی که نیاز به درک مفهوم یک دنباله دارند مفید است [۲۴]. این مدل در شناسایی و دسته‌بندی دقیق ترافیک شبکه رمزگذاری‌شده نتایج بسیار خوبی ارایه داده است [۲۵].

مدل برت: مدل برت[3] (BERT)، یک مدل یادگیری عمیق برای پردازش زبان طبیعی (NLP) است که بر اساس معماری ترانسفورمر ساخته شده است. این مدل به دلیل توانایی گرفتن اطلاعات از دوطرف توکن ورودی، به‌عنوان دوجهته شناخته می‌شود [۲۶]. مدل‌هایی که از برت استفاده می‌کنند، نمایش‌های داده متنی را از ترافیک رمزگذاری شده با استفاده از ترانسفورمرهای پیش آموزش‌دیده یاد می‌گیرند [۲۷]. شکل ۲ (الف) ساختار مدل برت را نشان می‌دهد.



شکل ۲ (الف) ساختار معماری ترانسفورمری مدل BERT [۲۸] (ب) مراحل اجرای مدل CSCNN [۲۹]

[1] Long short-term memory (LSTM)
[2] Bidirectional Long Short-Term Memory (Bi-LSTM)
[3] BERT (Bidirectional Encoder Representations from Transformers)

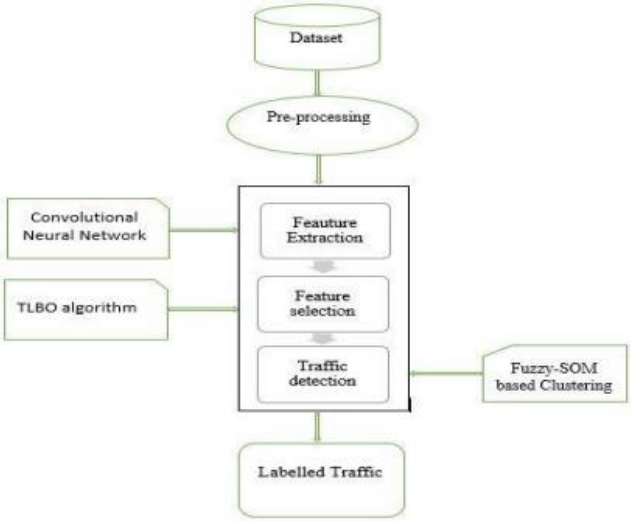
۳ - مرور کارهای پیشین در حوزه تکنیک های دسته بندی ترافیک های رمزنگاری

مطالعات بررسی شده در این حوزه بر اساس مدل پیاده‌سازی، می‌توانند به سه دسته مدل‌های مبتنی بر شبکه عصبی پیچشی، مدل‌های مبتنی بر شبکه عصبی عمیق و مدل‌های ترکیبی تقسیم بندی میشوند. در ادامه به بررسی بیشتر این مطالعات پرداخته خواهد شد.

۱.۳ مدل‌های مبتنی بر شبکه عصبی پیچشی

در مطالعه [۲۹]، یک مدل دسته‌بندی جدید به منظور دسته‌بندی ترافیک رمزگذاری شده شبکه پیشنهاد شده است. این مدل سعی دارد به مشکل عدم تعادل داده‌ها در طول فرآیند آموزش بپردازد. روش پیشنهادی از یک شبکه عصبی پیچشی حساس به هزینه استفاده می‌کند و شبکه عصبی پیچشی حساس به هزینه[1] (CSCNN) نامیده می‌شود. این مدل، از یک ماتریس هزینه استفاده می‌کند که بر اساس توزیع هر کلاس هزینه‌ای را به هر دسته‌بندی اشتباه اختصاص می‌دهد. سپس این هزینه در مرحله آموزش اعمال می‌گردد. ماتریس هزینه در مرحله پیش‌پردازش با استفاده از توزیع داده‌های کلاس‌های مختلف تولید می‌گردد و در آن هزینه بیشتری به کلاس‌های اقلیت نسبت به کلاس‌های اکثریت اختصاص داده می‌شود. مجموعه‌داده ISCX VPN-nonVPN برای ارزیابی مدل CSCNN استفاده شده است. طبق نتایج به دست آمده مدل CSCNN به دقت ۹۷.۷ درصد دست می‌یابد. ساختار مدل CSCNN در شکل ۲ (ب) نشان داده شده است.

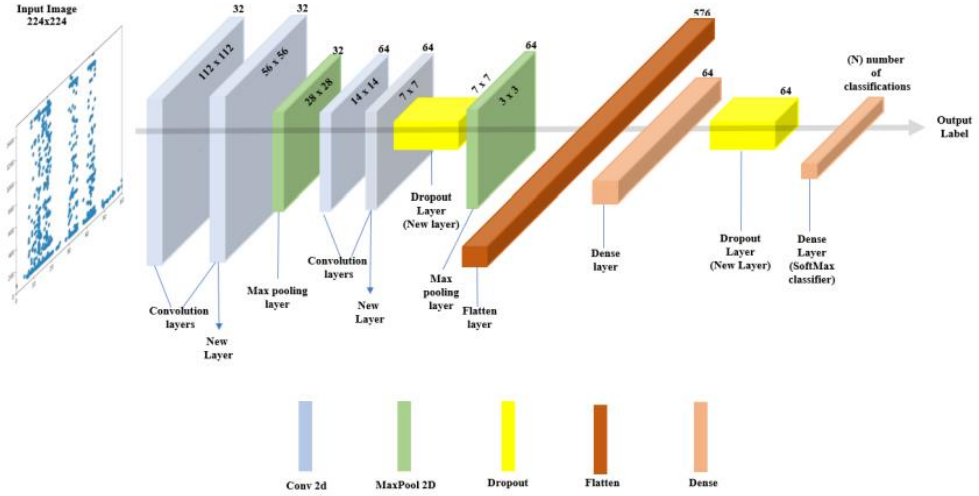
مطالعه [۳۰]، به منظور ساخت یک مدل دسته‌بندی ترافیک، روش‌های CNN، الگوریتم بهینه‌سازی مبتنی بر آموزش-یادگیری[2] (TLBO) و نقشه‌های خود سازماندهی[3] (SOM) را ترکیب می‌کند. رویکرد پیشنهادی ترکیبی از CNN و TLBO است که در آن CNN یک روش مبتنی بر تصویر است که می‌تواند داده‌های شبکه رمزگذاری‌شده را به دقت شناسایی کند. TLBO نیز یک مکانیسم انتخاب ویژگی است که نقشه‌های خودسازماندهی را ترکیب می‌کند. ارزیابی مدل پیشنهادی با مجموعه‌داده ISCX VPN-non-VPN انجام شده است. طبق نتایج گزارش شده، دقت این مدل ترکیبی به ۹۷ درصد می‌رسد. شکل ۳ ساختار مدل را نشان می‌دهد.



شکل ۳ ساختار مدل ترکیبی CNN، TLBO و SOM [۳۰]

[1] Cost-Sensitive CNN (CSCNN)
[2] Teaching-Learning Based Optimization (TLBO)
[3] Self-Organizing Maps (SOM)

مدل پیشنهادی در مطالعه [۳۱]، یک شبکه CNN یازده لایه، با طیف وسیعی از تصاویر تولید شده از کلان داده‌های ترافیک رمزگذاری‌شده است. مجموعه‌داده‌های مورد استفاده در این آزمایش، ISCXVPN2016 و ISCXTor2016 هستند. ویژگی‌های استفاده شده، اندازه بسته و زمان رسیدن بسته‌اند که برای تولید تصاویر منحصربه‌فرد ترافیک برنامه‌های مختلف استفاده می‌شوند. پس از تولید تصاویر، مدل دسته‌بندی‌کننده طراحی‌شده با CNN برای هفت مسئله دسته‌بندی مختلف به کارگرفته شده‌است. این هفت مسئله عبارتند از: "شناسایی برنامه‌های non-VPN"، "شناسایی نوع ترافیک non-VPN"، "شناسایی برنامه‌های VPN"، "شناسایی نوع ترافیک VPN"، "شناسایی برنامه‌های TOR"، "شناسایی نوع ترافیک TOR" و "شناسایی نوع رمزگذاری". مدل مبتنی بر CNN، برای هفت مسئله دسته‌بندی، با استفاده از سه نوع رمزگذاری (https، vpn، tor) آموزش دیده و آزمایش شده است. برای تمام وظایف دسته‌بندی، مدل به دقت‌هایی از ۹۱ درصد تا ۹۹ درصد دست می‌یابد. شکل ۴ ساختار این مدل پیشنهادی را نشان می‌دهد.



شکل ۴ ساختار مدل مبتنی بر شبکه CNN یازده لایه [۳۱]

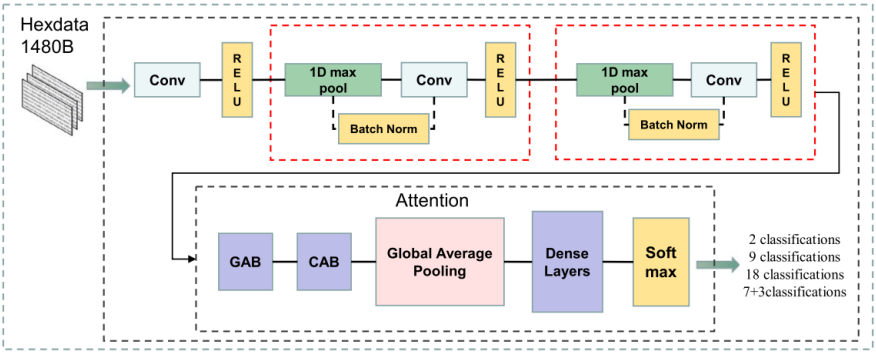
در مقاله [۳۲]، یک مدل شبکه عصبی پیچشی یک بعدی با داده‌های هگزادسیمال (HexCNN-1D) تعریف شده است که مکانیزم‌های پردازش عادی و توجه را ترکیب می‌کند. با افزودن ماژول‌های مکانیسم توجه بلوک توجه جهانی (GAB)[1] و بلوک توجه دسته‌بندی[2](CAB) ، ترافیک شبکه دسته‌بندی و شناسایی می‌شود. با استخراج اطلاعات بار موثر از ترافیک شبکه هگزا دسیمال، مدل می‌تواند اکثر دسته‌های ترافیک شبکه، از جمله داده‌های ترافیک رمزگذاری‌شده و مخرب را شناسایی کند. در این مطالعه از مجموعه‌داده‌هایISCX-VPN-NonVPN-2016 و USTC-TFC2016 استفاده شده است. نتایج نشان می‌دهد که میانگین دقت ۹۸.۸ درصد است. شکل ۵ ساختار مدل HexCNN-1D را نشان می‌دهد.

۲.۳ مدل های مبتنی بر شبکه عصبی عمیق

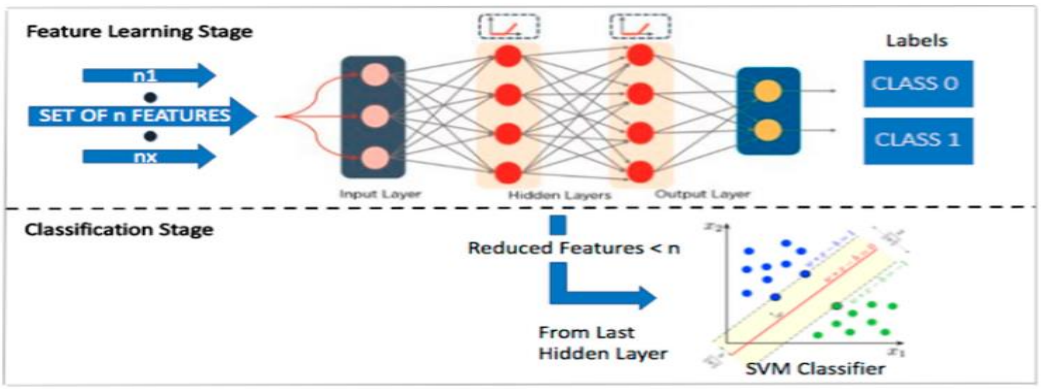
تمرکز مطالعه [۳۴]، ارزیابی عملکرد روش ماشین بردار پشتیبان[3] (SVM) در دسته‌بندی بسته‌های شبکه بر اساس نوع کاربرد است. این مطالعه از یک شبکه عصبی عمیق برای بهبود عملکرد الگوریتم ماشین بردار پشتیبان استفاده می‌کند. ارزیابی مدل پیشنهادی بر روی مجموعه‌داده ISCXVPN2016 انجام شده است. این مطالعه نتیجه می‌گیرد که شبکه عصبی عمیق می‌تواند امتیاز F1 دسته‌بند ماشین بردار پشتیبان را از ۷۸ درصد به ۹۰ درصد بهبود بخشد. علاوه بر این، این

[1] Global Attention Block
[2] Category Attention Block
[3] Support Vector Machine (SVM)

مطالعه نشان می‌دهد که استفاده از ساختار ترکیبی شبکه عصبی عمیق به‌همراه ماشین بردار پشتیبان می‌تواند مشکل عدم تعادل کلاس را که اغلب در یادگیری ماشین وجود دارد، برطرف کند. شکل ۶ ساختار مدل را نشان می‌دهد.



شکل ۵ ساختار مدل HexCNN-1D [۳۲]

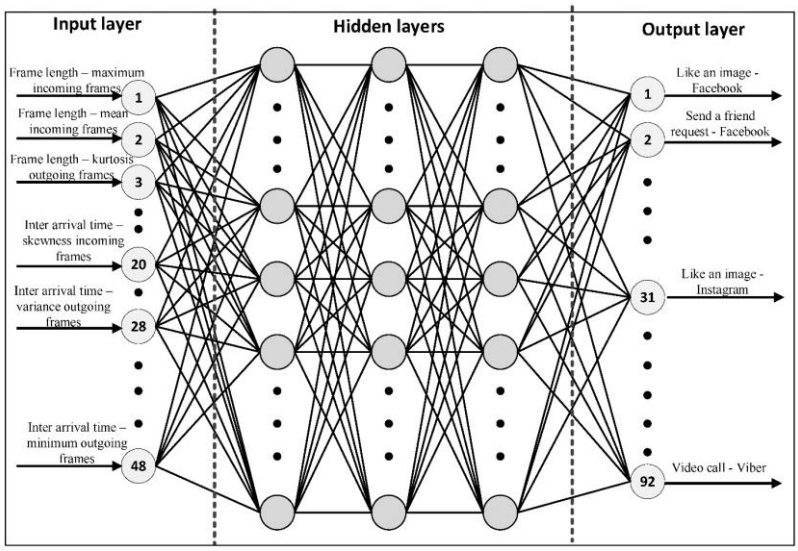


شکل ۶ ساختار مدل مبتنی بر ماشین بردار پشتیبان و شبکه عصبی عمیق [۳۴]

در مطالعه [۳۵]، با استفاده از یادگیری عمیق، ترافیک رمزگذاری شده داده‌های غیر موبایلی دسته‌بندی شده‌اند. برای این منظور از مجموعه‌داده UNB ISCX VPN-non-VPN استفاده شده است که شامل ترافیک رمزگذاری شده و رمزگذاری نشده برنامه‌های مختلف است. سپس الگوریتمی بر اساس شبکه عصبی عمیق طراحی شده که بتواند این ترافیک‌ها را به‌طور مؤثر دسته‌بندی کند. پس از ارزیابی مدل، دقت برابر با ۸۶ درصد و امتیاز F1 برابر با ۷۸ درصد به‌دست می‌آید.

در مطالعه [۳۶]، یک شبکه عصبی عمیق مبتنی بر چارچوب تشخیص فعالیت کاربر برای شناسایی فعالیت‌های کاربر از یک جریان ترافیک اینترنتی رمزگذاری‌شده در برنامه‌های کاربردی تلفن همراه پیشنهاد شده است. در این مطالعه، از توزیع احتمال یک لایه خروجی شبکه عصبی عمیق برای فیلتر کردن داده‌ها در برنامه‌هایی که در طول آموزش مدل در نظر گرفته نشده‌اند (یعنی داده‌های ناشناخته) استفاده می‌شود. چارچوب پیشنهادی از یک رویکرد مبتنی بر پنجره زمانی[1] استفاده می‌کند تا جریان ترافیک فعالیت را به بخش‌هایی تقسیم کند، به‌طوری که فعالیت‌های درون برنامه‌ای را بتوان تنها با مشاهده بخشی از ترافیک مرتبط با فعالیت شناسایی کرد. مجموعه‌داده جمع‌آوری شده در این مطالعه، مجموعه‌ای از فعالیت‌های کاربر در هشت برنامه موبایلی (Facebook، Instagram، YouTube، Viber، WhatsApp، Gmail، Skype و Messenger) است. نتایج این آزمایش نشان داده است که با استفاده از ساختار مبتنی بر شبکه عصبی عمیق، شناسایی فعالیت‌های درون برنامه‌ای برای داده‌های آموزش‌دیده به دقت ۹۰ درصد یا بالاتر می‌رسد. همچنین در شناسایی ترافیک فعالیت‌های درون برنامه‌ای برای داده‌هایی که قبلاً آموزش ندیده‌اند (داده‌های ناشناخته)، مدل دقت متوسط ۷۹ درصد را دارد. ساختار این شبکه عصبی عمیق در شکل ۷ نشان داده شده است.

[1] Time window-based approach



شکل ۷ مدل شبکه عصبی عمیق برای شناسایی فعالیت کاربر از جریان ترافیک برنامه‌های تلفن همراه [۳۶]

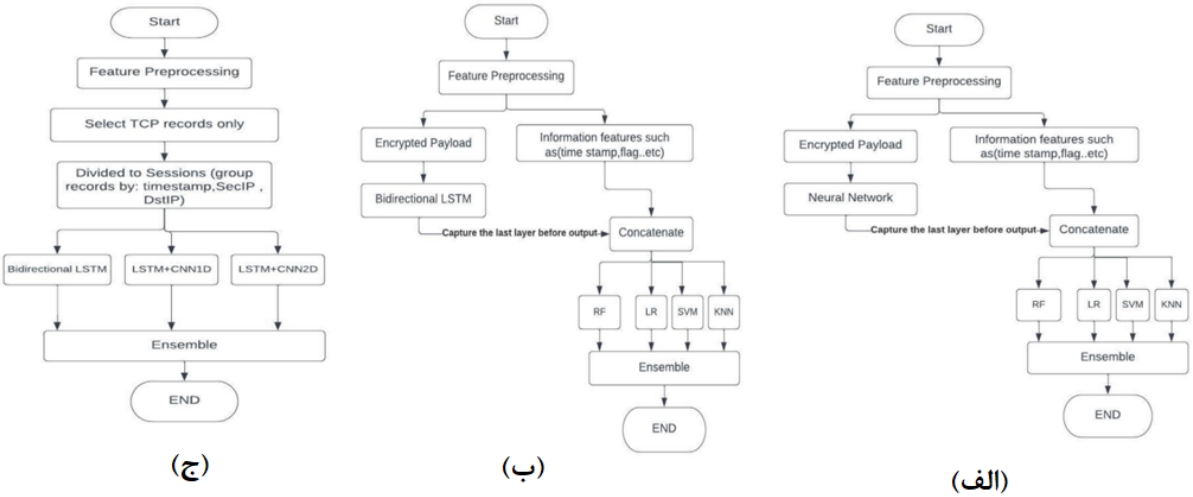
۳.۳. مدل های ترکیبی

در مطالعه [۳۷]، نشان داده شده است که ویژگی‌هایی مانند طول بسته، برچسب‌های زمانی یا امنیت لایه انتقال[۱] (TLS) و اطلاعات بسته رمزگذاری‌شده می‌توانند به‌عنوان ویژگی‌های ورودی هنگام انجام دسته‌بندی استفاده شوند. مجموعه‌داده مورد مطالعه توسط ابزار Wireshark با تعداد کل ۳۳۲۸۶ بسته جمع‌آوری شده است. در این آزمایش، سه روش برای شناسایی ترافیک رمزگذاری‌شده وجود دارد. دو روش اول شامل دو مرحله است. در این دو مرحله، روش‌های دسته‌بندی مبتنی بر یادگیری ماشین یعنی جنگل تصادفی[۲]، ماشین بردار پشتیبان، رگرسیون خطی[۳] و K-نزدیک‌ترین همسایه[۴] با یک روش یادگیری عمیق ترکیب می‌شوند. در مرحله اول روش یادگیری عمیق، یک شبکه عصبی و در مرحله دوم یک BiLSTM است. در این دو مرحله، نتیجه نهایی با استفاده از روش رأی‌گیری گروهی[۵] به‌دست می‌آید. در روش سوم، بسته‌های شبکه بر اساس IP مبدأ، IP مقصد و زمان نشست[۶] انتخاب شده و با استفاده از سه روش یعنی لایه‌های پیچش ۱ بعدی یا ۲ بعدی، یا بدون آنها، با شبکه LSTM ترکیب می‌شوند. سپس، مانند دو روش اول، نتیجه نهایی با استفاده از رأی‌گیری گروهی به‌دست می‌آید. نحوه عملکرد این روش ها در شکل ۸ نشان داده شده است. نتایج این مطالعه نشان می‌دهد که روش اول، دقت ۹۶.۷ درصد و روش دوم و سوم به‌ترتیب، دقت ۹۵.۲ درصد و ۹۶ درصد را به‌دست آورده‌اند.

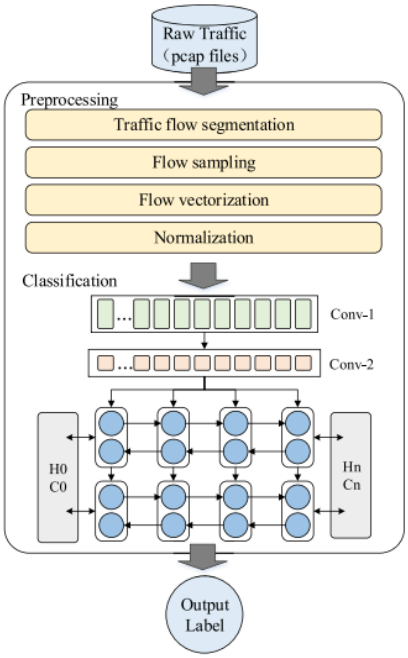
در مطالعه [۳۸]، یک مدل جدید برای دسته‌بندی ترافیک رمزگذاری شده، به نام TSCRNN، معرفی شده است. مدل TSCRNN شامل مرحله پیش‌پردازش و مرحله دسته‌بندی است. در مرحله پیش‌پردازش، داده‌های ترافیک با بخش‌بندی جریان[۷]، نمونه‌برداری[۸] و برداری‌سازی[۹] پردازش می‌شوند. برای حل مسئله دسته‌بندی جریان طولانی‌مدت[۱۰]، از استراتژی‌های

[1] Transport layer security (TLS)
[2] Random Forest
[3] Linear regression
[4] K-nearest neighbor
[5] Ensemble voting technique
[6] Session time
[7] Flow segmentation
[8] Sampling
[9] Vectorization
[10] Long-time flow

نمونه‌گیری برای جمع‌آوری نمونه‌ها از بین جریان طولانی مدت استفاده می‌شود. در مرحله دسته‌بندی، مدل TSCRNN ویژگی‌های فضایی-انتزاعی[1] را توسط CNN استخراج می‌کند و سپس پشته BiLSTM[2] را برای یادگیری ویژگی‌های زمانی[3] استفاده می‌کند. آزمایش‌ها بر روی مجموعه‌داده ISCXTor2016 انجام شده است. نتایج نشان می‌دهد که TSCRNN در دسته‌بندی دودویی Tor یا nonTor به دقت تا ۹۹.۴ درصد دست می‌یابد. ساختار مدل TSCRNN در شکل ۹ نشان داده شده است.



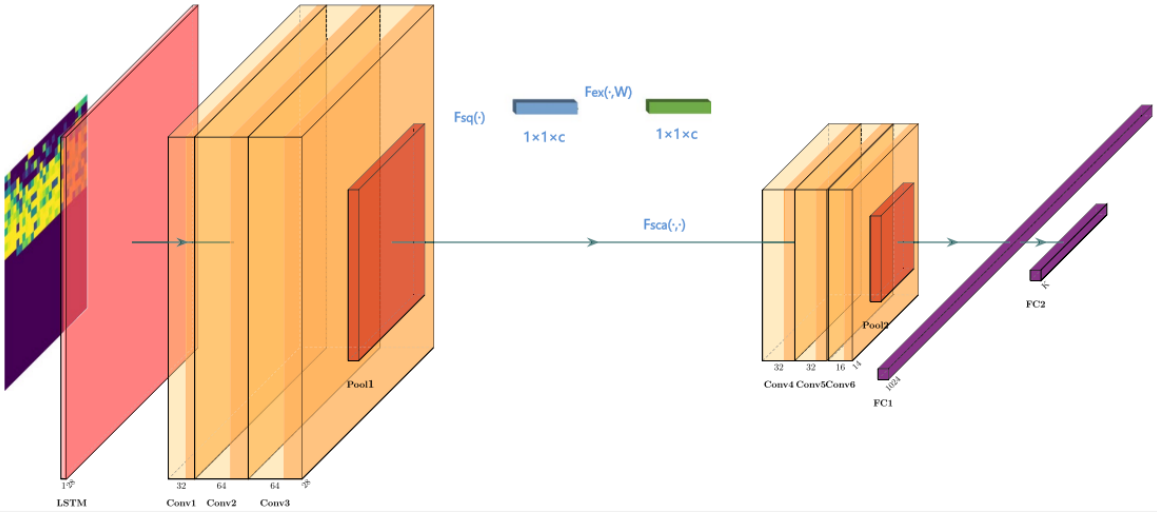
شکل ۸ (الف) ترکیب شبکه‌های عصبی و دسته‌بندهای مختلف (ب) ترکیب BiLSTM و دسته‌بندهای مختلف، (ج) ترکیب LSTM ، LSTM-Conv1D و LSTM-Conv2D [۳۷]



شکل ۹ ساختار مدل TSCRNN [۳۸]

[1] Abstract spatial features
[2] Stack bidirectional LSTM
[3] Temporal characteristics

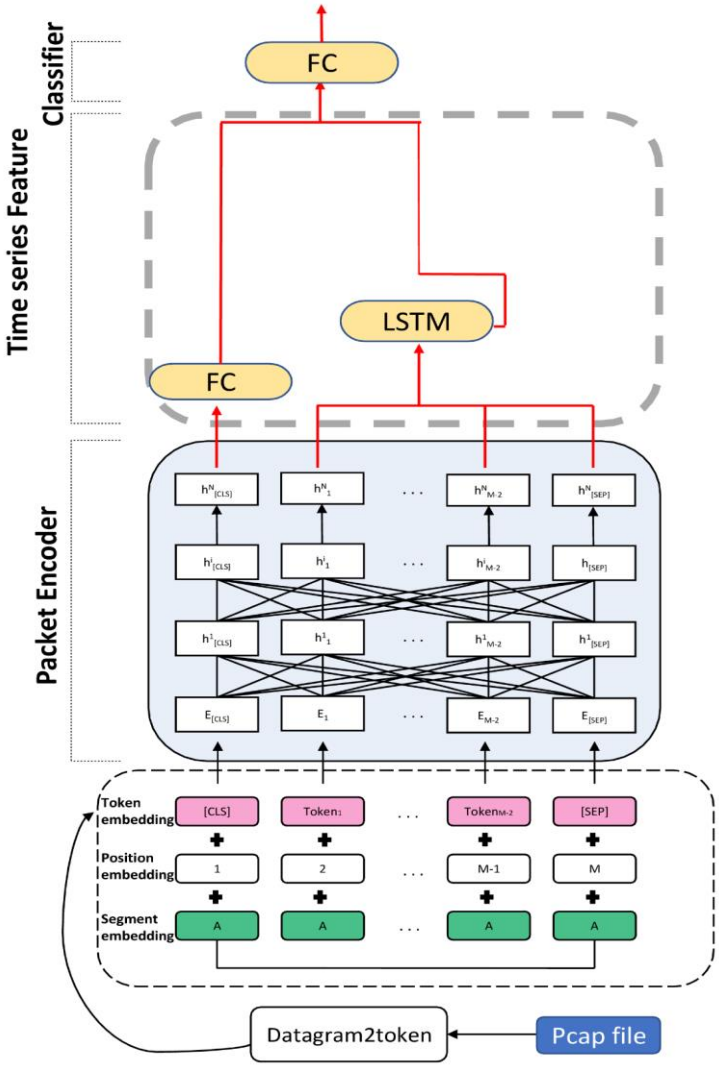
مطالعه [۱۵]، یک مدل دسته‌بندی ترافیک رمزگذاری شبکه را پیشنهاد می‌کند که مکانیسم‌های توجه و ویژگی‌های مکانی-زمانی را ترکیب می‌نماید. این مدل ابتدا از روش LSTM برای تحلیل جریان‌های پیوسته شبکه و یافتن ویژگی‌های همبستگی زمانی بین این جریان‌های شبکه استفاده می‌کند. در مرحله دوم، از روش CNN برای استخراج ویژگی‌های فضایی مرتبه بالا در جریان شبکه استفاده کرده و سپس، ماژول فشار و تحریک[1] (SE) برای وزن‌دهی و توزیع مجدد ویژگی‌های فضایی مرتبه بالا استفاده می‌شود. ویژگی‌های فضایی جریان شبکه در نهایت از طریق این سه مرحله آموزش داده شده و دسته‌بندی سریع جریان‌های شبکه حاصل می‌گردد. این مطالعه برای ارزیابی مدل، از سه مجموعه‌داده ISCX VPN-nonVPN، USTC-TFC2016و مجموعه‌داده YouTube استفاده نموده است. نتایج نشان می‌دهد که می‌توان از این مدل برای دسته‌بندی ترافیک شبکه در برنامه‌های رمزگذاری‌شده و رمزگذاری‌نشده به‌طور همزمان استفاده کرد. دقت دسته‌بندی ترافیک زیربنایی برنامه‌های رمزگذاری‌شده در این مدل، بیش از ۹۰ درصد است. شکل ۱۰ معماری این مدل را نشان می‌دهد.



شکل ۱۰ ساختار مدل مبتنی بر LSTM ، CNN وSE [۱۵]

در مطالعه [۴۰]، یک مدل شبکه ویژگی سری زمانی[2] (TSFN) مبتنی بر برت پیشنهاد شده است. این مدل، یک ماژول رمزگذار بسته است که توسط مدل برت ساخته شده است و با استفاده از مکانیسم توجه، ضبط ویژگی‌های کلی ترافیک را انجام می‌دهد. همچنین این مدل، یک ماژول استخراج ویژگی زمانی است که توسط مدل LSTM ساخته شده است و ویژگی‌های سری زمانی ترافیک را به تصویر می‌کشد. سپس، ویژگی‌های کلی و سری زمانی ترافیک مخرب به‌عنوان ویژگی نهایی با هم ترکیب می‌شوند که می‌تواند ترافیک مخرب را بهتر نشان دهد. نتایج نشان می‌دهد که رویکرد پیشنهادی می‌تواند دقت دسته‌بندی ترافیک مخرب را در مجموعه‌داده‌های USTC-TFC بهبود بخشد و به مقدار امتیاز F1 برابر با ۹۹.۵۰ درصد برسد. شکل ۱۱ ساختار مدل TSFN را نشان می‌دهد.

[1] Squeeze and excitation
[2] Time-Series Feature Network



شکل ۱۱ ساختار مدل TSFN [۴۰]

۲. پایگاه داده

برای ساخت یک مدل طبقه بندی، مجموعه داده ها باید برای اهداف آموزشی و ارزیابی مورد استفاده قرار گیرند. معیارهای فرآیند انتخاب مجموعه داده عبارت بودند از: تنوع ترافیک شبکه جمع آوری شده، در دسترس بودن قالب فایل PCAP/Attribute-Relation (ARFF)، گسترش گسترده مجموعه داده در مقالات و در دسترس بودن مجموعه داده ها می باشد.

در این بخش، مجموعه داده‌های مختلف مربوط به ترافیک شبکه که در تحقیقات و تحلیل‌های مختلف مورد استفاده قرار گرفته‌اند، معرفی می‌شوند:

- مجموعه داده Moore [41] : این مجموعه داده شامل ردگیری‌های شبکه است که در سال ۲۰۰۵ در آزمایشگاه‌های دانشگاه کمبریج جمع‌آوری شده‌اند. این مجموعه شامل داده‌های مربوط به بسیاری از برنامه‌ها از جمله HTTP ، FTP، MySQLو BitTorrent است که در قالب ۱۰ گروه خدماتی مانند P2P و بازی‌های چندرسانه‌ای برچسب‌گذاری شده‌اند. فرمت ARFF و ۲۴۹ ویژگی آماری استخراج‌شده، موجب محبوبیت این مجموعه شده است.

- مجموعه داده USTC-TFC2016 [42]: این مجموعه داده خصوصی شامل ترافیک شبکه مربوط به برنامه‌های مخرب و سالم است. هر مجموعه شامل ترافیک ۱۰ برنامه مختلف در فرمت PCAP است، از جمله FaceTime ، Skype، Zeus و Cridex.
- مجموعه داده ISCX [43] : این مجموعه در سال ۲۰۱۶ توسط موسسه امنیت سایبری کانادا جمع‌آوری شده است. داده‌ها شامل ترافیک برنامه‌های مختلف هستند که در هفت گروه خدماتی دسته‌بندی شده‌اند. ترافیک VPNشامل داده‌هایی است که از تونل VPN عبور کرده‌اند، در حالی که ترافیک غیر VPN-از تونل‌های غیر-VPNعبور کرده‌اند.
- مجموعه داده MAWI [45] : این مجموعه توسط گروه کاری MAWI تحت پروژه WIDE در ژاپن جمع‌آوری شده است. داده‌ها از سال ۲۰۰۰ تاکنون از نقاط مختلف شبکه WIDE برای تحلیل ترافیک جمع‌آوری شده‌اند و شامل ترافیک سالم و مخرب برنامه‌های گوناگون هستند.
- مجموعه داده Auckland II [46] : این مجموعه در دانشگاه آکلند جمع‌آوری شده و بیشتر داده‌ها مربوط به سال ۲۰۰۰ هستند. هر نمونه ۲۴ ساعت یا کمتر بوده و ترافیک غیر IP-حذف شده است. پروتکل‌های معمول جمع‌آوری شده شامل HTTP ، IMAP، POPو SMTP هستند.
- مجموعه داده دانشگاه برسیا (UNIBS) [47] : این مجموعه شامل ترافیک شبکه به مدت سه روز است که در سال ۲۰۰۹ با استفاده از ۲۰ ایستگاه کاری در دانشگاه برسیا جمع‌آوری شده است. بیشتر داده‌ها ترافیک TCP هستند و شامل BitTorrent ، Skype، HTTPو eDonkey می‌شوند.
- مجموعه داده دانشگاه جینان (UJN) [119] : شامل ردگیری‌های ترافیک شبکه به مدت دو روز است که در سال ۲۰۱۳ در دانشگاه جینان جمع‌آوری شده‌اند. جریان‌هایی با کمتر از ۱۰ بسته حذف شده‌اند. این داده‌ها شامل مرور، چت، دیسک ابری و به‌روزرسانی زنده هستند که از دستگاه‌های میزبان ویندوز جمع‌آوری شده‌اند.
- مجموعه داده Anon17 [48] :شامل ترافیک شبکه واقعی ناشناس است که بین سال‌های ۲۰۱۴ تا ۲۰۱۷ در آزمایشگاه NIMS جمع‌آوری شده است. ابزارهایی مانندTor ، JonDonymو I2P برای تولید ترافیک استفاده شده و ابزار Tranalyzer برای استخراج ویژگی‌های آماری به کار رفته است. در مجموع پنج مجموعه داده ARFF شامل کلاس‌های مختلف مانند مرور، IRC، استریم و تورنت وجود دارد.
- مجموعه داده MIRAGE-2019 [49] : شامل ترافیک واقعی برنامه‌های موبایل اندرویدی است که بین سال‌های ۲۰۱۷ تا ۲۰۱۹ در آزمایشگاه ARCLAB دانشگاه ناپولی جمع‌آوری شده است. داده‌ها در فرمت JSONبرای هر نمونه PCAP ثبت شده‌اند و شامل ترافیک ۴۰ برنامه با استفاده از دستگاه‌های اندرویدی مختلف هستند.
- مجموعه دادهUNSW IoT [50] :شامل ترافیک واقعی دستگاه‌های IoT است که بین سال‌های ۲۰۱۶ و ۲۰۱۷ طی ۲۶ هفته در UNSW جمع‌آوری شده‌اند. این آزمایش شامل ۲۸ دستگاه هوشمند متصل به دروازه اینترنت از طریق نقطه دسترسی WiFi بوده است.
- مجموعه داده MobileGT [51] : شامل ترافیک شبکه برنامه‌های موبایل است که در محیط گوشی هوشمند نظارت‌شده جمع‌آوری شده‌اند. داده‌ها شامل ترافیک فعال (AMTD) و غیرفعال (PMTD) هستند AMTD . با استفاده از ابزار mgtClient در ۱۰ گوشی هوشمند بین سال‌های ۲۰۱۶ و ۲۰۱۷ و PMTD در سال ۲۰۱۸ جمع‌آوری شده‌اند. ترافیک ۱۲ برنامه برای تولید این داده‌ها استفاده شده و داده‌ها در فرمت ARFF در دسترس هستند.

جدول ۱- پارامترهای محاسبه شده در دو مقطع

نام پایگاه داده	تعداد کلاس ها	نوع ترافیک	سال	برچسب گذاری شده	نوع فایل
Moore	۱۰	Web,SMTO,POP3,FTP,DNS, BitTorrent,MySQL,Virus, W,Telnet,WOW,windows media player	۲۰۰۵	بله	ARFF
Auckland II	۱۰	FTP, FTP-data, http, imap, pop3, smtp, nntp, ssh, dns, Telnet	۲۰۰۰	خیر	Packet header (No payload)
UNIBS traces	۱۰	BitTorrent,Skype,HTTP, eDonkey,IMAP,POP3, MSN, SMTP, urd, SSH	۲۰۰۹	بله	Full pcap
UJN traces	۹	Browsing, chat, cloud disk, live update, stream media, mail, ftp, p2p, other	۲۰۱۳	بله	Ful PCAP
Anon 17	متفاوته	Browsing, IRC, streaming, Torrent, other	۲۰۱۴-۲۰۱۷	بله	ARFF
ISCX	۷	HTTPS, SMTP, Facebook, Chrome, FTP, Skype, BitTorrent	۲۰۱۶	بله	Full PCAP
USTC-TFC2016	۲	Facetime, Gmail, Skype, Zeus, Cridex, Htbot	۲۰۱۶	بله	Full PCAP
Mirage	۴۰	40 android apps	۲۰۱۷-۲۰۱۹	بله	ARFF

جمع بندی و نتیجه‌گیری

در این مقاله مروری، روش‌های مختلف دسته‌بندی ترافیک رمزگذاری‌شده شبکه با تمرکز بر مدل‌های یادگیری عمیق مورد بررسی قرار گرفتند. مطالعه نشان داد که روش‌های مبتنی بر یادگیری عمیق، به دلیل قابلیت خود در استخراج خودکار ویژگی‌ها و کاهش وابستگی به دانش قبلی، به طور قابل‌توجهی در دسته‌بندی ترافیک رمزگذاری‌شده مؤثرتر از روش‌های سنتی هستند. مدل‌هایی مانند شبکه‌های عصبی پیچشی(CNN) ، حافظه کوتاه‌مدت طولانی(LSTM) ، و مدل‌های ترکیبی مانندTSCRNN ، توانایی بالایی در شناسایی الگوهای پیچیده و وابستگی‌های زمانی در داده‌های شبکه نشان داده‌اند. همچنین استفاده از مجموعه‌داده‌های متنوع با ویژگی‌های مختلف به محققان این امکان را داده است که مدل‌های خود را در سناریوهای واقعی تست و ارزیابی کنند. محور های مهم تحقیقاتی در ادامه این کار به شرح زیر می باشد:

۱. بهبود دقت مدل‌ها :با ترکیب فناوری‌های نوین مانند مدل‌های توجه (Attention Mechanism) و معماری‌های پیشرفته مانند ترانسفورمرها، می‌توان دقت مدل‌ها را بهبود بخشید.
۲. استفاده از داده‌های بزرگ‌تر و واقعی‌تر :جمع‌آوری مجموعه‌داده‌های واقعی‌تر و گسترده‌تر که تنوع بیشتری در انواع ترافیک شبکه داشته باشند، می‌تواند عملکرد مدل‌ها را در شرایط واقعی تقویت کند.
۳. کاهش پیچیدگی محاسباتی :بهینه‌سازی مدل‌ها برای کاهش هزینه‌های محاسباتی و زمان آموزش، به ویژه در محیط‌های با منابع محدود، یکی از چالش‌های مهم آینده است.
۴. پشتیبانی از داده‌های بلادرنگ :توسعه مدل‌هایی که توانایی پردازش بلادرنگ ترافیک شبکه را داشته باشند، می‌تواند به بهبود کاربردپذیری در سیستم‌های عملی کمک کند.

۵. بررسی مسائل حریم خصوصی :با توجه به حساسیت اطلاعات ترافیک شبکه، توسعه مدل‌هایی که بدون نیاز به دسترسی مستقیم به داده‌های خام، دسته‌بندی را انجام دهند، حائز اهمیت است.

این پژوهش‌ها می‌توانند به پیشرفت فناوری دسته‌بندی ترافیک رمزگذاری‌شده و بهبود امنیت شبکه‌ها در برابر تهدیدات نوظهور کمک کنند.

فهرست مراجع:

[۱] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in *2017 IEEE international conference on intelligence and security informatics (ISI)*, 2017: IEEE, pp. 43-48 .

[۲] A. Almomani, "Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms," *Egyptian Informatics Journal*, vol. 23, no. 4, pp. 57-68, 2022/12/01/ 2022, doi: https://doi.org/10.1016/j.eij.2022.06.006.

[۳] J. Zhang, X. Chen, Y. Xiang, W. Zhou, and J. Wu, "Robust network traffic classification," *IEEE/ACM transactions on networking*, vol. 23, no. 4, pp. 1257-1270, 2014.

[٤] S. Bagui, X. Fang, E. Kalaimannan, S. C. Bagui, and J. Sheehan, "Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features," *Journal of Cyber Security Technology*, vol. 1, no. 2, pp. 108-126, 2017/04/02 2017, doi: 10.1080/23742917.2017.1321891.

[٥] I. Akbari Azirani, "Encrypted Web Traffic Classification Using Deep Learning," University of Waterloo, 2021.

[٦] F. Pacheco, E. Exposito, M. Gineste, C. Baudoin, and J. Aguilar, "Towards the deployment of machine learning solutions in network traffic classification: A systematic survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1988-2014, 2018.

[۷] Y. Bengio, "Deep learning of representations for unsupervised and transfer learning," in *Proceedings of ICML workshop on unsupervised and transfer learning*, 2012: JMLR Workshop and Conference Proceedings, pp. 17-36.

[۸] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *2017 International conference on information networking (ICOIN)*, 2017 :IEEE, pp. 712-717.

[۹] S. Rezaei and X. Liu, "Deep learning for encrypted traffic classification: An overview," *IEEE communications magazine*, vol. 57, no. 5, pp. 76-81, 2019.

[۱۰] Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," *IEEE transactions on pattern analysis and machine intelligence*, vol. 35, no. 8, pp. 1798-1828, 2013.

[۱۱] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *science*, vol. 313, no. 5 ,۷۸٦pp. 504-507, 2006.

[۱۲] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural computation*, vol. 18, no. 7, pp. 1527-1554, 2006.

[۱۳] Z. Bu, B. Zhou, P. Cheng, K. Zhang, and Z. H. Ling, "Encrypted Network Traffic Classification Using Deep and Parallel Network-in-Network Models," *IEEE Access*, vol. 8, pp. 132950-132959, 2020, doi: 10.1109/ACCESS.2020.3010637.

[۱٤] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in neural information processing systems*, vol. 25, 2012.

[۱٥] F. Hu, S. Zhang, X. Lin, L. Wu, N. Liao, and Y. Song, "Network traffic classification model based on attention mechanism and spatiotemporal features," *EURASIP Journal on Information Security*, vol. 2023, no. 1, p. 6, 2023/07/12 2023, doi: 10.1186/s13635-023-00141-4.

[۱٦] A. Canziani, A. Paszke, and E. Culurciello, "An analysis of deep neural network models for practical applications," *arXiv preprint arXiv:1605.07678*, 2.۰۱٦

[۱۷] D. H. Hubel and T. N. Wiesel, "Receptive fields and functional architecture of monkey striate cortex," *The Journal of physiology*, vol. 195, no. 1, pp. 215-243, 1968.

[۱۸] Z. Zhang, X. Han, Z. Liu, X. Jiang, M. Sun, and Q. Liu, "ERNIE: Enhanced language representation with informative entities," *arXiv preprint arXiv:1905.07129*, 2019.

[۱۹] C. Dos Santos and M. Gatti, "Deep convolutional neural networks for sentiment analysis of short texts," in *Proceedings of COLING 2014, the 25th international conference on computational linguistics: technical papers*, 2014, pp. 69-78.

[۲۰] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[۲۱] M. Lotfollahi, M. Jafari Siavoshani, R. Shirali Hossein Zade, and M. Saberian, "Deep packet: A novel approach for encrypted traffic classification using deep learning," *Soft Computing*, vol. 24, no. 3, pp. 1999-2012, 2020.

[۲۲] S.-H. Noh, "Analysis of Gradient Vanishing of RNNs and Performance Comparison," *Information*, vol. 12, p. 442, 10/25 2021, doi: 10.3390/info12110442.

[۲۳] F. Karim, S. Majumdar, H. Darabi, and S. Chen, "LSTM fully convolutional networks for time series classification," *IEEE access*, vol. 6, pp. 1662-1669, 2017.

[۲٤] C. Li, G. Zhan, and Z. Li, "News text classification based on improved Bi-LSTM-CNN," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, 2018: IEEE, pp. 890-893.

[۲٥] C. Y. Lin, B. Chen, and W. Lan, "An Efficient Approach for Encrypted Traffic Classification using CNN and Bidirectional GRU," in *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, 14-16 Jan. 2022 2022, pp. 368-373, doi: 10.1109/ICCECE54139.2022.9712708.

[۲٦] A. Rogers, O. Kovaleva, and A. Rumshisky, "A primer in BERTology: What we know about how BERT works," *Transactions of the Association for Computational Linguistics*, vol. 8, pp. 842-866, 2021.

[۲۷] X. Lin, G. Xiong, G. Gou, Z. Li, J. Shi, and J. Yu, "ET-BERT: A Contextualized Datagram Representation with Pre-training Transformers for Encrypted Traffic Classification," presented at the Proceedings of the ACM Web Conference 2022, Virtual Event, Lyon, France, 2022. [Online]. Available: https://doi.org/1.۳٤۸٥٤٤۷,۳٥۱۲۲۱۷/۰,۱۱٤٥

[۲۸] Z. Shi, N. Luktarhan, Y. Song, and G. Tian, "BFCN: A Novel Classification Method of Encrypted Traffic Based on BERT and CNN," *Electronics*, vol. 12, no. 3, p. 516, 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/3/.٥۱٦

[۲۹] S. Soleymanpour, H. Sadr, and H. Beheshti, "An efficient deep learning method for encrypted traffic classification on the web," in *2020 6th International Conference on Web Research (ICWR)*, 2020: IEEE, pp. 209-216.

[۳۰] K. Harinath and G. Kishorekumar, "Encrypted Network Traffic Classification and Feature Selection by Ensemble of CNN and TLBO Meta-Heuristic Algorithm," EasyChair, 2516-2314, 2023.

[۳۱] Z. Okonkwo, E. Foo, Q. Li, and Z. Hou, "A CNN Based Encrypted Network Traffic Classifier," presented at the Proceedings of the 2022 Australasian Computer Science Week, Brisbane, Australia, 2022. [Online]. Available: https://doi.org/10.1145/3511616.3513101.

[۳۲] Y. Zhou *et al.*, "Identification of encrypted and malicious network traffic based on one-dimensional convolutional neural network," *Journal of Cloud Computing*, vol. 12, no. 1, p. 53, 2023/04/10 2023, doi: 10.1186/s13677-023-00430-w.

[۳٤] S. Ramraj and G. Usha, "Hybrid feature learning framework for the classification of encrypted network traffic," *Connection Science*, vol. 35, no. 1, p. 2197172, ۲۰۲۳ ۳۱/۱۲/۲۰۲۳doi: 10.1080/09540091.2023.2197172.

[۳٥] S. B. Banihashemi and E. Akhtarkavan, "Encrypted Network Traffic Classification Using Deep Learning Method," in *2022 8th International Conference on Web Research (ICWR)*, 11-12 May 2022 2022, pp. 1 ,۸-doi: 10.1109/ICWR54782.2022.9786247.

[۳٦] M. H. Pathmaperuma, Y. Rahulamathavan, S. Dogan, and A. M. Kondoz, "Deep Learning for Encrypted Traffic Classification and Unknown Data Detection," *Sensors*, vol. 22, no. 19, p. 7643, 2022. [Online]. Available : https://www.mdpi.com/1424-8220/22/19/7643.

[۳۷] R. T. Elmaghraby, N. M. Abdel Aziem, M. A. Sobh, and A. M. Bahaa-Eldin, "Encrypted network traffic classification based on machine learning," *Ain Shams Engineering Journal*, vol. 15, no. 2, p. 102361, 2024/ ,۲۰۲٤ /۰۱/۰۲doi:
K. Lin, X. Xu, and H. Gao, "TSCRNN: A novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT," *Computer Networks*, vol. 190, p. 107974, 2021/05/08/ 2021, doi: https://doi.org/10.1016/j.comnet.2021.107974.

[۳۹] X. Hu, C. Gu, Y. Chen, and F. Wei, "CBD: A Deep-Learning-Based Scheme for Encrypted Traffic Classification with a General Pre-Training Method," *Sensors*, vol. 21, no. 24, p. 8231, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/24/8231.

[٤۰] Z. Shi, N. Luktarhan, Y. Song, and H. Yin, "TSFN: A Novel Malicious Traffic Classification Method Using BERT and LSTM," *Entropy*, vol. 25, no. 5, p. 821, 2023. [Online]. Available: https://www.mdpi.com/1099-4300/25/5/821

[٤۱] Z. Shi, N. Luktarhan, Y. Song, and H. Yin, "TSFN: A Novel Malicious Traffic Classification Method Using BERT and LSTM," *Entropy*, vol. 25, no. 5, p. 821, 2023. [Online]. Available: https://www.mdpi.com/1099-4300/25/5/821

[42] A. W. Moore and D. Zuev, "Internet Traffic Classification Using Bayesian Analysis Techniques," *ACM SIGMETRICS Performance Evaluation Review*, vol. 33, no. 1, pp. 50–60, 2005. [Online]. Available: https://doi.org/10.1145/1071690.1064212

[43] T. Wang, L. Sun, X. Wei, and Y. Wang, "USTC-TFC2016: A dataset of malicious and benign network traffic for research," *International Journal of Network Security*, vol. 20, no. 6, pp. 1202–1212, 2018. [Online]. Available: https://ijns.org

[44] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *Proceedings*

of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116. [Online]. Available: https://doi.org/10.5220/0006639801080116

[45] M. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18–28, 2009. [Online]. Available: https://doi.org/10.1016/j.cose.2008.08.003

[46] K. Fukuda, H. Esaki, and A. Kato, "The MAWI Working Group: Real network traffic and its application to Internet research," *International Journal of Internet Protocol Technology*, vol. 3, no. 1, pp. 1–11, 2008. [Online]. Available: https://mawi.wide.ad.jp

[47] I. Graham and J. Harkins, "Auckland-II Dataset: A network traffic characterization study," *Technical Report*, The University of Auckland, 2000. [Online]. Available: https://www.cs.auckland.ac.nz

[48] R. Fontugne, P. Borgnat, P. Abry, and K. Fukuda, "MAWILab: Combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking," *ACM CoNEXT Conference*, 2010, pp. 1–12. [Online]. Available: https://doi.org/10.1145/1921168.1921173

[49] Y. Zhang and S. Zhou, "Traffic Labeler: A tool for automatic network traffic classification," *IEEE/ACM Transactions on Networking*, vol. 24, no. 4, pp. 2245–2257, 2016. [Online]. Available: https://doi.org/10.1109/TNET.2016.2547903

[50] A. Azab, S. Alrabaee, and K.-K. R. Choo, "Anon17: A dataset for anonymous network traffic analysis," *Digital Communications and Networks*, vol. 10, no. 1, pp. 676–692, 2024. [Online]. Available: https://doi.org/10.1016/j.dcan.2022.09.009

[51] F. Di Franco, G. Anastasi, and M. Conti, "MIRAGE-2019 Dataset: A mobile application dataset for traffic analysis," *IEEE Transactions on Mobile Computing*, vol. 21, no. 6, pp. 1904–1915, 2022. [Online]. Available: https://doi.org/10.1109/TMC.2022.3145567

[52] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2015, pp. 1–6. [Online]. Available: https://doi.org/10.1109/MilCIS.2015.7348942

[53] D. Wang, C. Wang, and T. Zheng, "MobileGT: Mobile application traffic analysis dataset," *Journal of Network and Computer Applications*, vol. 125, pp. 128–140, 2019. [Online]. Available: https://doi.org/10.1016/j.jnca.2018.10.013

تحلیل حملات SSH brute force برای تشخیص نفوذ

مارال صالحی [*۱]، محمد جواد صفری[۲]، محمد مهدی عباسی[۲]

۱- عضو هیات علمی دانشکده ریاضی، آمار و علوم کامپیوتر، دانشگاه سمنان

۲- دانشجوی کارشناسی علوم کامپیوتر، دانشکده ریاضی، آمار و علوم کامپیوتر، دانشگاه سمنان

چکیده

حملات SSH brute force ، از رایج ترین نوع حملات شبکه های کامپیوتری هستند. گزارش های اخیر تجزیه و تحلیل تهدید، به طور مداوم بر شیوع این حملات به عنوان بیشترین آسیب پذیری امنیت وب، تاکید دارند. متدولوژی های فعال و غیر فعال مختلفی توسعه یافته اند که هرکدام مزایا و معایب منحصر به فرد خود را دارند. در بین این روشها، پایش گزارش ها برای درک علت اصلی مشکل و اجرای اقدامات متقابل، مهم هستند. بر همین اساس، این مقاله بر پیاده سازی راه حل های تشخیص نفوذ خودکار، با تجزیه و تحلیل تلاش های ناموفق تاریخی SSH، تمرکز دارد. به همین منظور، ابتدا با تجزیه و تحلیل مجموعه داده، الگوهای رایج در مجموعه داده (مانند مبدأ آدرس های IP ، نام کاربری زمان تلاش SSH) درک شد. سپس انواع مختلفی از الگوهای حمله، از جمله الگوهای پنهان، و آهسته و پیوسته شناسایی شدند. از آنجائیکه گزارش ها شامل هر دو حالت تلاش های مخرب و غیر مخرب بودند، برای دسته بندی آنها به عنوان مخرب و غیر مخرب از پایگاه داده‌های خارجی (به عنوان مثال IPWHOIS وABUSEIPDB) استفاده شد، که به عنوان یک داده ی آموزشی برای مدل های یادگیری ماشین عمل میکند. همچنین چندین مدل یادگیری ماشین ایجاد شد تا بتوان تلاش های SSH را به صورت مخرب یا غیر مخرب دسته بندی نمود. مدل ها، به چندین ویژگی از جمله نام کاربری، تفاوت زمانی حملات، تعداد تلاش های قبلی و شباهت آدرس های IP ، متکی بودند. مدل های متعددی مانند جنگل تصادفی، درخت تصمیم و... آموزش داده شد. در این میان، مدل درخت تصمیم بهترین عملکرد را داشت و دقت ۱۰۰ درصد و نرخ فراخوان ۹۷,۹ را کسب نمود. در مقایسه، بهترین فرمول مبتنی بر قاعده، نتوانست ۱,۵ درصد IP های مخرب را شناسایی کند. درحالیکه مدل درخت تصمیم، فقط ۰,۰۱ درصد را شناسایی نکرد. همچنین، مدل پیشنهادی، پنج آدرس IP مخرب را شناسایی کرد، قبل از آنکه توسط پایگاه داده عمومی مانند ABUSEIPDB شناسایی شوند که نتیجه ای امیدوارکننده برای مدل پیشنهادی است.

کلمات کلیدی: حملات SSH brute force ، سیستم تشخیص نفوذ، امنیت شبکه های کامپیوتری، الگوریتم های یادگیری ماشین، برچسب گذاری مجموعه داده

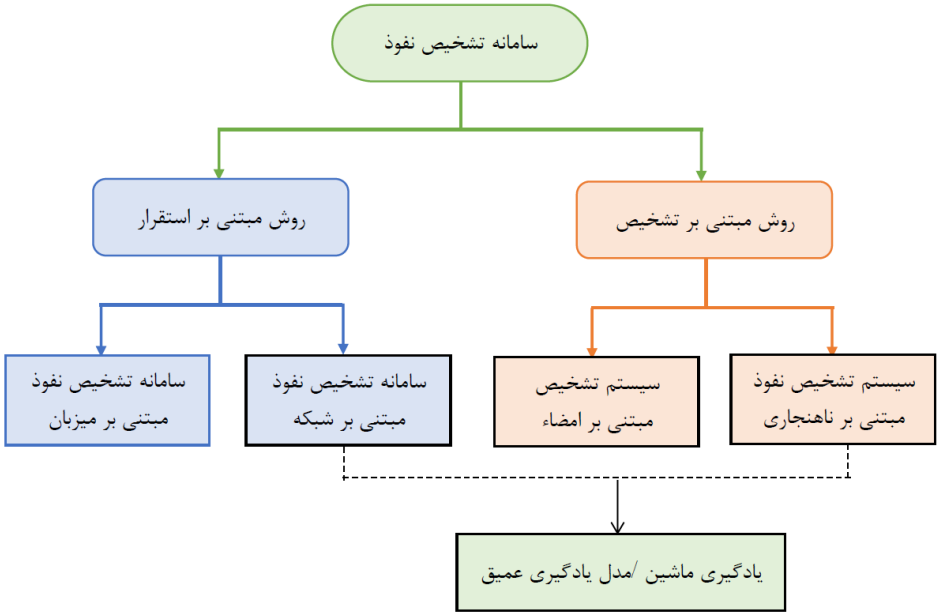
[*] **Corresponding author:**
Email: Maralsalehi@semnan.ac.ir

۱. مقدمه

اینترنت بیشتر از هر زمان دیگری بر زندگی ما تاثیر می‌گذارد. با پیشرفت در هوش مصنوعی، اینترنت اشیاء، روباتیک، سیستم های ابری و...، شبکه های کامپیوتری توانسته اند خدماتی بسیار فراتر از دسترسی به اطلاعات، فراهم آورند و در تعاملات و ارتباطات ما نقش ویژه ای داشته باشند. در کنار این مزایا، تهدیداتی نیز متوجه استفاده کنندگان از اینترنت میباشد.

حملات SSH brute force ، یکی از رایج ترین حملات برای دسترسی از راه دور به سرورها میباشد. این حمله با اینکه قدیمی است ولی همچنان بالاترین آسیب پذیری در امنیت وب محسوب میشود .به طور خلاصه، حمله SSH brute force حمله ای در سطح شبکه های کامپیوتری است که در آن، مهاجم نام های کاربری و رمزهای عبور متعددی را امتحان میکند تا در نهایت بتواند از راه دور وارد سیستم کامپیوتری شود .در این حمله، مهاجم با دسترسی به داده ها و مصرف منابع سیستم (از جمله پردازنده، حافظه و پهنای باند)، به حسن اعتبار کسب و کاری که روی این سیستم در حال اجرا میباشد لطمه میزند و در نهایت منجر به کاهش رضایت مشتریان از خدمات آن کسب و کار میشوند.

برای غلبه بر حملات SSH brute force ، روش های مختلفی به کار گرفته میشوند. اجبار به استفاده از رمزهای عبور قوی، غیر فعال کردن ورود به سیستم در حالت root ، استفاده از احراز هویت دو عاملی، استفاده از سیستم‌های تشخیص نفوذ و غیره. پایش لاگ ها، مرحله مهمی در درک علت اصلی این مشکل و انجام اقدامات احتیاطی، میباشد. سیستم تشخیص نفوذ یا IDS ، سیستمی است که پایش[*] لاگ ها، دسترسی غیرمجاز را تشخیص میدهد. پایش لاگ ها، در سطح میزبان (سیستم تشخیص نفوذ مبتنی بر میزبان یا HIDS[†]) یا در سطح شبکه (سیستم تشخیص نفوذ مبتنی بر شبکه یا NIDS[‡]) انجام میشود. ایراد سیستم تشخیص نفوذ مبتنی بر میزبان، ضعف آن در مقیاس پذیری میباشد و زمان و هزینه پردازشی زیادی برای مقیاس پذیری، به همراه دارد. در مقابل، سیستم تشخیص نفوذ مبتنی بر شبکه، به طور مداوم ترافیک شبکه را بررسی نموده و به منظور محافظت از دستگاه ها، هر تهدید احتمالی را پایش میکند.



شکل ۱- دسته بندی روش های تشخیص نفوذ [۱]

[*] Intrusion Detection System
[†] Host-based Intrusion Detection System
[‡] Network-based Intrusion Detection System

از منظر دیگر، تشخیص نفوذ به دو روش انجام می‌شود. تشخیص نفوذ مبتنی بر امضا و مبتنی بر تشخیص ناهنجاری. سیستم تشخیص نفوذ مبتنی بر امضا، برای تهدیدات شناخته شده موثر است زیرا الگوی آن فرموله شده و در پایگاه داده ذخیره می‌شود. زمانیکه الگوی داده با یکی از الگوهای ذخیره شده مطابقت داشته باشد زنگ هشدار به صدا درمی‌آید. از طرف دیگر، اگر الگوی حمله ی جدیدی پدید آید که قبلاً تجربه نشده است این روش اشتباه میکند و آنرا تشخیص نمی‌دهد. سیستم های تشخیص نفوذ مبتنی بر ناهنجاری، بر اساس رفتار فعالیت غیرمخرب عمل میکنند. اگر فعالیتی از این رفتار عدول نماید، فعالیتی مخرب به حساب می‌آید. این روش، برخلاف روش قبلی، حملات جدید را به خوبی تشخیص می‌دهد. با این وجود، نرخ خطای بیشتری نسبت به روش قبلی دارد و چون تنظیم مرز بین الگوی داده های مخرب و غیرمخرب مشکل است، این روش زمان و هزینه ی زیادی را به سیستم تحمیل میکند. به طور خلاصه، سیستم تشخیص نفوذ مبتنی بر امضا، از قوانین و آستانه ها برای تشخیص فعالیت های مخرب استفاده میکند. درحالیکه، سیستم تشخیص نفوذ مبتنی بر ناهنجاری، از مدل‌های یادگیری ماشین و یادگیری عمیق بهره می‌برد، که هرکدام مزایا و معایب خود را دارند [۱]،[۵].

مطالعات اخیر در مورد تشخیص نفوذ، مدل‌های یادگیری ماشین و یادگیری عمیق، در تشخیص رفتارهای مخرب تمرکز دارند. برچسب گذاری مجموعه داده‌ها، همچنان امری حیاتی و در عین حال زمانبر و متمرکز بر دانش می‌باشد. بدون برچسب گذاری دقیق مدل‌ها ممکن است آنطور که انتظار می‌رود عمل نکنند و دقت و صحت حاصل منعکس کننده نتایج واقعی نباشد. این مطالعه با مجموعه داده‌های جدید و توصیف نحوه برچسب گذاری آنها، سهمی در برچسب گذاری دقیق مجموعه داده‌ها دارد.

طبق بررسی‌های انجام شده، هیچ معیار مشخصی برای ارزیابی وجود ندارد. این وضعیت به ویژه در مواردی که از مجموعه داده‌های نامتعادل استفاده می‌شود مقایسه نتایج را چالش برانگیز می‌کند. در این مطالعه از ماتریس سردرگمی به عنوان آموزنده‌ترین معیار ارزیابی برای مشاهده نتایج مثبت کاذب و منفی کاذب استفاده شده است. علاوه بر این، هر سازمانی ترافیک شبکه منحصر به فرد خود را دارد که منجر به الگوهای ترافیکی متفاوت بر اساس فعالیت‌های وب سازمان می‌شود. بنابراین تنظیم دقیق مدل‌ها با توجه به خصوصیات هر شبکه بسیار مهم است. این مطالعه بر شناسایی فعالیت‌های مخرب با اطلاعات محدود تمرکز دارد و منبع اصلی گزارش‌ها فایل btmp لینوکس در دایرکتوری var/log می‌باشد. فایل btmp تمام تلاش‌های ناموفق برای ورود را ثبت می‌کند. در این مطالعه از سه ویژگی نام کاربری, نام میزبان و تاریخ استفاده شده است. همانطور که قبلاً ذکر شد، یکی از اشکالات سیستم‌های مبتنی بر میزبان،عدم مقیاس پذیری آنها است. با این حال، لاگ های مهم مانند گزارش‌های امنیتی (از جمله تلاش‌هایی برای ورود به سیستم)، گزارش‌های سیستم و گزارش‌های برنامه معمولا به راه حل های SIEM ارسال می‌شوند. این عمل به طور قابل توجهی، به مقیاس پذیر کردن سیستم‌های مبتنی بر میزبان کمک می‌کند. در حالی که مطالعات قبلی بر راه حل‌های مبتنی بر شبکه متمرکز بودند، این مطالعه با داشتن مجموعه داده جدید که به دقت برچسب گذاری شده‌اند و شامل ویژگی‌های کمتر ولی مهم‌تر و معیارهای ارزیابی قابل اعتمادتری هستند، به روش یادگیری ماشین و بر رویکرد مبتنی بر میزبان تمرکز دارد.

۲. بررسی پیشینه و مفاهیم

۱.۲. SSH و لاگ های لینوکس

SSH، پروتکل رمزنگاری در شبکه، راهکاری امن برای ورود به سیستم کامپیوتری از راه دور و با اجرای خط فرمان می‌باشد. Telnet در سال ۱۹۶۹ و با هدف دسترسی از راه دور به سیستم کامپیوتری توسعه یافت ولی به خاطر رمز نشدن دستورات و داده‌های آن، خود یک خطر امنیتی برای دسترسی مهاجمان به سیستم کامپیوتری محسوب می‌شد. برای رفع این نقص ایمنی، SSH در سال ۱۹۹۵ توسط دانشمند فنلاندی طراحی و عرضه شد. طراحی شفاف، سادگی اجرا و استقلال از زیرساخت‌های متمرکز به SSH کمک کرد تا به عنوان راه حل ارتباطی ایمن مورد پذیرش جهانی قرار گیرد. SSH یکی از

محبوب‌ترین پروتکل‌های ارتباطی اینترنت است که توسط توسعه دهندگان سیستم، به عنوان راه حل ارتباطی امن ارائه شده است. به این ترتیب و با به کارگیری SSH، امکان دسترسی از راه دور به سیستم با استفاده از کانال ارتباطی رمزنگاری شده فراهم می‌شود.

سیستم عامل لینوکس، اطلاعات مربوط به امنیت را در پوشه var/log ثبت می‌کند. چهار فایل کلیدی زیر مربوط به فعالیت SSHهستند. var/log/auth شامل اطلاعات سطح دسترسی کاربران در سیستم، var/log/utmp شامل رکوردهایی که در حال حاضر وارد سیستم شده‌اند. var/log/wtmp شامل تمامی ورودها (فعلی و گذشته) به سیستم، var/log/btmp شامل تمام تلاش‌های ناموفق (مخرب) برای ورود میباشد. هنگامی که مهاجم یا کاربر غیر مجاز تلاش می‌کند به سیستم دسترسی پیدا کند، سعی می‌کند با وارد کردن چندین نام کاربری و رمز عبور از راه دور به سیستم متصل شود. برای به دست آوردن نام کاربری و رمز عبور، مهاجمان اغلب دست به حمله SSH brute force می‌زنند و دائماً تلاش می‌کنند تا از ترکیب‌های مختلف نام کاربری و رمز عبور برای نقض امنیت سیستم استفاده نمایند. این گزارش‌ها اطلاعات ضروری را در مورد اینکه چه کسی در چه زمانی و چند بار وارد سیستم شده است ارائه می‌کنند.

۲.۲. حملات SSH brute force

حمله SSH brute force، اغلب با هدف ورود به سیستم کامپیوتری انجام می‌شود، با این حال مهاجمان اهداف دیگری را نیز دنبال می‌کنند، از جمله دستیابی به صفحات یا محتوای پنهان یک سیستم، رمزگشایی از مقادیر شناسه جلسه، شکستن رمزهای عبور یکبار مصرف، آشکارسازی اطلاعات کارت اعتباری، توابع هش رمزنگاری معکوس و تمام کردن منابع سیستم کامپیوتری. این موارد در نهایت موجب بدتر شدن کیفیت خدمات یا از کار انداختن سیستم می‌شوند. حمله SSH brute force، یکی از ساده‌ترین و قدیمی‌ترین نوع حمله در حوزه امنیت سیستم‌های کامپیوتری است که پیامدهای آن ممکن است تاثیر قابل توجهی داشته باشد. در گزارش ریسک امنیتی منتشر شده در سال ۲۰۰۷، حمله SSH brute force را به عنوان یکی از رایج‌ترین حملات گزارش کردند. همچنین در سال ۲۰۲۱ (شکل ۲) ، OWASP* اعلام کرد کنترل دسترسی نقض شده رایج‌ترین آسیب پذیری در این سال می‌باشد.

۱.۲.۲. انواع حملات SSH brute force بر اساس حدس زدن

رمز عبور حملات SSH brute force انواع مختلفی دارند که هر کدام برای رسیدن به رمز عبور، روش خاص خود را دارند.

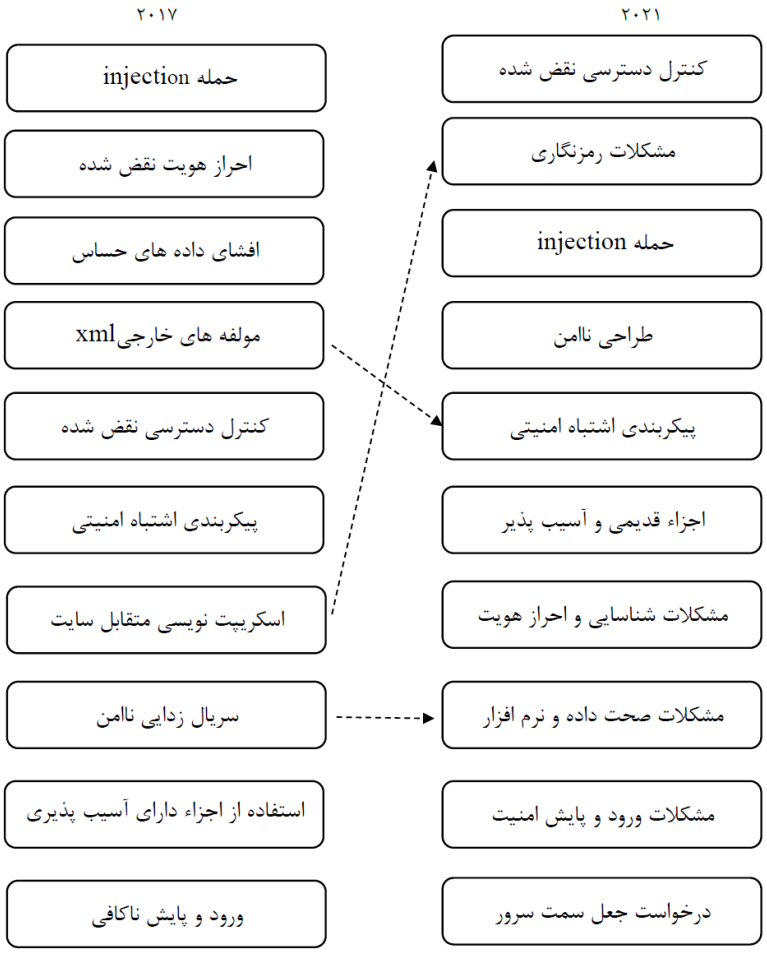
الف) حملات ساده، در این روش، مهاجم بدون اتکا به نرم‌افزار یا ابزار، سعی می‌کند رمز عبور را حدس بزند. این روش برای رمزهای ساده استفاده می‌شود.

ب) حملات لغت‌نامه‌ای، در این روش از فرهنگ لغت استفاده می‌شود و هر ترکیبی از کلمات و کاراکترها که در فرهنگ لغت آمده باشد در این حمله امتحان می‌شود.

ج) حمله معکوس، در این روش مهاجم با یک رمز عبور شناخته شده یا فاش شده حمله را شروع می‌کند و این رمز را بر روی میلیون‌ها نام کاربری امتحان می‌کند.

د) به کارگیری اعتبار، وقتی مهاجم موفق می‌شود با نام کاربری و رمز عبور وارد حساب کاربری در یک سایت شود، آن نام کاربری و رمز عبور را در سایت‌های دیگر نیز امتحان می‌کند. این استراتژی این روش به طور خاص کاربرانی را هدف قرار می‌دهد که از رمز عبور تکراری در چندین سایت استفاده می‌کنند.

*OWASP: Open Worldwide Application Security Project



شکل ۲- بیشترین آسیب پذیری ها در سال ۲۰۲۱ به نقل از OWASP [۲]

۲.۲.۲. انواع حملات brute force بر اساس منبع حملات

brute force را می‌توان بسته به اینکه از یک منبع واحد و یا چندین منبع توزیع شده ارسال می‌شوند دسته‌بندی نمود. بر همین اساس روش‌های امنیتی موثری برای شناسایی و کاهش این تهدیدها پیشنهاد شده است. [۷]

الف) حملات تک منبع

در این سناریو، مهاجمان از یک کامپیوتر برای اجرای حمله استفاده می‌کنند. شناسایی این حمله در مقایسه با انواع دیگر ساده‌تر است، با این وجود زمانی که مهاجم از روش‌های طفره رفتن استفاده کند حمله تک منبع همچنان می‌تواند تهدید مهمی به حساب آید.

ب) حملات تک دامنه

در این نوع حملات، مهاجمان از کامپیوترهای مختلفی که همگی در یک منطقه قرار دارند (در یک شهر، در یک کشور) و پیشوند آدرس‌های IP مشابهی دارند حمله می‌کنند.

ج) حملات توزیع شده

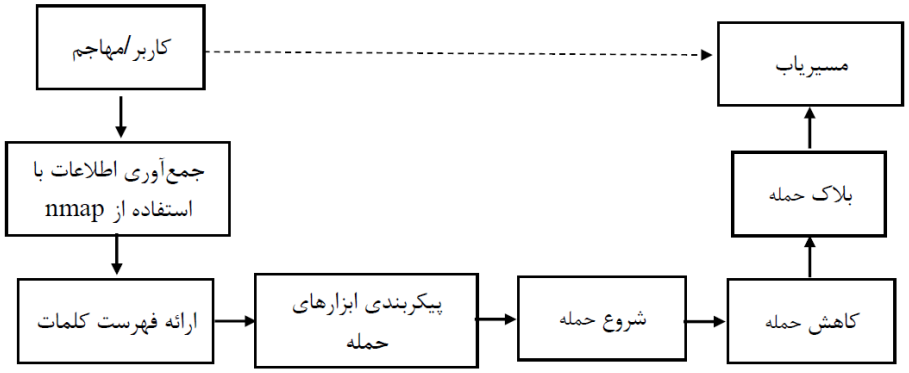
در حملات توزیع شده، مهاجمان شبکه‌ای از کامپیوترهای توزیع شده در سراسر جهان را سازماندهی می‌کنند (بدون تشابه در پیشوند آدرس‌های IP). اگر مهاجمان حمله خود را در طولانی مدت گسترش دهند تشخیص این حملات دشوار خواهد بود.

۳.۲.۲. ابزارهای مورد استفاده در حملات brute force

ابزارهای متعددی برای حمله brute force وجود دارد که هر کدام ویژگی‌های خاصی دارند و از پروتکل‌ها و سیستم عامل‌های مختلف پشتیبانی می‌کنند. به طور مثال, ابزارهایی که برای حمله brute force با پروتکل SSH استفاده می‌شود عبارتند از BruteX، Secure Shell Bruteforcer (SSB)، Patator و Ncrack. همچنین بات نت جدید به نام RapperBot بر سرورهای لینوکس تمرکز دارد و از ۳۵۰۰ آدرس IP منحصر به فرد برای دستگاه‌های اینترنت اشیا استفاده می‌کند.

۴.۲.۲. روش‌های کاهش حمله brute force

قبل از انجام اقدامات پیشگیرانه، بایستی درک کاملی از مراحل حمله brute force داشت. قبل از آغاز حمله به سیستم، بایستی حمله را شناسایی کرد. این شناسایی توسط ابزارهای پایش شبکه (مانند nmap) یا به کارگیری لیست‌هایی که در دسترس عموم هستند، شامل اهداف بالقوه (مشابه آنچه در ParstBin انجام شده) یا خدمات به دست آمده مانند Shadon انجام می‌شود. پس از شناسایی، حمله brute force ممکن است رخ دهد. بنابراین در صورتی که مستندات معتبر شناسایی حمله را تایید می‌کنند, مرحله سازش (توافق) آغاز می‌شود. به طور خلاصه حملات brute force سه مرحله دارند. مرحله پایش و به دنبال آن مرحله شناسایی حمله و در صورت موفقیت آمیز بودن حمله، مرحله سازش (توافق).



شکل ۳- مراحل حمله [۳]

روش‌های پیشگیری فعال و غیر فعال مختلفی برای مقابله با حمله brute force وجود دارد که هر کدام مزایا و معایب خود را دارند. با به کارگیری ترکیبی از این روش‌ها و بر اساس اهداف و نیازهای خاص و با در نظر گرفتن عوامل امنیتی، دسترسی و هزینه، می‌توان به امنیتی قوی و عمیق دست یافت.

الف) تشویق به استفاده از رمزهای عبور قوی و طولانی

طول رمز عبور و پیچیدگی آن بر زمان شکستن رمز عبور تاثیر می‌گذارد. جدول زیر، زمان لازم برای شکستن رمز عبور با در نظر گرفتن طول و پیچیدگی آن و با قدرت کرک ۶۳۲ میلیارد رمز عبور جدید در هر ثانیه را نشان می‌دهد.

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years

شکل ۴- زمان لازم برای شکستن رمز عبور [۴]

ب) اعمال محدودیت در تعداد تلاش‌های ناموفق برای ورود به سیستم

بعد از چند تلاش ناموفق برای ورود به سیستم، محدودیتی اعمال شود به این صورت که حساب کاربری به طور موقت غیر فعال شود یا با تاخیر به کاربر پاسخ داده شود یا از CAPTCHA استفاده شود. در این صورت اقدام متقابل مهاجم ممکن است حملات DOS و DDOS باشد که در آن, کاربران مخرب با ارسال درخواست‌های مکرر, سیستم را از دسترس خارج می‌کنند تا کاربر مجاز امکان فعالیت و ورود به سیستم را نداشته باشد.

ج) استفاده از احراز هویت دو عاملی

احراز هویت دو عاملی موجب افزایش امنیت می‌شود. این روش به خاطر هزینه‌های راه‌اندازی و مدیریت مداوم، پیچیدگی‌های بیشتری را شامل می‌شود.

د) استفاده از لیست سیاه آدرس‌های IP

استفاده از این روش در برابر تهدیدات شناخته شده و داشتن واکنش سریع به حوادث، بسیار موثر است. با این حال، به دلیل ماهیت پویای تخصیص آدرس ,IP این لیست‌ها کافی نیستند و مهاجمان میتوانند با دستکاری آدرس‌های IP حملات خود را انجام می‌دهند.

ه) استفاده از احراز هویت مبتنی بر کلید عمومی

استفاده از این روش می‌تواند به جلوگیری از حملات brute force ی که با فراهم آوردن امنیت کلید عمومی، بدون سازش باقی مانده‌اند کمک کند. [۸]

و) پایش لاگ ها

پایش لاگ ها امکان تشخیص زود هنگام حملات brute force را فراهم می‌کند. در این روش، امکان مداخله به موقع قبل از آنکه دسترسی غیر مجاز به سیستم صورت پذیرد فراهم می‌باشد. همچنین با پایش لاگ ها امکان ردیابی منبع حملات brute force، مسدود کردن آدرس‌های IP ، شناسایی تکنیک‌ها تاکتیک‌ها و رویه‌های مهاجمان، فراهم می‌شود.

۳.۲. کارهای انجام شده

ایده تشخیص نفوذ در شبکه های کامپیوتری به سال ۱۹۸۰ برمیگردد و از آن زمان پیشرفت های زیادی در سیستم های تشخیص نفوذ صورت گرفته است. در سال‌های اخیر، محققان اثربخشی مدل های یادگیری ماشین و یادگیری عمیق در

ترافیک شبکه برای شناسایی فعالیت های مخرب را بررسی کرده اند .سیستم های تشخیص مبتنی بر یادگیری ماشین برای پیش بینی نتایج، در درجه اول به مهندسی ویژگی توجه میکنند، درحالیکه سیستم های مبتنی بر یادگیری عمیق بر داده های خام عمل میکنند و هزینه های بالاتری را متحمل میشوند و اطلاعات ویژگی های قابل توضیح کمتری را فراهم مینمایند . همانطور که در بخش مقدمه ذکر شد، دو روش تشخیص مبتنی بر امضا و مبتنی بر تشخیص ناهنجاری وجود دارد که هریک مزایا و معایبی دارند. سیستم مبتنی بر امضا، کارآیی خوبی در برابر تهدیدات شناخته شده دارند و سریعتر هستند، اما در برابر حملات جدید شکست میخورند .در مقابل، سیستم های مبتنی بر ناهنجاری در تشخیص حملات روز صفر برتری دارند اما اغلب با نرخ هشدار نادرست بیشتر و زمان بررسی طولانی تر و هزینه های اضافی بیشتری همراه هستند. [۶]
بررسی جامع ارائه شده در مرجع [۵]، مطالعات صورت گرفته بین سال‌های ۲۰۱۷ و ۲۰۲۰ را بیان می‌نماید. در این مطالعات از مجموعه داده های KDD Cup'99 وNSL-KDD مقالات مرتبط استفاده شده است .همچنین مطالعات اخیر، بر مدل های یادگیری ماشین و یادگیری عمیق تمرکز دارند و به کارگیری مجموعه داده هایCIC-IDS 2018 انتخاب برجسته ای به شمار میرود .با این وجود، به دلیل تفاوت در ویژگی ها و معیارهای ارزیابی، نتایج متفاوت هستند. کمبود جزئیات روشن در مطالعات مربوط نحوه ی تقسیم و آموزش داده ها احساس میشود.

۳. روش پژوهش

۱.۳. مجموعه داده مورد استفاده

در مطالعه ما برای شناسایی حملات بروت‌فورس SSH با استفاده از الگوریتم‌های یادگیری ماشین، از ترکیبی دیتاستی از پلتفرم کگل، یک پلتفرم برجسته برای داده‌نگاری و علاقه‌مندان به یادگیری ماشین، به دست آمده بود استفاده کردیم.

۱.۱.۳. توضیحات دیتاست

این دیتاست شامل ورودی‌های لاگ از سرورهای SSH است که ویژگی‌های مختلف مربوط به تلاش‌های ورود را ثبت می‌کند. این دیتاست شامل حدود ۲۸۰۰۰ رکورد است که هرکدام شامل زمان‌سنجی‌ها، آدرس‌های IP مبدا و مقصد، شناسه‌های کاربری و نتیجه تلاش‌های ورود (موفق یا ناموفق) می‌باشد. این مجموعه غنی از ویژگی‌ها امکان تحلیل دقیق الگوهایی که نشان‌دهنده حملات بروت‌فورس هستند را فراهم می‌آورد.

۲.۱.۳. پیش‌پردازش داده‌ها

برای اطمینان از قابلیت استفاده داده‌ها، چندین مرحله پیش‌پردازش انجام دادیم. ابتدا، مقادیر گمشده را با حذف یا جایگزینی آن‌ها پردازش کردیم تا از کامل بودن داده‌ها اطمینان حاصل شود. سپس، رکوردهای تکراری را حذف کردیم تا از تأثیر داده‌های اضافی بر آموزش مدل جلوگیری شود. علاوه بر این، نوع داده‌ها را استاندارد کردیم تا از انسجام فرمت‌ها در تمام فیلدها اطمینان حاصل کنیم و این کار برای تحلیل‌های بعدی تسهیل شود.

۳.۱.۳. مهندسی ویژگی‌ها

علاوه بر داده‌های خام، ویژگی‌های جدیدی برای تقویت توانایی مدل در شناسایی حملات ایجاد کردیم. این ویژگی‌ها شامل محاسبه فراوانی تلاش‌های ورود از آدرس‌های IP خاص در یک بازه زمانی معین و شناسایی الگوهای غیرمعمول در تلاش‌های ناموفق ورود بودند.

۴.۱.۳. برچسب‌گذاری داده‌ها

دیتاست برای تفکیک فعالیت‌های ورود عادی از حملات بروت‌فورس برچسب‌گذاری شد. برای این کار از یک معیار از پیش تعریف‌شده به عنوان تلاش‌های ناموفق برای ورود برای برچسب گذاری استفاده کردیم.

۵.۱.۳. مناسب بودن برای تحقیق

این دیتاست برای تحقیق ما بسیار مناسب است زیرا نمایشی واقع‌گرایانه از فعالیت‌های ورود SSH را ارائه می‌دهد، شامل الگوهای عادی و حملات. این به ما این امکان را می‌دهد که مدل‌های یادگیری ماشین را به‌طور مؤثر آموزش داده و ارزیابی کنیم و عملکرد آن‌ها را در شناسایی حملات بروت‌فورس بررسی کنیم.

۲.۳. الگوریتم‌های یادگیری ماشین مورد استفاده

الگوریتم‌های یادگیری ماشین نقش مهمی در شناسایی ناهنجاری‌ها، به ویژه در امنیت سایبری دارند. روش‌های تجمیعی و شبکه‌های عصبی معمولاً به دلیل قدرت و توانایی آن‌ها در شبیه‌سازی الگوهای پیچیده داده‌ها ترجیح داده می‌شوند.

۱.۲.۳. جنگل تصادفی

جنگل تصادفی یک روش یادگیری تجمیعی است که چندین درخت تصمیم را ترکیب می‌کند تا دقت پیش‌بینی را افزایش داده و از اورفیتینگ جلوگیری کند. این روش بسیار انعطاف‌پذیر است و می‌تواند به طور مؤثر برای کارهای طبقه‌بندی و رگرسیون استفاده شود. جنگل تصادفی برای مشکل ما مناسب است زیرا قادر است داده‌های بزرگ را مدیریت کند و مکانیسم درونی برای کاهش اورفیتینگ دارد.

۲.۲.۳. XGBOOST

یک چارچوب تقویت گرادیان است که یک تجمیع از مدل‌های پیش‌بینی ضعیف، معمولاً درخت‌های تصمیم، می‌سازد. این الگوریتم به دلیل کارایی بالا و عملکرد برتر در رقابت‌های یادگیری ماشین شناخته شده است. قابلیت مقیاس‌پذیری و توانایی مدل‌سازی تعاملات پیچیده ویژگی‌ها باعث می‌شود که XGBoost گزینه مناسبی برای دیتاست ما باشد.

۳.۲.۳. شبکه عصبی

در این روش از یک شبکه عصبی پیش‌خور با چندین لایه پنهان استفاده شده است که هر لایه از توابع فعال‌سازی خاص خود بهره می‌برد. شبکه‌های عصبی توانایی بالایی در شناسایی روابط غیرخطی دارند و به همین دلیل برای شناسایی الگوهای پیچیده در تلاش‌های ورود به سیستم بسیار مناسب هستند. این ویژگی آن‌ها را قادر می‌سازد تا به‌طور مؤثر ناهنجاری‌ها و الگوهای پیچیده را در داده‌های ورودی تشخیص دهند.

۳.۳. روش ارزیابی

۱.۳.۳ دقت (Accuracy)

دقت نسبت پیش‌بینی‌های صحیح (چه مثبت و چه منفی) به تعداد کل پیش‌بینی‌ها گفته می‌شود که طبق معادله (۱) بیان میشود.

$$\text{Accuracy}=\frac{TP+TN}{TP+FP+TN+FN} \quad (۱)$$

که در این معادله TP = مثبت‌های صحیح (True Positives)، TN = منفی‌های صحیح (True Negatives)
FP = مثبت‌های غلط (False Positives)، FN = منفی‌های غلط (False Negatives)

۲.۳.۳. صحت (Precision)

نسبت پیش‌بینی‌های درست مثبت به مجموع پیش‌بینی‌های مثبت را طبق معادله (۲) صحت گویند

$$\text{Precision}=\frac{TP}{TP+FP} \quad (۲)$$

۳.۳.۳. فراخوانی (Recall)

نسبت پیش‌بینی‌های درست مثبت به مجموع موارد واقعی مثبت فراخوانی گفته میشود.

$$\text{Recall}=\frac{TP}{TP+FN} \quad (۳)$$

۴.۳.۳. نمره F1 (F1 Score)

نمره F1 میانگین هارمونیک دقت و فراخوانی میباشد که اندازه‌گیری متوازن از هر دو ارائه می‌دهد.

$$\text{F1-Score}=2\times\frac{\text{Precision}}{\text{Precision}+\text{Recall}} \quad (۴)$$

۴. نتایج

در این بخش، نتایج عملکرد مدل‌های یادگیری ماشین که برای شناسایی حملات brute force SSH استفاده شده‌اند، ارائه می‌شود. مدل‌های ارزیابی‌شده شامل Random Forest ، XGBoost و یک شبکه عصبی هستند، و معیارهای ارزیابی شامل دقت، صحت، فراخوانی و نمره F1 در نظر گرفته شده‌اند.

۱.۴ عملکرد مدل ها

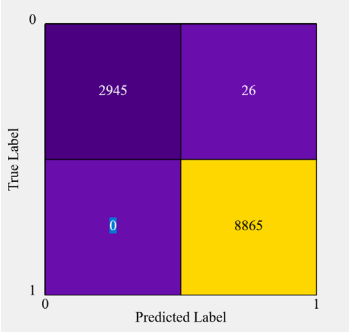
میانگین نتایج عملکرد مدل‌ها در جدول ۱ خلاصه شده است.

جدول ۱- میانگین نتایج عملکرد مدل‌ها

مدل	دقت	صحت	یادآوری	نمره F1
جنگل تصادفی	۰,۹۹۸۳	۰,۹۹۷۹	۰,۹۹۹۸	۰,۹۹۸۸
XGBoost	۰,۹۹۷۸	۰,۹۹۷۰	۱,۰	۰,۹۹۸۴
شبکه عصبی	۰,۹۹۶۵	۰,۹۹۵۵	۰,۹۹۹۸	۰,۹۹۷۶

۱.۱.۴. XGBoost

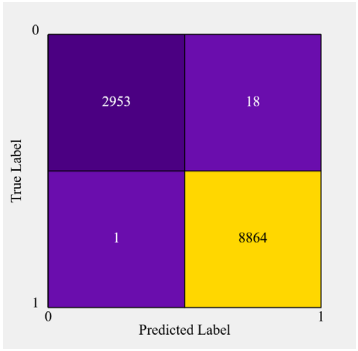
در اولین تعامل مدل XGBoost با آدرس‌های IP جدید که قبلاً دیده نشده بودند، این مدل ۲۶ نمونه را به اشتباه به‌صورت False Positive (FP) طبقه‌بندی کرد (شکل ۵). در زمینه False Negatives (FN) مدل ۰ نمونه را اشتباه طبقه‌بندی کرد. به طور کلی، مدل XGBoost عملکرد خوبی داشت و هیچ موردی از False Negatives نداشت.



شکل ۵- ماتریس سردرگمی مدل XGBoost

۲.۱.۴. جنگل تصادفی

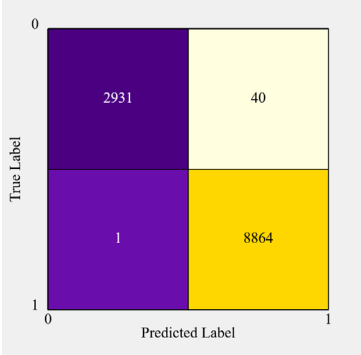
جنگل تصادفی ۱۸ مورد FP داشت (شکل ۶). مدل Random Forest یک مدل یادگیری ماشین نظارت‌شده است که چندین درخت تصمیم‌گیری تصادفی را ترکیب کرده و پیش‌بینی‌های آن‌ها را از طریق میانگین‌گیری ادغام می‌کند. این مدل به دلیل دقت بالا و توانایی آن در کار با اندازه نمونه‌های کوچک و فضای ویژگی‌های با ابعاد بالا شناخته شده است.



شکل ۶- ماتریس سردردگمی مدل جنگل تصادفی

۳.۱.۴. شبکه عصبی

شبکه عصبی ۴۰ مورد FP داشت (شکل ۷). مدل Neural Network یکی از مدل‌های پیشرفته یادگیری ماشین است که از ساختارهای الهام گرفته از مغز انسان برای پردازش داده‌ها استفاده می‌کند .این مدل از لایه‌های متعددی از نورون‌ها تشکیل شده که هر کدام وزن‌های قابل تنظیم دارند و از طریق فرآیندهای غیرخطی برای پیش‌بینی یاد می‌گیرند. شبکه عصبی به دلیل توانایی آن در یادگیری روابط پیچیده بین داده‌ها و مدیریت ویژگی‌های غیرخطی شناخته شده است .مدل Neural Network عملکردی مشابه با XGBoost داشت، اما در برخی از موارد خاص، به دلیل پیچیدگی بیشتر، مدت زمان آموزش طولانی‌تر و نیاز به داده‌های بیشتر برای بهبود دقت مشاهده شد. این مدل توانایی خوبی در تشخیص الگوهای پیچیده از داده‌ها داشت، اما در مقابله با داده‌های نامتوازن کمی چالش‌برانگیز بود.



شکل ۷- ماتریس سردرگمی شبکه عصبی

۵. نتیجه‌گیری

در این پژوهش، از سه الگوریتم یادگیری ماشین شامل XGBoost، شبکه عصبی و جنگل تصادفی برای تحلیل و پیش‌بینی داده‌ها استفاده شد. دقت این الگوریتم‌ها به ترتیب ۰,۹۹۷۸، ۰,۹۹۶۵ و ۰,۹۹۸۳ به دست آمد. با توجه به نتایج به‌دست‌آمده، هر سه الگوریتم عملکرد بسیار مطلوبی در تحلیل داده‌ها داشتند و توانستند به دقتی نزدیک به یک دست یابند، که نشان‌دهنده تطابق بالای مدل‌ها با داده‌های مسئله است. بر اساس مقایسه انجام‌شده، الگوریتم جنگل تصادفی با دقت ۰,۹۹۸۳ بهترین عملکرد را از خود نشان داد. این نتیجه می‌تواند به دلیل توانایی بالای این الگوریتم در مدل‌سازی داده‌های چند بعدی باشد. از سوی دیگر، الگوریتم‌های XGBoost و شبکه عصبی نیز با دقت‌های مشابه ۰,۹۹۷ عملکرد قابل‌توجهی ارائه دادند، که حاکی از قدرت این مدل‌ها در مدیریت داده‌های پیچیده و جلوگیری از بیش‌برازش است. این نتایج نشان می‌دهد که انتخاب مدل مناسب بسته به نوع داده‌ها و هدف مسئله می‌تواند تفاوت قابل‌توجهی در عملکرد ایجاد کند. به‌طور کلی، هر سه الگوریتم

در این مطالعه به‌عنوان ابزارهای قابل اعتماد برای تحلیل داده‌های موردنظر تأیید شدند و می‌توانند در پروژه‌های مشابه مورد استفاده قرار گیرند.

مراجع

[1] N. Sultana, N. K. Chilamkurti, W. Peng, and R. Alhadad, “Survey on sdn based network intrusion detection system using machine learning approaches,” *Peer-to-Peer Networking and Applications*, vol. 12, pp. 493–501, 2019.

[2] “Top 10 Web Application Security Risks,” [https://owasp.org/www-project-top-ten/], 2021.

[3] [5] C. Pamungkas, P. Hendradi, D. Sasongko, and A. Ghifari, “Analysis of brute force attacks using national institute of standards and technology (nist) methods on routers,” *Journal of Informatics Information System Software Engineering and Applications*, vol. 5, no. 2, pp. 115–125, 2023.

[4] “Password cracking speed,” [https://thesecurityfactory.be/password-cracking-speed/], 2020.

[5] [7] Z. Ahmad, A. S. Khan, W. S. Cheah, J. bin Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, 2020.

[6] A. Alkan, “Analysis of Failed SSH Attempts for Intrusion Detection”, Master of Science Theis in Computer Science and Engineering, University of Nevada, Reno, 2024

[7] N. Tiwari and N. Hubballi, “Secure socket shell bruteforce attack detection with petri net modeling,” *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 697–710, 2023.

[8] P. Khandait, N. Tiwari, and N. Hubballi, “Who is trying to compromise your SSH server? an analysis of authentication logs and detection of bruteforce attacks,” *International Conference on Distributed Computing and Networking*, 2020

بررسی چالش ها و راهکارهای تامین امنیت و حریم خصوصی کاربران، در شبکه‌های خانگی هوشمند

مارال صالحی [*1,]

۱- هیات علمی، دانشکده آمار، ریاضی و علوم کامپیوتر، دانشگاه سمنان

چکیده

امروزه با گسترش کاربردهای اینترنت، عملکردهای جدی‌تری برای آن در سرتاسر دنیا رواج یافته است. حضور در محیط کار از راه دور، آموزش و یادگیری مجازی، خرید اینترنتی و...، برای بسیاری از افراد تبدیل به روال معمول زندگی‌شان شده است که در تمامی آنها استفاده از اینترنت خانگی و عملکرد درست شبکه وای فای از ضروریات محسوب می‌شود. یک شبکه خانگی معمولی، شامل یک روتر متصل به مودم، و تجهیزاتی است که دستگاه‌های هوشمند درون خانه را به اینترنت متصل می‌کنند. روتر، سیگنال‌های بیسیم را تا جایی که ممکن است به نقاط دور در داخل خانه ارسال می‌کند، اما دیوارها، مبلمان، مصالح ساختمانی و سایر موانع و نیز دور شدن کاربر از روتر، بر انتشار سیگنال‌های بی‌سیم در سرتاسر خانه تاثیر می‌گذارند و آنها را تضعیف می‌کنند. اینجاست که لزوم استفاده از شبکه‌های مش نمایان می‌شود. یک شبکه مش از چندین گره یا روتر استفاده می‌کند. این گره‌ها می‌توانند با یکدیگر ارتباط برقرار کرده و به منظور پوشش دادن قسمت بیشتری از خانه، سیگنال‌های وای فای را پراکنده کنند. در این مقاله، به بررسی اجمالی چالش ها و راهکارهای ارائه شده برای تامین امنیت و حفظ حریم خصوصی کاربرانی که از شبکه هوشمند استفاده می‌کنند، پرداخته می‌شود و مقایسه‌ای بین امنیت در شبکه‌های مش وای فای معمولی و شبکه‌های مش که از VPN و VLAN برای امنیت بیشتر استفاده می‌کنند، انجام می‌شود.

کلمات کلیدی: شبکه خانگی هو شمند، شبکه مش وای فای، حریم خ صو صی و امنیت کاربران، اینترنت ا شیاء، آ سیب پذیری شبکه وای فای، بررسی عمیق بسته، پایش ترافیک

۱. مقدمه

با گسترش فناوری و افزایش کاربردها و فواید آن، سبک زندگی افراد تغییراتی داشته است. در این میان، اینترنت اشیا با توسعه حمل و نقل هوشمند، صنایع هوشمند، شهرها و خانه‌های هوشمند، گسترش یافته است. از این رو، چالش‌های امنیتی و حملات جدیدی در شبکه‌های موجود ایجاد می‌شوند. تا چند سال پیش، محیط شبکه خانگی فقط شامل دستگاه‌های محاسباتی شخصی (مثل لپ‌تاپ‌ها و تلفن‌ها) بود. امروزه حسگرهای جدید مختلفی در دستگاه‌ها تعبیه شده‌اند تا محیط خانه را به هم پیوسته‌تر و خودکارتر سازند. محیط خانه هوشمند را می‌توان به دسته‌های مختلفی تقسیم کرد که عبارتند از:

یک) دستگاه‌های سرگرمی خانگی: تلویزیون‌های هوشمند، کنسول‌های بازی، جعبه‌های راه‌اندازی وای فای، و کلاینت‌های کنترل شده با صدا (مثل الکسا و دستیار گوگل)

دو) وسایل روشنایی خانه: لامپ‌ها و چراغ‌های هوشمند

* **Corresponding author:**
Email: Maralsalehi@semnan.ac.ir

سه) لوازم خانگی: یخچال هوشمند، ماشین لباسشویی، فر و ترموستات‌ها
چهار) امنیت خانه: قفل‌های هوشمند، دوربین‌ها و سنسورهای امنیتی
پنج) دستگاه‌های محاسباتی شخصی: لپ تاپ، تلفن‌های هوشمند، ساعت و تبلت
شش) وسایل تناسب اندام: دوچرخه‌های هوشمند و سایر تجهیزات بدنسازی خانگی

محیط خانه هوشمند معمولی از سه جز اصلی تشکیل شده اند: دستگاه‌های اینترنت اشیا ، حسگرهای اینترنت اشیا* و حالت‌های ارتباطی [1] .

یک) دستگاه‌های اینترنت اشیا: دستگاه‌های خانه هوشمند طوری طراحی شده‌اند که سرویس گیرنده‌ها کم مصرف و دارای مدیریت مرکزی باشند. کم مصرف بودن دستگاه‌ها، کاهش قابلیت‌های CPU را به همراه دارد، که منجر به عدم استفاده از الگوریتم‌های رمزنگاری در ارسال داده‌ها و به میان آمدن امکان جاسوسی سایبری و در نهایت به خطر افتادن حریم خصوصی کاربر و دستگاه می‌شود.

دو) حسگرهای اینترنت اشیا: طراحی محصولات خانگی با ابعاد کوچک، تولید کنندگان را مجبور به حذف لوازم جانبی غیر ضروری (مانند صفحه کنترل usb و پورت‌های نمایش) میکند و موجب افزایش وابستگی به برنامه‌های تلفن هوشمند برای مدیریت دستگاه ها می‌شود. وابستگی به برنامه‌های کاربردی تلفن همراه، کاربران نهایی را مجبور می‌کند به شبکه‌های خانگی اجازه دسترسی پیشرفته بدهند.

سه) شیوه‌های ارتباطی: دستگاه‌های خانه هوشمند، برای اتصال به شبکه خانگی از پروتکل‌های مختلفی مانند وای فای و زیگبی و بلوتوث استفاده می‌کنند. هیچ پروتکل یکسان و استانداردی در سراسر صنعت مورد استفاده قرار نمی‌گیرد. بدین ترتیب چندین کاربر اینترنت اشیا در یک شبکه از پشته‌های پروتکل‌های مختلف استفاده می‌کنند و محیطی ناهمگن ایجاد می‌کنند.

امروزه با گسترش سریع شبکه‌های بیسیم و نیاز روز افزون به افزایش عملکرد و امنیت، استانداردهای IEEE802.11 تکامل یافته‌اند. در حال حاضر، وای فای ۶ آخرین استانداردی است که قادر به دستیابی به نرخ داده بیش از ۱۰ گیگابیت در ثانیه می‌باشد. همچنین امنیت شبکه‌های وای فای از زمان ظهور WEP به طور قابل توجهی تکامل یافته است WPA3† .به عنوان جانشین WPA2 ، محرمانگی را بهبود داده و آسیب پذیری‌های امنیتی ناشی از انتخاب ضعیف رمز عبور را کاهش داده است.

شبکه وای فای خانگی هوشمند، به دلیل نبود مکانیزم‌های امنیتی حفظ حریم خصوصی، می‌تواند در برابر بیش از ۱۲ هزار حمله، آسیب‌پذیر باشد و دستگاه‌های خانگی را در برابر هکرها آسیب‌پذیر نماید [2] . این مقاله سعی دارد به مشکلات حریم خصوصی و امنیتی خانه‌های هوشمند متصل به وای فای بپردازد. اکثر دستگاه‌های خانه هوشمند برای کار بر روی معماری TCP/IP طراحی شده‌اند، که برای اتصال به شبکه گسترده WAN و شبکه محلی LAN به یک دروازه یا گیت وی نیاز دارد، که در آن کاربران مختلف اینترنت اشیا متصل شده با یکدیگر ارتباط برقرار کنند. امروزه اکثر کاربران اینترنت اشیا، برای انجام کارهای خاص در خانه به یک اتصال اینترنتی فعال نیاز دارند اگر این کلاینت، تین باشد بدان معناست که منابع او محدود است، که در اینصورت از تنظیمات امنیتی توصیه شده پیروی نمیکند.

کلاینت‌های تین ، کل محیط شبکه‌ خانگی را در برابر هکرها آسیب‌پذیر کرده و امنیت و حریم خصوصی سایر دستگاه‌های بیسیم شبکه را به خطر می‌اندازند [3] . با پیشرفت فناوری‌هایی مانند بازرسی عمیق بسته(DPI§) ، ISPها قادر هستند بر ترافیک شبکه خانگی نظارت کنند زیرا بیشتر ترافیکی که توسط کاربر مرور می‌شود رمزگذاری نشده اند و ابر

* Internet of Things
† Wi-Fi Protected Access
‡ Thin Client
§ Deep Packet Inspection
* Internet Service provider

داده‌هایی (مانند برنامه‌های کاربردی مرور شده، وب سایت‌های مرور شده، تعداد بسته‌های مبادله شده و فعالیت دستگاه) را ارائه می‌دهند. تعبیه مکانیزم‌های حفظ حریم خصوصی و امنیت در طراحی مش وای فای، خانه‌های هوشمند را کمتر در معرض خطر استراق سمع در اینترنت قرار می‌دهد. در نهایت، تمرکز بر حفظ امنیت و حریم خصوصی شبکه خانگی مورد نظر میباشد. اولویت دادن به امنیت حریم خصوصی، مستلزم ایجاد تغییراتی بر روی روترهای مش وای فای خانگی میباشد، مانند پیاده سازی VPN*, SAE, WPAS و سرویس DNS رمزگذاری† شده، و شبکهVLAN‡ ها.

طبق [4]، در این زمینه سه سوال و سه نکته مطرح می‌شود .سوال اول: بهترین پیکربندی مش، در برابر تجزیه و تحلیل نظارت بر ترافیک که توسط ISP انجام میشود و حریم خصوصی را برای کاربر اینترنت اشیا فراهم می‌کند چیست؟ سوال دوم: بهترین پیکربندی مش، که در برابر استراق سم کنندگان در شبکه‌های مجاور، حریم خصوصی را برای کاربر اینترنت اشیا فراهم می‌کند چیست؟ سوال سوم: بهترین پیکربندی مش، که در مقایسه با شبکه خانگی سنتی، ناشناس بودن را در اینترنت فراهم می‌کند چیست؟ نکته یک) پیکربندی مش با VPN و VLAN در مقایسه با اجرای مش خروجی از نشت بسته‌های TCP/IPجلوگیری می‌کند .نکته دو) تقسیم بندی شبکه بک هال رمزگذاری شدهٔ§ با WPA3 ، از کاربران در برابر ارتباط متقابل سیستم مهاجم و حمله انکار سرویس در شبکه محلی بیسیم، محافظت می‌کند. نکته سه) رمزگذاری ترافیک LAN به WANبا استفاده ازVPN ، ناشناس بودن در اینترنت را برای شبکه خانگی هوشمند فراهم می‌کند.

هدف، مقایسه راهکارهای مختلف حفظ امنیت و حفظ حریم خصوصی و انتخاب بهترین تنظیمات امنیتی برای شبکه‌های مش امن خانگی میباشد. تحقیقات قبلی نشان داد، حتی ترافیک دستگاه‌های رمزگذاری شده نیز می‌تواند در معرض حملات تجزیه و تحلیل نظارت بر ترافیک قرار گیرند [5] . بنابراین* رمزگذاری بار * دستگاه برای محافظت از حریم خصوصی و امنیت شبکه کافی نیست و مستلزم استقرار چندین مکانیزم امنیتی می‌باشد .در این مقاله، چهار رویکرد پیاده سازی شبکه برای شبکه مش وای فای خانگی هوشمند، که می‌تواند توسط آی‌ISP ها، در بازار اینترنت موجود، استقرار یابد . این رویکرد شامل استفاده از چندین راهکار امنیت شبکه‌های دیگر، مانند VPN, PMF با WPA2 برای امنیت فرانت هال † و WPA3 برای امنیت بک هال و ایجاد سه VLAN به ترتیب برای کاربران کم مصرف اینترنت اشیا، کاربران محاسباتی پیشرفته، و کاربران مهمان، می‌باشد.

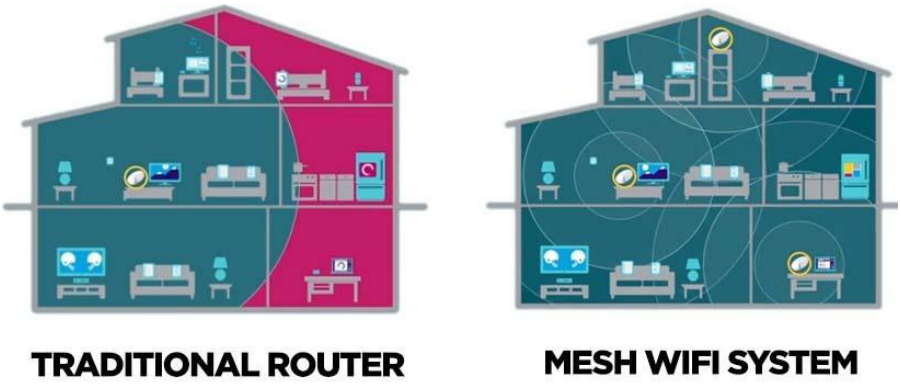
با بررسی پروتکل‌های رمزگذاری پیشرفته مانند WPA3 با کلمات عبور الفبایی عددی طولانی، برای اطمینان از مدیریت و ذخیره داده‌ها به صورت محلی در روتر مش، می‌توان با معایب آن مقابله نمود .ذخیره سازی داده‌ها به صورت محلی در دستگاه، با استفاده از رمزگذاری پیشرفته برای شبکه‌های محلی بی‌سیم، و رمزگذاری DNS در یک شبکه با چندین VLAN باعث بهبود وضعیت امنیت و حریم خصوصی شبکه می‌شود [6] . استفاده از VPN برای هر کاربر شبکه برای اهداف امنیتی توصیه می‌شود. با این حال، فعال کردن VPN در تین کلاینت ها، چالش برانگیز است، زیرا استفاده از VPN در هر دستگاه نیاز به منابع قوی دارد که تین کلاینت این ویژگی را ندارد [7] .

۲. بررسی راه کارها

یک سیستم گره مش، شبکه وای فای ما را گسترش می‌دهد و در سراسر خانه پوشش دهی دارد. در مقایسه با سایر دستگاه‌های شبکه، یک سیستم مش، برای افزایش محدوده وای فای، بهبود اتصال دستگاه، و حذف مناطقی از خانه که اتصال وای فای ندارند، طراحی شده است (شکل ۱). یک روتر وای فای استاندارد تقریباً ۱۵۰ فوت برد دارد، هنگام عبور سیگنال

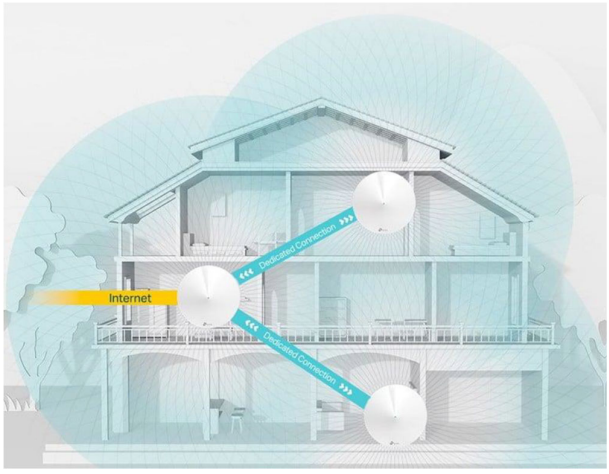
* Virtual Private Network
† Domain Name System
‡ Virtual Local Area Network
§ Backhaul
* Payload *
† Fronthaul †

وای فای از دیوارها کف و سایر موانع این پوشش کاهش می‌یابد. از طرف دیگر یک سیستم مش به شبکه وای فای اجازه می‌دهد تا ۵۰۰۰ فوت مربع یا بیشتر گسترش یابد [8] . حضور سایر شبکه‌های وای فای می‌توانند بر اتصال دستگاه تاثیر بگذارند و منجر به سرعت اتصال کندتر شوند. هر دیواره یا ماده‌ای در خط دید روتر و دستگاه باعث تخریب سیگنال وای فای می‌شود.



شکل ۱- پوشش دهی شبکه مش وای فای، در مقایسه با شبکه وای فای معمولی [8]

مفهوم سیستم‌های مش وای فای، برای افزایش پوشش دهی اتصال دستگاه معرفی شدند. در شکل ۲، یک توپولوژی مش وای فای نشان داده شده که شامل یک مسیریاب اصلی و دو دستگاه اضافی که به عنوان نقاط دسترسی (AP) یا توسعه دهنده شناخته می‌شوند، می‌باشد. این دستگاه‌ها با هم همکاری می‌کنند تا یک شبکه وای فای یکپارچه را تشکیل دهند که می‌تواند بسته به اندازه و شکل یک خانه، بسته به تعداد دیوارها سفارشی سازی شود .اتصال رادیویی بک هال اتصال بین روتر و نقاط دسترسی را فراهم می‌کند در حالی که شبکه فرانت هال دسترسی به اینترنت را برای دستگاه‌های وای فای فراهم می‌نماید.



شکل ۲- توپولوژی مش وای فای، در یک خانه مدرن بزرگ [9]

۱.۲. تهدیدات امنیتی برای شبکه‌های خانگی هوشمند

برخی از نگرانی‌های رایج مربوط به حریم خصوصی مرتبط با شبکه‌های وای فای عبارتند از
یک) شنود داده‌ها: سیگنال‌های وای فای از طریق هوا پخش می‌شوند و مستعد رهگیری توسط افراد غیر مجاز در آن محدوده هستند. مهاجمان می‌توانند ترافیک شبکه را ضبط و تجزیه و تحلیل کنند. ترافیک شبکه شامل اطلاعات حساس مانند اعتبار ورود، داده‌های شخصی یا فعالیت‌های مرور میباشد [10].
دو) حملات :MiTM* مهاجمان می‌توانند خود را بین دستگاه کاربر و شبکه وای فای قرار دهند و بسته‌های داده را رهگیری و دستکاری کنند. آنها اجازه می‌یابند تا اطلاعات حساس را ضبط کنند بدافزار با محتوای مخرب به سیستم وارد کنند یا کاربران را به وب سایت‌های جعلی هدایت کنند و داده‌های آنها را به سرقت برده یا به خطر بیندازند [11].
سه) دسترسی غیر مجاز :کلمات عبور ضعیف که به راحتی قابل حدس زدن هستند امکان دسترسی کاربر غیر مجاز را از طریق شبکه فراهم می‌آورد. کاربر غیر مجاز، پس از اتصال هر کاری انجام می‌دهد؛ ؛ استراق سمع از ترافیک شبکه، به خطر انداختن دستگاه‌ها و شرکت در فعالیت‌های مخرب [12].
چهار) ضبط و ردیابی شبکه: شبکه‌های وای فای می‌توانند اطلاعات مربوط به دستگاه‌های متصل را ردیابی و ضبط کنند، اطلاعاتی مانند آدرس‌های مک، شناسه‌های دستگاه، علاقمندی‌های کاربر و عادات مرور. این داده‌ها را می‌توان برای تبلیغات هدفمند، ضبط فعالیت یا برای فروش به اشخاص دیگر بدون رضایت کاربر، استفاده نمود [10].
پنج) شمارش شبکه: دستگاه‌هایی که به طور فعال شبکه‌های وای فای موجود را جستجو می‌کنند، می‌توانند ناخواسته نام شبکه‌های متصل قبلی را فاش کنند .(SSID†) این اطلاعات می‌توانند جزئیاتی را در مورد موقعیت مکانی کاربر، ترجیحات او، یا شبکه‌هایی که اغلب به آنها متصل می‌شوند فاش نمایند [7].
شش) شبکه‌های وای فای سرکش: مهاجمان می‌توانند شبکه‌های وای فای مخرب را با نام‌های موجه راه اندازی نمایند و به این ترتیب کاربر را فریب دهند تا به آن شبکه مخرب متصل شود. این شبکه‌های سرکش می‌توانند اطلاعات حساس کاربر را ضبط کنند، حملاتی را انجام دهند یا به عنوان دروازه ای برای سوء استفاده‌های بعدی عمل کنند [11].
هفت) آسیب پذیری‌های پروتکل امنیتی :WiFi پروتکل‌های امنیتی قبلی مانند WEP وWPA2 ، در طول زمان آسیب پذیری‌هایی را آشکار کرده‌اند و با رمزگشایی ترافیک رمزگذاری شده، منجر به دسترسی غیر مجاز میشوند [13].
هشت) بهره‌برداری از دستگاه وای فای: مهاجمان می‌توانند از آسیب پذیری‌های موجود در دستگاه‌هایی با قابلیت وای فای، مانند روترها، نقاط دسترسی و دستگاه‌های اینترنت اشیا، به منظور دسترسی غیر مجاز به دستگاه، به خطر انداختن دستگاه، یا استفاده از آن به عنوان نقطه محوری برای حمله به دستگاه‌های دیگر شبکه، سوءاستفاده نمایند [14].

۲.۲. راهکار یک) شبکه های مش وای فای: مسائل امنیتی و حریم خصوصی در شبکه مش موجود

اکثرISP ها به چهار دلیل داده‌ها را جمع آوری می‌کنند: اول) جمع آوری شاخص عملکرد کلید خدمات (مثلاً ویدئو، صدا یا اینترنت) به مشتری، دوم) تبلیغات، سوم) فروش سایر خدمات یا محصولات اینترنت اشیا، چهارم) ارائه خدمات بر اساس مناطق جغرافیایی.

۱.۲.۲. بازرسی عمیق بسته‌ها در اینترنت

بسته‌های داده‌ای که ترافیک اینترنت را تشکیل می‌دهند معمولاً دو بخش اصلی دارند؛ اطلاعات هدر و اطلاعات بار. اطلاعات بار شامل اطلاعات واقعی در حال تحویل از طریق اینترنت است، اطلاعات هدر شامل اطلاعات مسیریابی برای ارسال پیام‌ها به مقصدهای مورد نظرشان می‌باشد. موجودیتی با این قدرت عمل، می‌تواند اطلاعات را تغییر دهد (اطلاعاتی مانند آنچه

* Man in the Middle
Service Set Identifier

گفته شده زمان و شخص گوینده) این توانایی برای عمل یکپارچه بر روی اطلاعات هدر و بار در زمان واقعی، آنها را قادر می سازد کنترل فوق العاده‌ای بر ارتباطات داشته باشند. ارائه دهندگان خدمات اینترنت (ISP ها)، به تدریج فناوری شبکه‌ای را به کار می‌گیرند تا بتوانند بر داده‌های عظیم نظارت کنند. این روش را بازرسی عمیق بسته می‌نامند [15] . در مقایسه با قابلیت‌های شبکه قبلی، DPI درک کامل‌تری به اطلاعاتی که مشترکین اینترنت ارسال و دریافت می‌کنند ارائه می‌دهد.

۲.۲.۲. استفاده از DPI در روترهای اینترنت خانگی

امروزه اکثرISP ها و روترهای اینترنت خانگی، مجهز به سخت‌افزار DPI میباشند. با بازرسی عمیق بسته ها، ISPها میتوانند به طور دقیق مبدا و محتوای بسته را شناسایی کنند. با DPI امکان بازرسی بسته‌های داده از لایه شبکه (لایه ۳ مدلOSI) تا لایه کاربرد (لایه ۷) را فراهم می‌نماید،و ضمن حفظ یکپارچگی سایر خدمات، ترافیک HTTP و ترافیک‌های رمزگذاری نشده دیگر را به طور کامل بررسی می‌نماید [16] .

تجهیزات دی‌پی‌آی می‌توانند مسیر بسته را تغییر دهند، بسته را برچسب گذاری کنند، آنرا را حذف کنند، محدودیت نرخ تعیین کنند، یا بسته مورد نظر خود را به ISP ها گزارش دهند. تغییر مسیر ممکن است شامل ارسال بسته دارای ویژگی مشخص به یک مقصد خاص در شبکه باشد به عنوان مثال، تمام بسته‌های ایمیل را می‌توان به یک قطعه سخت‌افزاری خاص که قبل از ارسال ایمیل به گیرنده مشخص می‌کند هرزنامه است یا خیر، ارسال نمود. همچنین می‌توان برای دادن یک سطح کیفیت خدمات به بسته‌ها (QOS) ، مقدار تاخیر تجربه شده در سیستم تبادل بسته را علامت گذاری نمود [17] . بسته‌هایی که به سطوح بالای تاخیر حساس هستند، می‌توانند در هنگام هدایت به مقصد نسبت به بسته‌هایی که حساسیت کمتری نسبت به تاخیر دارند، اولویت بیشتری داشته باشند.

۳.۲.۲. سیستم نام دامنه (DNS) رمزگذاری نشده

اکثرISP ها و اپراتورهای چندگانه, خدمات DNS رمزگذاری نشده ارائه می‌دهند. به این ترتیب، سرورهای DNS به صورت پیش فرض برای روترهای اینترنتی خانگی (و بدون هیچ گزینه‌ای برای تغییر) در نظر گرفته می‌شوند. DNS از تمام فعالیت‌های اینترنتی پشتیبانی می‌کند و به عنوان جستجوی دایرکتوری در اینترنت عمل می‌کند و مرور خدمات آنلاین یا وب سایت‌ها را برای کاربران ساده‌تر می‌کند DNS به عنوان واسطی بین انسان و ماشین عمل می‌کند و به آنها امکان می‌دهد تا از فرمت‌های آدرس اینترنتی که برایشان مناسب‌تر هست استفاده کنند. بسیاری از برنامه‌های کاربردی خانه‌های هوشمند، شامل حسگرهای همیشه روشن هستند که اقدامات آفلاین کاربران را در محل زندگی آنها ثبت می‌کنند و اطلاعاتی در مورد این فعالیت‌ها، به خارج از خانه و به خدمات ابری که توسط تولید کنندگان دستگاه مدیریت می‌شود، ارسال می‌کنند. روتین‌های تمرین ورزشی و داده‌های پزشکی، نمونه‌ای از فعالیت‌های آفلاین ثبت شده توسط فناوری خانه‌های هوشمند هستند. حتی اگر یک دستگاه خانه هوشمند برای ضبط اقدامات حساس مربوط به حریم خصوصی در نظر گرفته نشده باشد، این عمل ممکن است همچنان داده‌های جمع‌آوری شده توسط حسگرهای دستگاه را به طور غیر مستقیم تحت تاثیر قرار دهد و ابزارهای استنتاج را قادر سازد تا آنها را شناسایی کنند. با وجود استفاده گسترده از رمزگذاری لایه حمل، ابر داده‌های دستگاه‌های خانه هوشمند نشت می‌کنند و به استراق سمع کننده اجازه می‌دهد تا ترافیک شبکه خانگی را نظارت یا جمع آوری نماید. نظارت بر ترافیک DNS رمزگذاری نشده یک روش رایج است که توسط استراق سمع کنندگان برای جمع آوری ابر داده از کلاینت‌های رمزگذاری شده و رمزگذاری نشده استفاده می‌شود.

۴.۲.۲. استفاده از WPA2 برای امنیت شبکه بک هال و فرانت هال

WPA2 پروتکلی امنیتی است که برای رمزگذاری و محافظت از ارتباطات شبکه وای فای استفاده می‌شود. این رمزگذاری برای ایمن سازی ارتباطات بی سیم و جلوگیری از دسترسی غیرقانونی به داده‌های شبکه مورد استفاده قرار میگیرد.

اکثر سیستم‌های مش موجود از شبکه بک هال مبتنی بر رمزگذاری WPA2 که روی منابع رادیویی مشترک با شبکه فرانتال میزبانی می‌شود استفاده می‌کنند. یکی از آسیب پذیری‌های کشف شده در رمزگذاری WPA2، آسیب پذیر بودن در برابر

حمله جداسازی میباشد. این حمله با هدف قطع اتصال گره یا کاربر تایید هویت شده از نقطه دسترسی یا روتر انجام می‌شود. وقتی دستگاه تلاش می‌کند دوباره متصل شود، بدافزارها به اطلاعات احراز هویت کاربر دست می‌یابند. پروتکل WPA2 در برابر حمله انکار سرویس DOS و حمله دیکشنری آسیب پذیر می‌باشد.

۵.۲.۲. خلاصه محدودیت‌های شبکه مش وای فای

یک) ISPها نظارت بر ترافیک را به روش "بررسی عمیق بسته" انجام می‌دهند. ISP با نظارت مداوم بر آدرس IP اختصاص داده شده به دستگاه‌ها، آدرس MAC مبدا و مقصد هر بسته، فعالیت دستگاه متصل به خود را زیر نظر دارد.

دو) همه دستگاه‌ها، بدون تقسیم بندی به یک شبکه خانگی متصل می‌شوند. جداسازی دستگاه‌های اینترنت اشیا، دستگاه‌های شخصی هوشمند مانند کامپیوترها و دستگاه‌های مهمان، انجام نمیشود. با نبود تقسیم بندی در شبکه فرانتال، یک نقطه دسترسی به عنوان gateway عمل می‌کند و بقیه دستگاه ها با مسیریابی بسته‌ها به سمت gateway، اتصال شبکه را گسترش می‌دهند. کامپیوترها، گوشی‌های هوشمند تین کلاینت‌های اینترنت اشیا، لوازم هوشمند و حسگرهای اینترنت اشیا، همگی بدون جداسازی در یک شبکه با یکدیگر ارتباط دارند.

سه) استفاده از رمزگذاری WPA2 برای اتصال شبکه بک هال

چهار) استفاده از DNS رمزگذاری نشده

پنج) عدم نصب VPN روی روتر ISP، و در نتیجه عدم رمزگذاری بسته‌های LAN به WAN. برنامه‌های VPN فقط روی رایانه‌ها و تلفن‌های هوشمند قابل نصب هستند اما برخی از سنسورهای اینترنت اشیا یا لوازم خانگی، سیستم عامل قدرتمندی برای نصب VPN ندارند یک تین کلاینت آسیب دیده می‌تواند کل شبکه مش را به خطر بیندازد. اکثر مشتریان اینترنت اشیا مانند تلویزیون‌ها و تلفن‌های هوشمند از VPN برای رمزگذاری ترافیک داخل شبکه WLAN استفاده نمی‌کنند. وقتی بسته‌ها رمزنگاری نمیشوند اطلاعات بسته ها از جمله، آی پی مقصد، آی پی مبدا و اطلاعات هدر، به ISP و اینترنت درز می‌کند [۵]

این محدودیت‌ها موجب می‌شوند شبکه مش فعلی، قادر به تامین امنیت و حریم خصوصی کاربران و دستگاه‌ها نباشد.

۲.۳. راهکار دو) شبکه های مش وای فای با VPN و VLAN

- در این راهکار، شبکه مش امن فرانتال با استفاده از VLAN به سه بخش مختلف تقسیم می‌شود که به جداسازی ترافیک دستگاه های LAN شخصی، اینترنت اشیا و مهمان کمک می‌کند.
- وقتی VPN که روی گیت وی نصب شده بود بسته‌ای را که از گیت وی به مودم ISP ارسال می‌شود, رمزگذاری کند در این صورت مکان همه ی دستگاه های متصل به مش امن، از استراق سمع کننده‌ای که موقعیت جغرافیایی دستگاه‌ها را جمع آوری می‌کند پنهان می‌ماند.
- همچنین DNS پیش فرض گیت وی، به یک DNS رمزگذاری شده که میزبان آن است, تغییر می‌کند تا مبدا، نوع و مکان ترافیک پوشانده شوند و این ویژگی‌های امنیتی کلیدی، از دسترس ISPها و روترها خارج شوند.
- این شبکه در مقایسه با سایر شبکه‌های مش، بهتر عمل می‌کند و احتمال نشت اطلاعات شبکه، برای استراق سمع کنندگان در مجاورت شبکه، کمتر است.

۳. خلاصه و نتیجه گیری

این تحقیق بر حفظ حریم خصوصی و امنیت شبکه وای فای خانه هوشمند تمرکز دارد. مفهوم استفاده از VPN و VLANبرای ایمن سازی شبکه، برای طراحان شبکه موضوع جدیدی نیست، بلکه رایج‌ترین رویکردی است که برای طراحی

WLANسازمانی استفاده می‌شود. اما وقتی صحبت از محصولات اینترنت خانگی می‌شود، تنظیمات VPN و VLAN در سطح روتر و نقطه دسترسی، توسط هیچ ISP پیاده‌سازی نمی‌شود [4] .

سوال اول) بهترین پیکربندی مش، در برابر تحلیل نظارت بر ترافیک انجام شده توسطISP ، که حریم خصوصی را برای مشتریان اینترنت اشیا فراهم آورد چیست؟ امروزهISP ها دارای قابلیت‌های پیشرفته‌ای برای نظارت بر ترافیک خانه می‌باشند. استفاده از VPN و VLAN در طراحی شبکه مش، حریم خصوصی دستگاه‌های اینترنت اشیاء را در برابر پایش ISP حفظ می‌کند.

نکته یک) در مقایسه با مش موجود، پیکربندی مش با VPN و VLAN از نشت اطلاعات بسته‌های TCP/IP جلوگیری می‌کند. نتایج آزمون مقایسه‌ای شبکه مش با پیکربندی VPN و VLAN نشان داد اطلاعات هیچ بسته داده به مسیریاب ISP نشت نکرده است، در حالیکه در تمام مش‌های دیگر پرس وجوهای DNS رمزگذاری شده و رمزگذاری نشده، بسته‌های HTTP، بار ICMP و پرس وجوهای ARP نشت داشتند. پیاده‌سازی بخش‌بندی شبکه را که در آن سه VLAN در شبکه فرانت هال و بک هال دنبال کردیم: شبکه‌های شخصی، اینترنت اشیا، و مهمان. شبکه بک هال با سه VLAN با استفاده از دو نقطه دسترسی گسترش یافت. از رمزگذاریWPA3 برای رمزگذاری شبکه بک هال به منظور محافظت از آن در برابر حملات DOS و دیکشنری استفاده شد.

سوال دو) بهترین پیکربندی مش که حریم خصوصی را برای کاربران متصل به اینترنت اشیا، در برابر استراق سمع شبکه مجاور، فراهم می‌کند چیست؟ برای انجام یک حمله احراز هویت، استراق سمع کنندگان باید در مجاورت شبکه باشند که در آن بسته‌های داده می‌توانند در طول یک حمله مداوم ضبط شوند. تقسیم بندی شبکه، دستگاه‌های اینترنت اشیا را از دستگاه‌های محاسبات شخصی جدا می‌کند. بک هال رمزگذاری شده باWPA3 ، امنیت را در برابر حملات DOS و دیکشنری فراهم میکند.

نکته دو) تقسیم بندی شبکه بک هال رمزگذاری شده باWPA3 ، از کاربران در برابر ارتباط متقابل سیستم مهاجم و حمله انکار سرویس (DOS) در شبکه محلی بیسیم محافظت می‌کند. تقسیم بندی شبکه با قوانین فایروال متفاوت برای هر بخش، در برابر تهدیدات داخلی امنیت بهتری را فراهم می‌کند و استفاده از WPA3 محافظت بهتری در برابر DOS و دیکشنری استراق سمع کنندگان ارائه می‌دهد .شبکه در دسترس و بسیار سریع مش وای فای، برای رفع نیازهای دستگاه‌های جدید اینترنت اشیا، مانند عینک‌های واقعیت افزوده (AR*) و واقعیت مجازی(VR†) ، سنسورهای خانه هوشمند و لوازم خانگی هوشمند مورد توجه میباشد.

سوال سه) بهترین پیکربندی مش، برای حفظ ناشناس بودن در اینترنت، در مقایسه با یک شبکه خانگی سنتی چیست؟ هر کاربر خانگی هوشمند با اتصال به اینترنت موجب درز فراداده در اینترنت می‌شود و برای استراق سمع در اینترنت مستعد می‌گردد. حتی از داده رمزگذاری شده اطلاعات حیاتی مانند اطلاعات جغرافیایی، ارائه دهندهISP ، منطقهISP ، آدرس IP دستگاه و اطلاعات DNS درز می‌کند. این اطلاعات جمع آوری شده برای تعیین نوع دستگاه، زمان فعالیت، مکان دستگاه یا کاربر کافی هستند.

نکته ۳) رمزگذاری ترافیک LAN به WAN با استفاده از VPN ، ناشناس بودن در اینترنت را برای شبکه خانگی هوشمند فراهم می‌کند .مش امن با VPN و VLAN در مقایسه با سایر سیستم‌های مش، عملکرد بهتری دارند. با این پیکربندی نشت اطلاعات سرویس گیرنده وای فای در اینترنت کمتر از یک درصد است در حالی که در سیستم‌های مش موجود تا ۸۰ درصد اطلاعات دستگاه در اینترنت نشت می‌کند .یک شبکه وای فای باید اتصال LAN و WAN به همه دستگاه‌های اینترنت اشیا، شخصی و مهمان را فراهم کند و این یکی از محدودیت‌های اصلی طراحی می‌باشد. به علاوه شبکه بک هال رمزگذاری شده با WPA2 مستعد حملات DOS است. اگر یک سیستم مش فاقد مدیریت شناسایی دسترسی مبتنی بر ابر باشد آنگاه این

* Augmented Reality
† Virtual Reality

شبکه با حمله یک مهاجم همزاد به خطر می‌افتد. استفاده از شبکه بک هال با WPA3 باعث بهبود امنیت شبکه در برابر حمله فرهنگ لغت آفلاین و حملات DOS خواهد شد.

۴. نتیجه گیری

همانطور که گفته شد، روتر ISP می‌تواند فراداده را از دستگاه‌های متصل در شبکه وای فای جمع آوری نماید و حریم خصوصی دستگاه‌ها را زیر سوال برد. فراداده‌های لو رفته از دستگاه‌های شخصی و اینترنت اشیا، مکان کاربر، نوع دستگاه یا فعالیت فعلی کاربر را فاش می‌کنند و ابرداده‌های رمزگذاری شده و رمزگذاری نشده توسط مهاجمین و ISP ها پایش و کنترل شدند. بنابراین سیستم‌های مش وای فای، برای محافظت از حریم خصوصی دستگاه‌های خانه هوشمند در اینترنت، باید مکانیزم‌های حفظ حریم خصوصی را در طراحی خود تعبیه نمایند.

شبکه وای فای مش امن با VPN وVLAN ، از حریم خصوصی دستگاه‌های متصل در برابرISP ها و ردیاب‌های اینترنتی، محافظت می‌کند. به علاوه، می‌توان نتیجه گرفت که مش وای فای امن با VPN و VLAN نسبت به سایر پیاده‌سازی‌های شبکه مش از امنیت بیشتری برخوردار است. وای فای مش امن، شبکه‌های شخصی را از اینترنت اشیا و شبکه‌های مهمان جدا می‌کند. این تقسیم بندی شبکه به همراه سایر ویژگی‌های امنیتی به کار رفته، شبکه وای فای خانگی را در برابر حملات امنیتی داخلی و خارجی مصون می‌دارد.

مراجع

[1] Z. Trabelsi, “IoT based Smart Home Security Education using a Hands-on Approach” *IEEE Global Engineering Education Conference.* Vienna, Austria, doi:10.1109/EDUCON46332.2021.9454085, 2021
[2] A. Laughlin, “How a smart home could be at risk from hackers. Retrieved from Which?: https://www.which.co.uk/news/article/how-the-smart-home-couldbe-at-risk-from-hackers-akeR18s9eBHU, 2021
[3] P. Cisar, S.M. Cisar, “General vulnerability aspects of Internet of Things”, 6th IEEE International Symposium on Computational Intelligence and Informatics. 2015, 117-121
[4] A.S. Bhagat, “A Secure Wi-Fi Mesh Network for Smart Homes”, *PhD. Thesis, The School of Engineering and Applied Science of the George Washington University*, 2024
[5] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, N. Feamster, “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic” *arXiv*., Retrieved from https://doi.org/10.48550/arXiv.1708.05044, 2017
[6] D. Anders, “10 Wi-Fi Network Security Tips You’ll Be Grateful for This Thanksgiving”, Retrieved from CNET: https://www.cnet.com/home/internet/how-to-secure-your-home-network-in-ten-simple-steps/, 2023
[7] N. Apthorpe, D. Reisman, N. Feamster, “Closing the Blinds: Four Strategies for Protecting Smart Home Privacy from Network Observers” *Cryptography and Security (cs.CR)*. *arXiv*. Retrieved from https://doi.org/10.48550/arXiv.1705.06809, 2017.
[8] Gateway Fiber, “Mesh vs. Wi-Fi Extender: What's the Difference?”, Retrieved from https://www.gatewayfiber.com/blog/mesh-vs-wi-fiextender-whats-the-difference, 2024
[9] TP-Link. (n.d.), “Smart Home Mesh WiFi System”, Retrieved from TP-Link Mesh Systems: https://www.tp-link.com/us/deco-mesh-wifi/product-family/deco-m9-plus/
[10] I. Hafeez, M. Antikainen, S. Tarkoma, “Protecting IoT environments against Traffic Analysis Attacks with Traffic Morphing”, *2019 IEEE Int. Conf. on Pervasive Computing and Communications Workshops,* doi:10.1109/PERCOMW.2019.8730787, 2019
[11] K. Murugesan, K.K. Thangadorai, V.N. Muralidhara, “PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks” *8th International Conference on Future Internet of Things and Cloud,* doi:10.1109/FiCloud49777.2021.00021, 2021
[12] S. Glass , M. Portmann,V. Muthukkumarasamy, “Securing wireless mesh networks”, *IEEE* Internet Computing”, 10.1109/MIC.2008.85, 30-36, 2008

[13] T.H. Kohlios, “A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3” *Electronics*. Retrieved from https://doi.org/10.3390/electronics7110284, 2018
[14] C. Lee, L. Zappaterra, K. Choi, H.A. Choi, “Securing smart home: Technologies, security challenges, and security requirements”, *IEEE Conference on Communications and Network Security.* San Francisco, CA: IEEE. doi:10.1109/CNS.2014.6997467, 2014
[15] C. Parsons, “Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials”, Surveillance Studies Centre, 2009
[16] A. Cooper, “Doing the DPI dance. Assessing the privacy impact of deep packet inspection”, In W. Aspray, & P. Doty, *Privacy in America* (pp. 139-165). Scarecrow Press, 2011
[17] A. Rafael, S. Fernandes, C. Kamienski, D. Sadok, J. Kelner, I. Godor, T. Westholm, “Deep packet inspection tools and techniques in commodity platforms: Challenges and trends”, *Journal of Network and Computer Applications*, 1863-1878. Retrieved from https://doi.org/10.1016/j. jnca.2012.07.010, 2012

کاربرد شبکه‌های عصبی پرسپترون چندلایه در پیش‌بینی پایداری ازدواج: تحلیلی بر داده‌های اجتماعی و روان‌شناختی

طوبی ترابی پور[۱]، رضا عزیزی[*۲].

۱- طوبی ترابی پور ، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد یزد، یزد، ایران

۲- رضا عزیزی ، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد میبد، میبد، ایران

چکیده

طلاق از معضلات اجتماعی با آثار مخرب معنوی و مادی است که آمارهای موجود نشان‌دهنده عدم اثربخشی کامل راهکارهای سنتی برای پیشگیری و کاهش آن است. این پژوهش، روشی مبتنی بر داده‌کاوی و یادگیری عمیق ارائه می‌دهد که با تحلیل اطلاعات ۳۳,۰۰۰ زوج ایرانی ثبت‌شده در سال‌های ۱۳۹۶ و ۱۳۹۷، مدلی برای پیش‌بینی موفقیت ازدواج توسعه داده است. مدل استفاده‌شده، شبکه عصبی پرسپترون چندلایه (MLP) بوده که پس از آموزش، به دقت ۹۵.۲ درصد دست یافته است. این دقت در مقایسه با مدل درخت تصمیم (۸۷ درصد) بهبود قابل‌توجهی را نشان می‌دهد. یافته‌های پژوهش نشان‌دهنده توانایی یادگیری عمیق در تحلیل الگوهای پیچیده رفتاری و ارائه ابزارهای کاربردی برای مشاوران خانواده جهت کاهش نرخ طلاق است.

کلمات کلیدی: تشخیص،طلاق،داده‌کاوی،شبکه عصبی

۱. مقدمه

پیش‌بینی آینده همواره یکی از اهداف اساسی مدیران در فرآیندهای تصمیم‌گیری و برنامه‌ریزی به‌شمار می‌رود. برای دستیابی به این هدف، استفاده از روش‌های نوین مبتنی بر داده‌کاوی و تحلیل رفتار می‌تواند بسیار مؤثر واقع شود. در سال‌های اخیر، داده‌کاوی به‌عنوان ابزاری توانمند برای تحلیل داده‌های گذشته و ارائه پیش‌بینی‌های دقیق از آینده مورد توجه ویژه قرار گرفته است. این روش نه تنها در تصمیم‌گیری‌های مدیریتی بلکه در حوزه‌های مختلف علمی و صنعتی نیز کاربرد یافته و نقش چشم‌گیری در حل مسائل و چالش‌های پیچیده ایفا کرده است.[1]

داده‌کاوی به‌عنوان رویکردی که امکان استخراج الگوهای معنادار از داده‌های حجیم را فراهم می‌کند، توانسته است ابزارهایی قابل اعتماد برای پیش‌بینی و بهبود فرآیندهای تصمیم‌گیری ارائه دهد. این فناوری به دلیل قدرت تحلیل عمیق و سرعت در پردازش داده‌ها، مورد استقبال گسترده‌ای قرار گرفته است و در مسیر رفع مشکلات پیچیده و ارائه بینش‌های ارزشمند، تحولی اساسی ایجاد کرده است .[2]

طلاق یکی از مسائل پیچیده و حساس اجتماعی است که نه تنها بر زندگی شخصی افراد بلکه بر سلامت اجتماعی و روانی جامعه نیز تأثیرگذار است. در سال‌های اخیر، روش‌های مختلفی برای پیش‌بینی و پیشگیری از طلاق مورد استفاده قرار گرفته

[*] **Corresponding author: رضا عزیزی**
Email: azizi.reza@maybodiau.ac.ir

است. یکی از رویکردهای نوین در این زمینه، استفاده از داده‌کاوی و یادگیری عمیق برای تحلیل داده‌های گذشته و پیش‌بینی نتایج آینده است. این روش‌ها قادرند الگوهای پنهان در رفتارهای زوجین را شناسایی کرده و به مشاوران خانواده کمک کنند تا توصیه‌های دقیق‌تری برای بهبود روابط و جلوگیری از طلاق ارائه دهند. با استفاده از این تکنیک‌ها، امکان پیش‌بینی موفقیت یا شکست یک ازدواج با دقت بالاتری فراهم می‌شود.[3]

در حالی که بسیاری از مشاوران خانواده از آزمون‌های روانشناسی برای ارزیابی زوجین استفاده می‌کنند، این ابزارها به‌تنهایی نمی‌توانند به پیش‌بینی دقیق‌تری برای موفقیت یا شکست ازدواج‌ها کمک کنند. دلیل اصلی این مشکل، عدم تطابق این آزمون‌ها با ویژگی‌های فرهنگی، اجتماعی و مذهبی جوامع مختلف است. بنابراین، نیاز به روشی بومی‌شده و دقیق‌تر که بتواند تمامی ابعاد زندگی زوجین را بررسی کند، احساس می‌شود. داده‌کاوی می‌تواند به‌عنوان ابزاری مؤثر در کنار آزمون‌های روانشناسی به کار رود و با استفاده از داده‌های بومی‌شده، الگوهای خاص جوامع مختلف را شناسایی کند.[3]

در این راستا، شبکه‌های عصبی پرسپترون چندلایه (MLP) به‌عنوان یکی از ابزارهای قدرتمند یادگیری عمیق در تحلیل داده‌ها، قابلیت بالایی در پیش‌بینی نتایج ازدواج‌ها دارند. این شبکه‌ها قادرند الگوهای پیچیده و غیرخطی موجود در داده‌های ازدواج‌های گذشته را شبیه‌سازی کرده و از آن‌ها برای پیش‌بینی موفقیت یا شکست یک ازدواج در آینده استفاده کنند. در این تحقیق، داده‌های مربوط به ۳۳،۰۰۰ زوج ایرانی ثبت‌شده در اداره ثبت‌احوال کشور در سال‌های ۱۳۹۶ و ۱۳۹۷ بررسی شده و از طریق تحلیل این داده‌ها، پیش‌بینی‌های دقیق‌تری در مورد نتایج ازدواج‌های جدید ارائه شده است.

در نهایت، هدف اصلی این پژوهش ایجاد یک سیستم توصیه‌گر مبتنی بر داده‌کاوی است که به مشاوران خانواده کمک کند تا علاوه بر استفاده از آزمون‌های روانشناسی، از پیش‌بینی‌های دقیق‌تری برای ارزیابی ازدواج‌ها بهره‌مند شوند. این سیستم قادر است با استفاده از داده‌های بومی و به‌روزرسانی‌های مداوم، پیش‌بینی‌های دقیق‌تری برای موفقیت یا شکست ازدواج‌ها ارائه دهد. با این کار، می‌توان به زوجین کمک کرد تا قبل از تصمیم‌گیری‌های مهم، اطلاعات لازم را برای داشتن زندگی مشترک پایدارتر دریافت کنند.

علاوه بر این، استفاده از سیستم‌های توزیع‌شده می‌تواند به بهبود عملکرد این سیستم توصیه‌گر کمک کند. در این سیستم‌ها، داده‌ها و پردازش‌ها به‌صورت موازی و توزیع‌شده در چندین گره پردازشی انجام می‌شود که به‌ویژه در مواجهه با داده‌های حجیم و پیچیده از جمله داده‌های ثبت‌احوال، می‌تواند به افزایش سرعت پردازش و دقت پیش‌بینی‌ها کمک شایانی کند. این سیستم‌های توزیع‌شده با امکان به‌کارگیری منابع پردازشی متعدد، قادرند زمان پردازش را کاهش داده و پیش‌بینی‌ها را به‌طور مؤثرتری به مشاوران ارائه دهند. در پژوهش حاضر، پیاده‌سازی چنین سیستمی می‌تواند به ارتقاء قابلیت‌های مدل و بهبود نتایج تحلیل‌های انجام‌شده کمک کند.[4]

بخش‌های مختلف پژوهش حاضر در بخش کارهای مرتبط، بخش ۳ جمع‌آوری داده‌ها، بخش ۴ روش پیشنهادی، بخش ۵ ارزیابی نتایج و درنهایت نتیجه‌گیری نیز ارائه‌شده است.

۲. کارهای مرتبط

در سال‌های اخیر، مقالات متعددی در زمینه پیش‌بینی و تشخیص نتیجه ازدواج با استفاده از روش‌های داده‌کاوی منتشر شده است که هرکدام به بررسی روش‌های مختلف یادگیری ماشین و تحلیل داده‌ها پرداخته‌اند. به‌عنوان مثال، ناصر و همکاران با استفاده از یادگیری عمیق برای پیش‌بینی احتمال طلاق، مدل ریاضی پیشنهادی خود را بر اساس ساختار بیولوژیکی موجودات زنده طراحی کردند که توانسته است با دقت ۱۰۰٪ پیش‌بینی‌های دقیقی را ارائه دهد [۵]. همچنین، رنجیتا و همکاران با حذف ویژگی‌های غیرضروری در داده‌ها، به دقت ۰.۹۸ در پیش‌بینی طلاق با استفاده از الگوریتم‌های یادگیری ماشینی بهبود یافته دست یافتند که می‌تواند ابزاری مفید برای مشاوران خانواده باشد.[6]

کنگ و همکاران به تشخیص طلاق با استفاده از الگوریتم‌های شبکه‌های عصبی چندلایه و درخت تصمیم پرداخته‌اند و در تحقیق خود دقت بالایی در پیش‌بینی نتایج طلاق به‌دست آورده‌اند [۷]. حفیدز و همکاران در ترکیه با استفاده از مدل‌های پیش‌بینی به دقت ۰.۹۸ و مقدار تشخیص ۰.۹۷ دست یافته‌اند و روش پیشنهادی آن‌ها در مقایسه با مدل‌های دیگر همچون SVMعملکرد بهتری داشته است [۸]. همچنین، شارما و همکاران روش‌های ترکیبی برای پیش‌بینی طلاق با استفاده از مدل‌هایی مانند جنگل‌های تصادفی، درخت تصمیم و ماشین‌های بردار پشتیبان پیشنهاد دادند که به دقت ۹۸٪ دست یافتند [9].

انگگری و همکاران روشی را برای پیش‌بینی طلاق با الگوریتم پیشینی و روش K-Means پیشنهاد کردند. اگر تعداد جستجوهای) PORN پورن(، SEX، GAY، و LESBIAN همه یه عنوان خوشه باشد، تعداد جلسات طلاق در رسانه خوشه ای است.[10]

فلورس و همکاران نیز در تحقیق خود چهار مدل یادگیری عمیق شامل پرسپترون، رگرسیون لجستیک، شبکه‌های عصبی و جنگل تصادفی را برای پیش‌بینی طلاق استفاده کردند و توانستند با ارزیابی ۳۵ سناریو مختلف، دقت، حساسیت و ویژگی‌های ۰.۹۸، ۱.۰ و ۰.۹۶ را به‌دست آورند [۱۱]. همچنین، فرید و همکاران از الگوریتم‌های SVM و MLP برای تشخیص طلاق استفاده کرده و توانسته‌اند به دقت ۹۷ درصد برسند و شاخص‌های کلیدی طلاق را شناسایی کنند [۱۲]. در ادامه، نارندران و همکاران با استفاده از مجموعه‌ای از داده‌ها در مورد وضعیت قبل از ازدواج زوج‌ها و الگوریتم‌های طبقه‌بندی چندگانه، به تحلیل امکان پیش‌بینی طلاق پرداخته‌اند و از الگوریتم‌های جنگل تصادفی، درخت تصمیم و XGBoost برای تحلیل این داده‌ها بهره جسته‌اند.[13]

با این وجود، هیچ‌یک از این پژوهش‌ها از داده‌های واقعی و مرتبط با کشور ایران استفاده نکرده‌اند. در این تحقیق، داده‌های استخراج‌شده از ثبت‌احوال ایران در سال‌های ۱۳۹۶ و ۱۳۹۷ مورد بررسی قرار گرفته‌اند و مدل‌های مختلف داده‌کاوی برای پیش‌بینی طلاق به‌کار گرفته شده است. پژوهش حاضر با استفاده از یک روش ترکیبی و ایجاد یک سیستم وب‌اپلیکیشن، قصد دارد به مشاوران خانواده کمک کند تا در کنار آزمون‌های روانشناسی، پیش‌بینی‌های دقیق‌تری درباره موفقیت یا شکست ازدواج‌ها داشته باشند و توصیه‌های مؤثرتری به زوجین ارائه دهند.

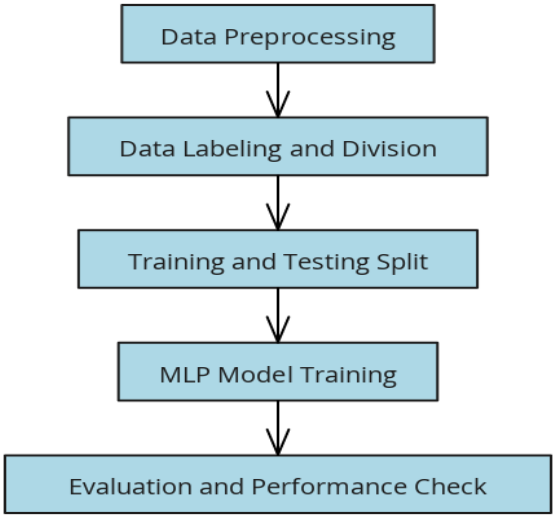
۳. جمع‌آوری داده‌ها

در این پژوهش، داده‌های مورد استفاده از اداره ثبت‌احوال ایران استخراج شده است و شامل اطلاعات مربوط به ۳۳ هزار مورد ازدواج و طلاق ثبت‌شده طی سال‌های ۱۳۹۶ و ۱۳۹۷ می‌باشد. این مجموعه داده شامل متغیرهای مختلفی مانند سطح تحصیلات، سطح درآمد، تعداد ازدواج، تعداد طلاق، سن زوجین و سایر ویژگی‌های مرتبط است. با این حال، داده‌ها در برخی موارد دچار نقص‌هایی بوده‌اند که ممکن بود بر روند یادگیری مدل تأثیر منفی بگذارد. به‌منظور رفع این نواقص، داده‌های نامناسب حذف یا با استفاده از روش‌های آماری، مقادیر جایگزین مناسب تخصیص داده شد تا از ایجاد ناپایداری در شبکه عصبی جلوگیری شود.

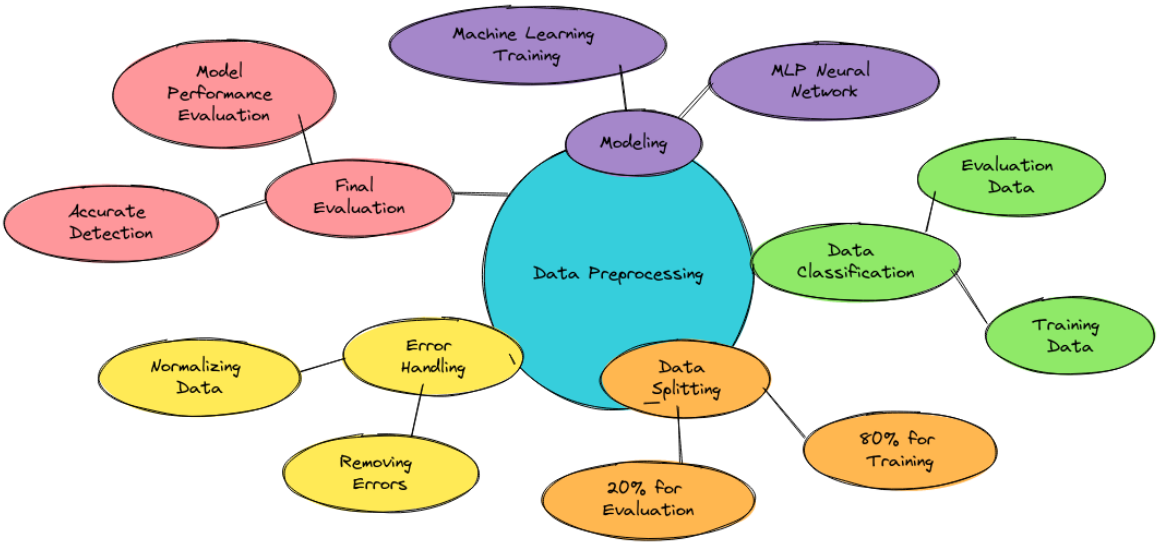
در این مجموعه داده، وضعیت افراد از جنبه‌های مختلف ازجمله سن، سطح تحصیلات، سطح درآمد، شغل، تعداد ازدواج‌ها، و ماه تولد بررسی و تحلیل شده است. پردازش این داده‌ها پیش از استفاده در مدل یادگیری عمیق، نقش مهمی در کیفیت نتایج داشته است و تلاش شده تا با اعمال روش‌های استاندارد پیش‌پردازش، دقت و پایداری مدل بهبود یابد. این داده‌ها اساس تحلیل‌ها و پیش‌بینی‌های انجام‌شده در این پژوهش را تشکیل داده و به‌عنوان یک مجموعه بومی از داده‌ها، شرایط خاص جامعه ایران را در نظر گرفته است.

۴. روش پیشنهادی

در بلوک دیاگرام و نقشه راه زیر به معرفی روش پیشنهادی انجام شده در این مقاله اشاره شده است:



شکل ۱ –بلوک دیاگرام تحقیق



شکل ۲ – نقشه راه تحقیق

در ادامه به توضیح قسمت‌های مختلف بلوک دیاگرام می‌پردازیم.

۱- Data preprocessing

در ابتدا داده‌ها جهت آماده‌سازی برای یادگیری سیستم، تحت فرآیند پیش‌پردازش قرار گرفتند و تغییرات لازم روی داده‌ها اعمال شد:

۱-۱.تبدیل داده‌های کیفی به عدد: داده‌های کیفی به مقادیر عددی تبدیل شدند تا قابل استفاده برای سیستم یادگیری باشند. به عنوان مثال:

سطح درآمد بر اساس شغل افراد به مقادیر عددی تبدیل شد.سطح تحصیلات مطابق با جدول ۱ به مقادیر کمی تبدیل گردید.

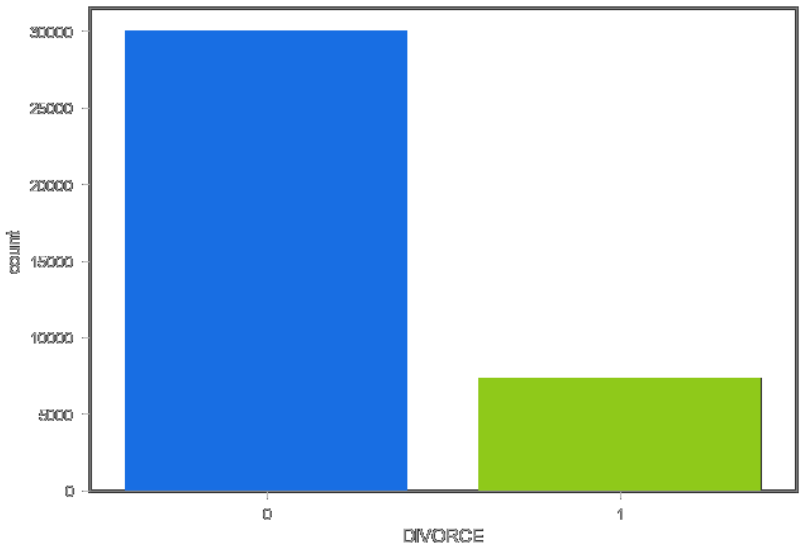
جدول ۱- سطح‌بندی سطح تحصیلات

دکتری	کارشناسی ارشد	کارشناسی	کاردانی	دیپلم
5	4	3	2	1

۱-۲ .سطح‌بندی داده‌ها: سطح درآمد افراد با توجه به نوع شغل، سطح شغلی و سایر پارامترها دسته‌بندی شد:

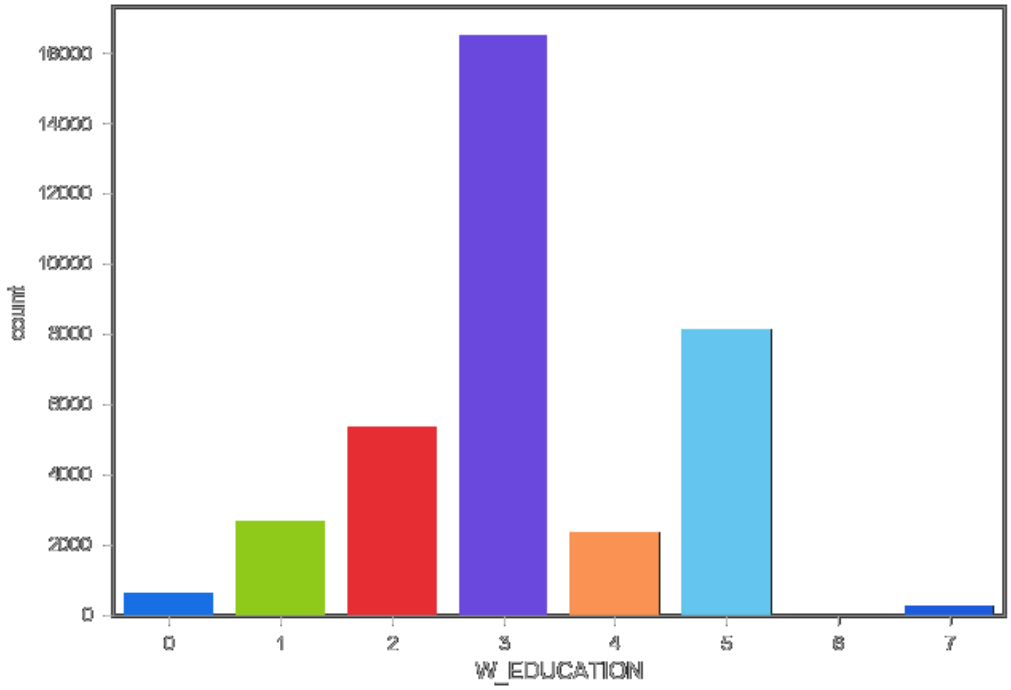
در راستای سطح‌بندی داده‌ها ،آنالیز اکتشافی داده ها Eda به ترتیب زیر انجام می شود:

۱- گزارش میزان ازدواج‌های منجر به طلاق و ازدواج‌های پایدار که در شکل ۳ مشاهده می شود:



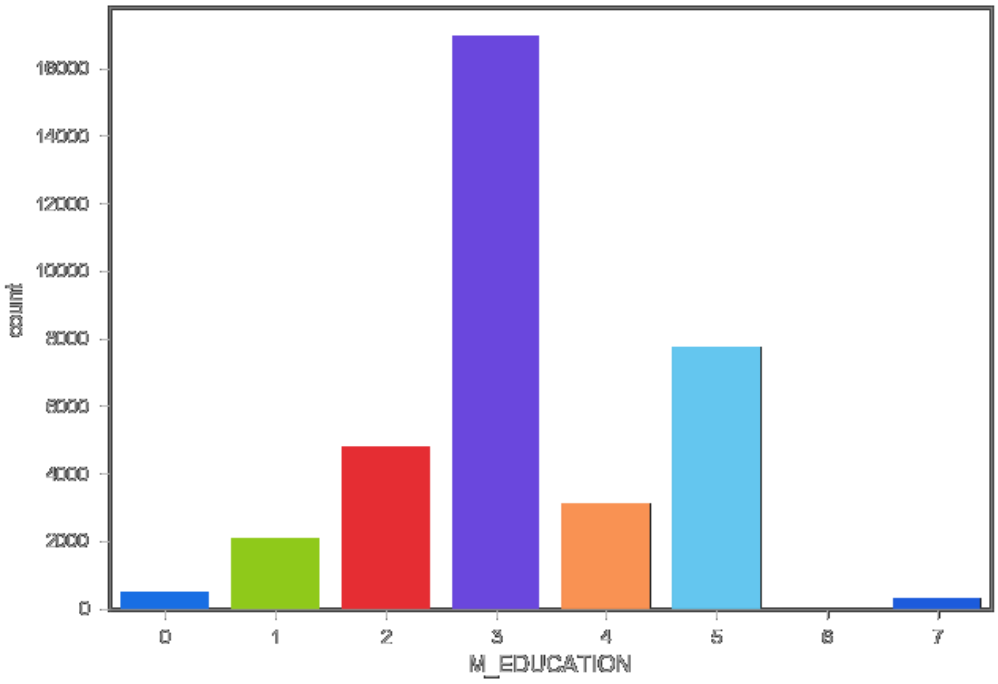
شکل ۳- گزارش نموداری وضعیت تعداد طلاق در دیتاست

۲- گزارش سطح تحصیلات خانم‌ها که در شکل ۴ مشاهده می شود:



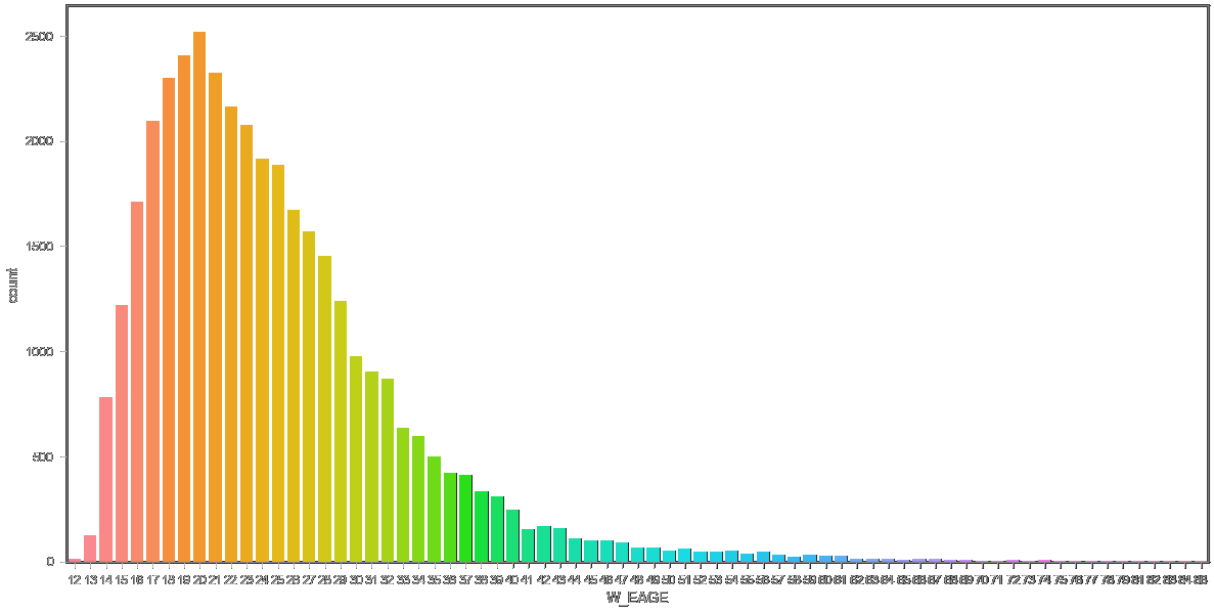
شکل۴-گزارش نمودار سطح تحصیلات خانم‌ها

۳- گزارش سطح تحصیلات آقایان که در شکل ۵ مشاهده می شود:



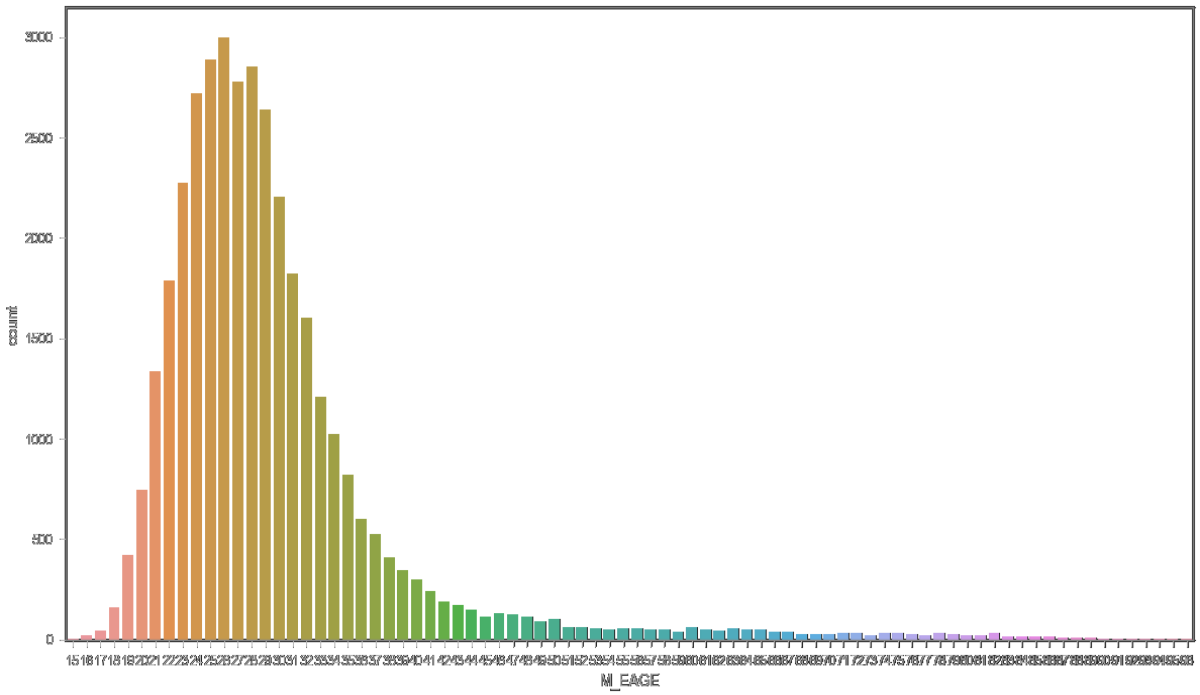
شکل ۵-گزارش نموداری سطح تحصیلات آقایان

۴- گزارش میزان سن خانم‌ها که در شکل ۶ مشاهده می شود:



شکل ۶-گزارش نموداری سن خانم‌ها

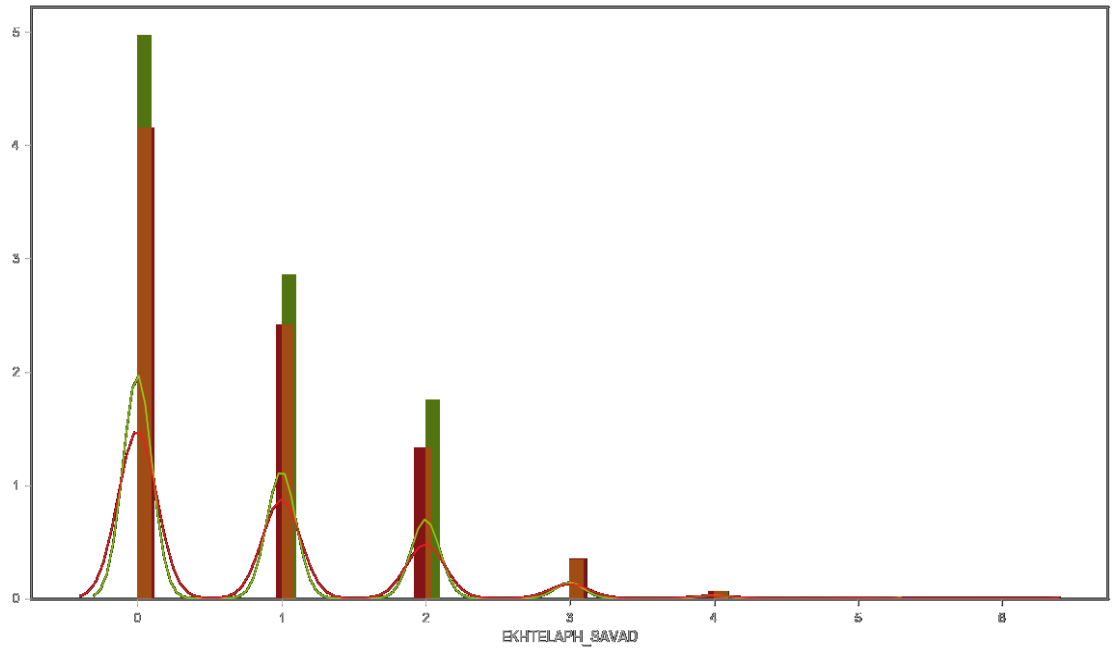
۵- گزارش میزان سن خانم‌ها که در شکل ۷ مشاهده می شود:



شکل ۷-گزارش نموداری سن آقایان

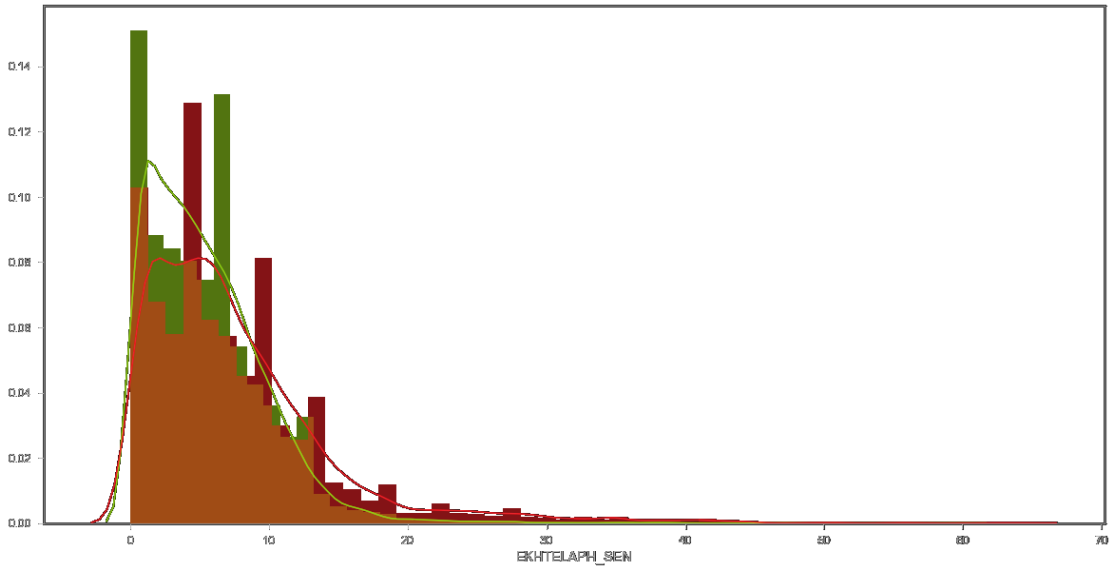
۶- گزارش تأثیر اختلاف سواد در اتفاق افتادن طلاق که در شکل ۸ مشاهده می شود:

همان‌طور که مشاهده می‌کنید بیشترین طلاق مربوط به تحصیلات مقطع سیکل هست:



شکل ۸-گزارش نموداری تأثیر سطح تحصیلات بر طلاق

۷- گزارش تأثیر اختلاف سن بر میزان طلاق که در شکل ۹مشاهده می شود:



شکل ۹- گزارش نموداری تأثیر اختلاف سن بر طلاق

۱-۳.نرمال‌سازی داده‌ها: در نهایت، نرمال‌سازی داده‌ها انجام شد تا تمام داده‌ها هم‌سطح شده و برای ارزیابی توسط سیستم آماده شوند.

برای این تحقیق، از نرم‌افزار Jupyter Notebook، زبان پایتون، کتابخانه‌های TensorFlow و Keras استفاده شد که ابزارهای کلیدی برای مدل‌سازی و یادگیری ماشین هستند.

۲-Data Labeling And Division

در این مرحله داده‌های برچسب گذاری شده به دوبخش (X) و (y) تقسیم می شود. Xها داده های ورودی و y ها خروجی شبکه هستند و سیستم از روی این داده‌ها آموزش دید.چنانچه در شکل ۱۰ و۱۱مشاهده می شود:

داده‌های آموزشی سیستم (X)

TH	M_EAGE	M_EDUCATION	M_JOB	M_M_TIME	W_MONTH	W_EAGE	W_EDUCATION	W_JOB	W_M_TIME	EKHTELAPH_SEN	EKHTELAPH_SAVAD	DIVORCE
1	28	3	4	1.0	6	23	3	4	1	5	0	0
5	39	6	6	2.0	6	36	6	6	2	3	0	0
6	30	2	2	1.0	2	24	3	4	1	6	1	0
8	29	3	4	1.0	3	20	3	4	1	9	0	0
6	35	3	4	1.0	11	32	3	4	1	3	0	0

شکل ۱۰- داده‌های آموزشی سیستم (X)

برچسب‌ها(y)

```
0        0
1        0
2        0
3        0
4        0
        ..
33873    1
33874    1
33875    1
33876    1
33877    1
Name: DIVORCE, Length: 33878, dtype: int64
```

شکل ۱۱- داده‌های آموزشی سیستم (X)

۳-Training And Testing Split: در این مرحله داده‌ها به دو بخش داده‌های آموزشی و آزمایشی تقسیم می‌شود نسبت این دو به هم ۸۰ به ۲۰ درصد است .داده‌های آزمایشی جهت آزمودن مدل به‌دست‌آمده از داده‌های آموزشی به‌کاربرده خواهد شد.

4 - MLP Model Training:در این مرحله در ابتداو باتوجه به نیاز به کلاس بندی داده ها در دو کلاس success,no sucsess به معنی ازادواج موفق و ناموفق مدل MLP ساخته می شود،ساختار لایه ها به شرح زیر است:

- لایه اول: Dense

در شبکه عصبی چندلایه‌ای (MLP)، لایه Dense به‌عنوان لایه اول استفاده می‌شود. این لایه به‌صورت کاملاً متصل عمل می‌کند و وظیفه اتصال نورون‌ها میان دو لایه مختلف را بر عهده دارد. این لایه یک لایه خطی است و از تابع فعال‌سازی ReLU بهره می‌گیرد.

این لایه دارای یک ورودی با نام input_dim است که شامل ۱۲ ویژگی انتخابی می‌شود. در این لایه ۵۱۲ نورون تعریف شده است و در انتهای این لایه، ۶۵۰۰ پارامتر تولید می‌شود.

- لایه دوم: Dropout

برای منظم‌سازی و جلوگیری از بیش‌برازش، لایه Dropout بین دو لایه Dense قرار داده می‌شود. خروجی لایه قبلی به این لایه وارد می‌شود. این لایه هیچ پارامتری ندارد و در انتهای آن ۰ پارامتر ایجاد می‌شود.

- لایه سوم: Dense

لایه سوم شبکه نیز یک لایه Dense است که به‌صورت کاملاً متصل نورون‌ها را میان لایه‌ها ارتباط می‌دهد. این لایه نیز خطی بوده و از تابع فعال‌سازی ReLU استفاده می‌کند. خروجی لایه قبلی به این لایه وارد می‌شود که شامل ۵۰۰ نورون است. در انتهای این لایه، ۲۵۰,۵۰۰ پارامتر تولید می‌شود.

- لایه چهارم: Dropout

در این مرحله، خروجی لایه قبلی برای منظم‌سازی به یک لایه Dropout وارد می‌شود. مشابه لایه Dropout قبلی، این لایه نیز ۰ پارامتر ایجاد می‌کند.

- لایه پنجم: Dense

یک لایه Dense دیگر با ۵۰۰ نورون به‌عنوان لایه پنجم استفاده می‌شود. این لایه نیز به‌صورت کاملاً متصل و با تابع فعال‌سازی ReLU تعریف شده است. خروجی لایه قبلی وارد این لایه می‌شود و در

انتهای آن ۲۵۰,۵۰۰ پارامتر ایجاد می‌شود.

- لایه ششم: Dropout

برای منظم‌سازی، خروجی لایه Dense پنجم به لایه Dropout وارد می‌شود. مشابه مراحل قبل، این لایه نیز ۰ پارامتر تولید می‌کند.

- لایه هفتم: Dense

در این مرحله نیز یک لایه Dense دیگر با ۵۰۰ نورون تعریف می‌شود. این لایه، همچون مراحل قبلی، خطی است و از تابع فعال‌سازی ReLU استفاده می‌کند. خروجی لایه قبل وارد این لایه می‌شود و در انتهای آن ۲۵۰,۵۰۰ پارامتر ایجاد می‌شود.

- لایه هشتم: Dropout

برای جلوگیری از بیش‌برازش، یک لایه Dropout دیگر در این مرحله به کار می‌رود. خروجی لایه قبلی وارد این لایه می‌شود و در انتهای آن ۰ پارامتر تولید می‌شود.

- لایه نهم: Dense

این لایه نیز یک لایه Dense با ۵۰۰ نورون است که خروجی لایه قبلی را دریافت می‌کند. همچون لایه‌های مشابه، تابع فعال‌سازی این لایه ReLU است و در انتهای آن ۲۵۰,۵۰۰ پارامتر ایجاد می‌شود.

- لایه دهم: Dropout

برای منظم‌سازی، خروجی لایه Dense نهم به یک لایه Dropout وارد می‌شود که مشابه لایه‌های Dropout قبلی ۰ پارامتر تولید می‌کند.

- لایه یازدهم: Fully Connected (Dense)

در پایان، یک لایه کاملاً متصل (Dense) برای کلاس‌بندی نهایی تعریف می‌شود. این لایه وظیفه پیش‌بینی و تشخیص در دو کلاس موفقیت (Success) و عدم موفقیت (No Success) را بر عهده دارد. تابع فعال‌سازی این لایه با توجه به دو کلاس Softmax انتخاب می‌شود.

در جدول ۲ ساختار شبکه عصبی MLP در پایتون نشان داده‌شده است.

جدول ۲-ساختار شبکه عصبی MLP

Layer (type)	Output Shape	Param #
dense (Dense)	(None, 500)	6500
dropout (Dropout)	(None, 500)	0
dense_1 (Dense)	(None, 500)	250500
dropout_1 (Dropout)	(None, 500)	0
dense_2 (Dense)	(None, 500)	250500
dropout_2 (Dropout)	(None, 500)	0
dense_3 (Dense)	(None, 500)	250500
dropout_3 (Dropout)	(None, 500)	0
dense_4 (Dense)	(None, 500)	250500
dropout_4 (Dropout)	(None, 500)	0
dense_5 (Dense)	(None, 2)	1002

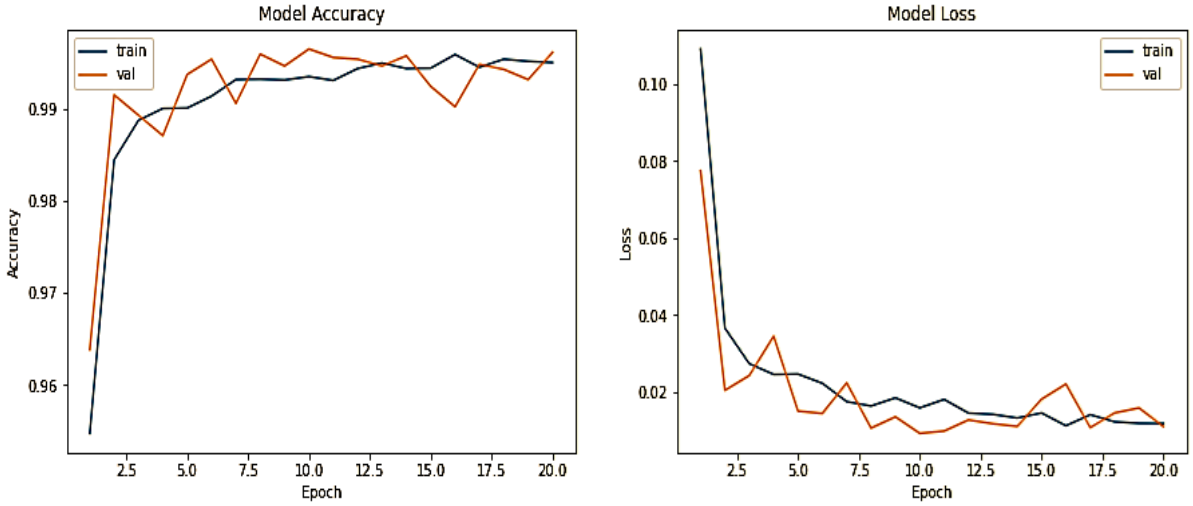
Total params: 1,009,502

Trainable params: 1,009,502

Non-trainable params: 0

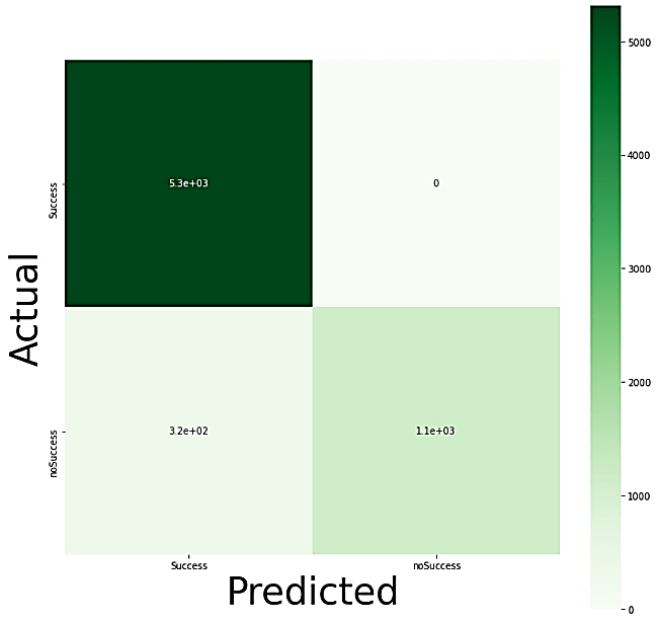
Training:در این تحقیق با دیتاست ذکر شده و تعداد ۲۰ دور آزمایش موردبررسی قرار می‌گیرد.

نتایج دقت و خطای مدل با داده های آموزش در شکل ۱۱ نمایش داده شده است:



شکل ۱۱ دیاگرام دقت و خطای مدل MLP

در شکل۱۲ ماتریس درهم‌ریختگی مدل MLP در پایتون نمایش داده شده است:



شکل۱۲- ماتریس درهم ریختگی MLP

۵. ارزیابی و نتایج :

در این مرحله، تشخیص طلاق زوجین با استفاده از داده‌های آزمایش انجام شده است. برای ارزیابی طبقه‌بندی ازدواج‌ها به دو دسته ازدواج موفق و ازدواج ناموفق، از معیارهای دقت (Accuracy)، دقت پیش‌بینی (Precision)، بازخوانی (Recall) و امتیاز F1 (F1-score) استفاده شده است.

- دقت (Accuracy) معیاری است که از نسبت تعداد موارد درست تشخیص داده‌شده به تعداد کل موارد محاسبه می‌شود. این معیار، نزدیکی یک مقدار محاسبه‌شده به مقدار واقعی یا طبیعی را نشان می‌دهد. فرمول محاسبه دقت، همان‌طور که در فرمول ۱ نشان داده شده، به این صورت است:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$$

فرمول۱

دقت پیش‌بینی (Precision):در معماری‌های یادگیری عمیق ، precision برای یک کلاس تعداد موارد واقعاً طبقه‌بندی‌شده (دارای برچسب صحیح) تقسیم بر مجموع اقلام درست یا نادرست با برچسب متعلق به آن طبقه است. چنانچه در فرمول ۲ مشاهده می نمایید.

$$\text{precision} = \frac{TP}{TP + FP}$$

فرمول ۲

بازخوانی (Recall): اشاره به کسری از مواردی که به‌درستی طبقه‌بندی‌شده به تعداد کل موارد طبقه‌بندی‌شده در یک کلاس دارد. چنانچه در فرمول ۳ مشاهده می نمایید.

$$\text{recall} = \frac{TP}{TP + FN}$$

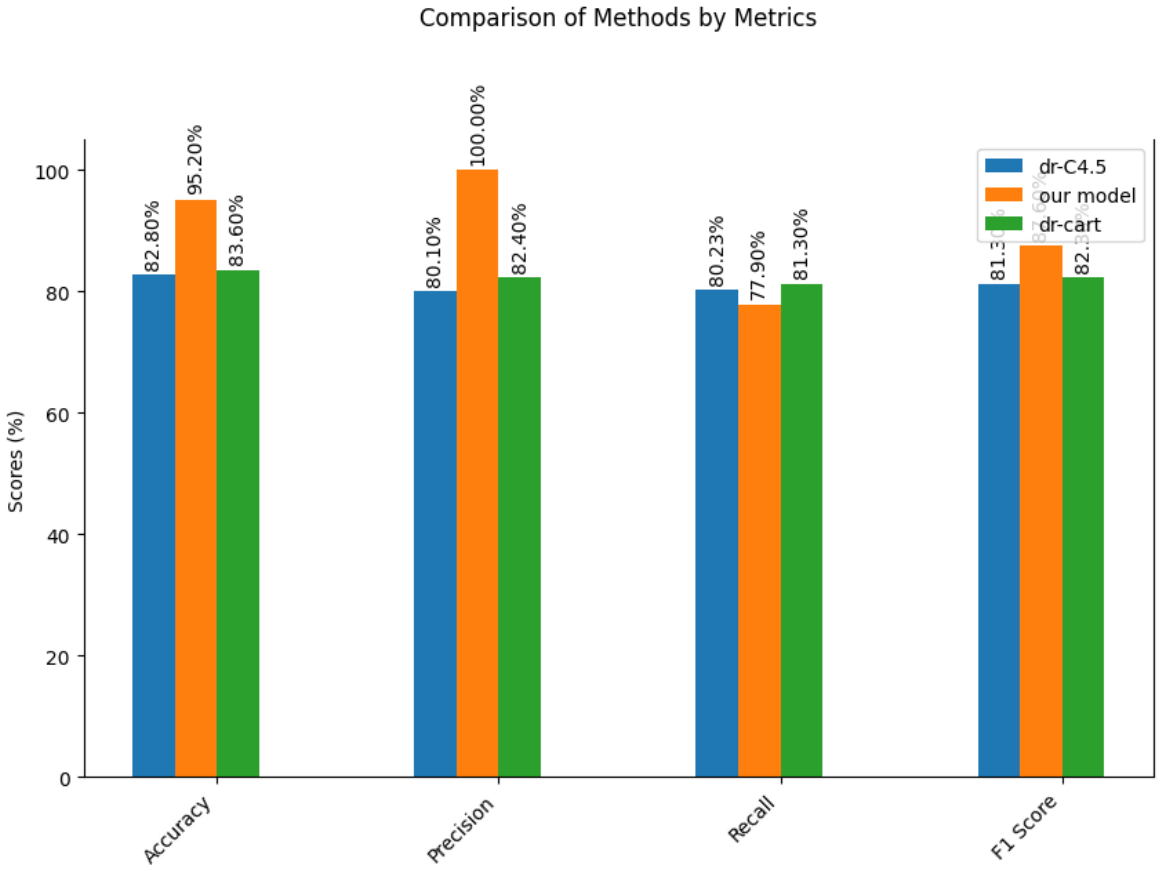
فرمول ۳

بر اساس مقادیر محاسبه‌شده برای بازخوانی (Recall) و دقت پیش‌بینی (Precision)، مقدار امتیاز F1 (F1-score) تعیین می‌شـــود. امتیاز F1 یک معیار کاربردی برای ارزیابی عملکرد مدل‌های طبقه‌بندی اســـت که به‌عنوان میانگین وزنی مقادیر بازخوانی و دقت پیش‌بینی تعریف می‌شـود.مقدار این معیار، در شـرایط ایده‌آل برابر با ۱ و در بدترین حالت برابر با ۰ است. [14].

همان‌طور که در جدول۳ وشکل ۱۳ مشاهده می‌شود، روش پیشنهادی با دو روش دیگر، شامل درخت تصمیم C4.5 و درخت تصمیم CART، مقایسه شده است. نتایج به‌دست‌آمده نشان می‌دهند که دقت روش پیشنهادی در مقایسه با سایر روش‌ها بالاتر بوده است. این امر بیانگر برتری و کارایی بالاتر این روش در تشخیص طلاق پیش از ازدواج بر اساس الگوهای استخراج‌شده از داده‌های واقعی می‌باشد.

جدول۳-مقایسه مدل های مختلف

روش	Accuracy	Precision	Recall	F1-score
درخت تصمیمC4.5	۸۲٫۸	۸۰,۱	۸۰,۲۳	۸۱,۳
روش پیشنهادی	۹۵,۲	۱۰۰	۷۷,۹	۸۷,٦
درخت تصمیمCART	۸۳,٦	۸۲,٤	۸۱,۳	۸۲,۳



شکل۱۳- مقایسه مدل های جدول ۳

۶. نتیجه‌گیری

نتایج ارائه‌شده در این تحقیق نشان‌دهنده‌ی عملکرد بالای روش پیشنهادی در مقایسه با سایر الگوریتم‌های متداول مانند درخت تصمیم C4.5 و CART است. از نظر دقت(Accuracy) ، روش پیشنهادی با مقدار ۹۵.۲ درصد به‌طور قابل‌توجهی بهتر از درخت تصمیم C4.5 (۸۲.۸ درصد) و CART (۸۳.۶ درصد) عمل کرده است. این نشان می‌دهد که روش پیشنهادی در پیش‌بینی درست نتایج ازدواج‌ها نسبت به سایر روش‌ها موفق‌تر بوده است.

در زمینه معیار دقت پیش‌بینی(Precision) ، روش پیشنهادی به مقدار قابل‌توجه ۱۰۰ درصد دست یافته است، که حاکی از توانایی بالای این روش در کاهش پیش‌بینی‌های مثبت اشتباه (False Positives) است. در مقایسه، درخت‌های تصمیم C4.5و CART به ترتیب مقادیر ۸۰.۱ و ۸۲.۴ درصد را نشان داده‌اند.

بااین‌حال، در معیار بازخوانی(Recall) ، روش پیشنهادی با مقدار ۷۷.۹ درصد عملکرد ضعیف‌تری نسبت به دقت کلی خود نشان داده است، که نشان‌دهنده کاهش توانایی در شناسایی تمامی نمونه‌های مثبت واقعی (True Positives) است. این موضوع در مقایسه با Recall در درخت تصمیم C4.5 (۸۰.۲۳ درصد) و CART (۸۱.۳ درصد) مشهود است.

در معیار ترکیبیF1-score ، روش پیشنهادی با مقدار ۸۷.۶ درصد در جایگاهی بین عملکرد مطلوب در معیار Precision و کاستی‌ها در Recall قرار دارد. این نتیجه، در مقایسه با F1-score برای C4.5 (۸۱.۳ درصد) و CART (۸۲.۳ درصد)، بهبود قابل‌توجهی را نشان می‌دهد و قدرت تعادل روش پیشنهادی در بین معیارهای Precision و Recall را تأیید می‌کند.

به‌طور کلی، می‌توان نتیجه گرفت که روش پیشنهادی در این پژوهش، با ارائه دقت بالا و عملکرد بهتر در برخی از معیارهای اصلی، نسبت به روش‌های متداول پیشین در پیش‌بینی موفقیت یا عدم موفقیت ازدواج‌ها مزیت قابل‌توجهی دارد و می‌تواند ابزار ارزشمندی برای تحلیل و تصمیم‌گیری در این زمینه باشد.

۷. مراجع

[1] F. Gorunescu, Data Mining: Concepts, models and techniques, vol. 12, Springer Science & Business Media, 2011, p. 201.
[2] J. Brownlee, Deep learning with Python: develop deep learning models on Theano and TensorFlow using Keras. Machine Learning Mastery, 2016.
[3] M. K. Yöntem, A. Kemal, T. Ilhan, and S. Kiliçarslan, “Divorce prediction using correlation based feature selection and artificial neural networks,” Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi, vol. 9, no. 1, pp. 259-273, 2019.
[4] M. Elahi Chooran, M. T. Heydari, H. Khorshidi, and M. Zafary, "Spatial analysis of divorce distribution in Iranian provinces using GIS," Human Geography Research, vol. 56, no. 3, pp. 17-33, 2024.
[5] Nasser, “Predicting whether a couple is going to get divorced or not using artificial neural networks,” International Journal of Engineering and Information Systems (IJEAIS), vol. 3, no. 10, pp. 49-55, 2019.
[6] P. Ranjitha and A. Prabhu, “Improved divorce prediction using machine learning- particle swarm optimization (PSO),” 2020 International Conference for Emerging Technology (INCET), Belgaum, India, IEEE, June 2020, pp. 1–5,
[7] J. Kong and T. Chai, "Is your marriage reliable? divorce analysis with machine learning algorithms," in Proceedings of the 2020 6th International Conference on Computing and Artificial Intelligence, 2020, pp. 1-4.
[8] N. Hafidz, Sfenrianto, Y. Sfenrianto, Y. Pribadi, E. Fitri, and Ratino, “ANN and SVM algorithm in divorce predictor,” International Journal of Engineering and Advanced Technology, vol. 9, no. 3, pp. 2523–2527, 2020.
[9] Sharma, A. S. Chudhey, and M. Singh, “Divorce case prediction using machine learning algorithms,” 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, March 2021, pp. 214–219,.
[10] S. Enggari and S. Defit, “Divorce Fact Detection Based on Internet User Behavior Using Hybrid Systems with Combination of Apriori Algorithm and K-Means

Method," Khazanah Informatika: Jurnal Ilmu Komputer dan Informatika, vol. 8, no. 1, 2022.

[11] N. Flores, S. Silva, S. Silva, A. I. Group, "Machine learning model to predict the divorce of a married couple," 3C Tecnolog´ıa_Glosas de innovaci´on aplicadas a la pyme, pp. 83–95, 2021.

[12] M. M. Sadiq Fareed, A. Raza, N. Zhao, A. Tariq, F. Younas, G. Ahmed, "Predicting divorce prospect using ensemble learning: Support vector machine, linear model, and neural network, " Computational Intelligence and Neuroscience, vol. 2022, no. 1, p. 1-15, 2022.

[13] Narendran, R. Abilash, and B. Charulatha, "Exploration of classification algorithms for divorce prediction," in Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, Springer, 2021,pp. 291-303.

[14] S. Fouladi, M. Ebadi, A. A. Safaei, M. Y. Bajuri, and A. Ahmadian, "Efficient deep neural networks for classification of COVID-19 based on CT images: Virtualization via software defined radio," Computer communications, vol. 176, pp. 234-248, 2021.

شناسایی و جبران‌سازی اختلال جمینگ GPS با استفاده از فیلتر وفقی مبتنی بر الگوریتم حداقل مربعات خطا

سامره صفری[۱]، کوروش زرین نگار[۲]، سید محمدرضا موسوی میرکلائی[*۳]

۱- کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۲- دانشجوی دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

۳- استاد، نویسنده مسئول، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران

چکیده

سامانه موقعیت‌یابی جهانی (GPS)[†] به دلیل ماهیت ضعیف سیگنال‌های دریافتی، در معرض تهدیدات مختلف از جمله حملات جمینگ قرار دارد. حملات جمینگ از طریق ارسال امواج مخرب باعث می‌شوند که گیرنده‌های GPS قادر به دریافت صحیح سیگنال‌های اصلی نباشند که می‌تواند منجر به از دست رفتن موقعیت‌یابی و زمان‌بندی دقیق شود. این تحقیق یک روش شناسایی و جبران‌سازی اختلال جمینگ GPS بر اساس فیلترهای وفقی، با تأکید بر الگوریتم حداقل مربعات خطا (LMS)[‡] ارائه می‌دهد که هدف آن، طراحی سامانه‌ای است که با استفاده از پردازنده ARM[§]، توانایی شناسایی و حذف اثرات جمینگ را داشته باشد. شبیه‌سازی‌ها و پیاده‌سازی‌های عملی نشان می‌دهند که سامانه پیشنهادی بهبود قابل توجهی در نسبت سیگنال به نویز (SNR) و کاهش میانگین مربعات خطا (MSE)[**] داشته است و می‌تواند به‌طور مؤثری در سامانه‌های تعبیه‌شده و کم‌مصرف به کار گرفته شود.

کلمات کلیدی: GPS، جمینگ، فیلتر وفقی، الگوریتم LMS، جمینگ موج پیوسته (CW)، جمینگ پالس.

۱. مقدمه

سامانه‌های موقعیت‌یاب جهانی (GPS) در بسیاری از کاربردها از جمله ناوبری، عملیات دفاعی، خدمات مکان‌یابی و زمان‌بندی استفاده می‌شوند. این سامانه از سه بخش فضایی، کنترل و کاربر تشکیل شده است. بخش فضایی شامل مجموعه‌ای از ۲۴ ماهواره در مدار زمین است که در ارتفاع ۲۰۲۰۰ کیلومتری به دور زمین می‌چرخند. این ماهواره‌ها سیگنال‌هایی را ارسال می‌کنند که اطلاعات موقعیت و زمان دقیق را در اختیار گیرنده‌ها قرار می‌دهند. بخش کنترل شامل ایستگاه‌های زمینی است که وظیفه نظارت و اصلاح مسیر ماهواره‌ها را بر عهده دارند و بخش کاربر نیز شامل گیرنده‌های GPS است که

[*] **Corresponding Author (Email: m_mosavi@iust.ac.ir)**

[†] Global Positioning System (GPS)
[‡] Least Mean Square (LMS)
[§] Advanced Risk Machine (ARM)
[**] Mean Square Error (MSE)

سیگنال‌های ماهواره‌ای را دریافت و پردازش می‌کنند تا موقعیت مکانی دقیق تعیین شود [۱-۵]. سیگنال GPS شامل چندین نوع کد است که مهم‌ترین آن‌ها عبارتند از:

- کد C/A: این کد برای کاربردهای تجاری طراحی شده است و با فرکانس ۱،۰۲۳ مگاهرتز مدوله شده است.
- کد P: این کد برای کاربردهای دفاعی طراحی شده و دارای امنیت بالاتری است.
- کد Y: نسخه رمزگذاری‌شده کد P که تنها در دسترس نظامیان آمریکاست.

ماهواره‌های GPS بر دو فرکانس L1 (۱۵۷۵،۴۲ مگاهرتز) و L2 (۱۲۲۷،۶۰ مگاهرتز) سیگنال ارسال می‌کنند. فرکانس L1 برای کاربردهای تجاری استفاده می‌شود و فرکانس L2 عمدتاً در کاربردهای دفاعی و پیشرفته‌تر به‌کار می‌رود. فناوری GPS سنگ بنای ناوبری و عملیات تجاری و دفاعی است. ساختار و ویژگی‌های سیگنال آن به آن اجازه می‌دهد تا اطلاعات موقعیت‌یابی بسیار دقیق را در طیف گسترده‌ای از برنامه‌ها ارائه دهد. با این حال، وابستگی به GPS نیز آسیب پذیری‌های آن را برجسته کرده است، به‌ویژه در مورد جمینگ که در بخش بعدی مورد بحث قرار خواهد گرفت [۶].

در سال‌های اخیر، تحقیقات گسترده‌ای برای مقابله با اختلالات جمینگ در سامانه‌های GPS انجام شده است. به‌عنوان مثال، بوریو [۷]، بر توسعه فیلترهای شکاف برای کاهش تداخلات فرکانسی در GPS تمرکز کردند. اگرچه روش آن‌ها برای کاهش جمینگ موج پیوسته (CW) مؤثر بود، اما در مقابله با سیگنال‌های جمینگ پیچیده‌تر (مانند جمینگ پالسی)، بهبود بیشتری نیاز داشت. چن و همکاران [۸]، استفاده از روش‌های یادگیری ماشین را برای تشخیص و کاهش جمینگ معرفی کردند. با وجود دقت بالای این روش‌ها، نیاز به منابع محاسباتی زیاد، باعث محدودیت استفاده از آن‌ها در سامانه‌های تعبیه‌شده کم‌مصرف شده است. از سوی دیگر، یوسف و همکاران [۹] با استفاده از روش‌های نوین پردازش سیگنال در حوزه فرکانس، به کاهش اثرات تداخلات جمینگ در گیرنده‌های GNSS پرداختند. روش آن‌ها، اگرچه به دلیل قابلیت پردازش سریع و دقت بالا در کاهش تداخل موثر بوده است، اما نیاز به سخت‌افزارهای پیشرفته مانند FPGA، پیچیدگی پیاده‌سازی و هزینه‌های سیستم را به میزان قابل‌توجهی افزایش می‌دهد. الیزی و همکاران [۱۰] یک روش شناسایی و تشخیص حملات جمینگ الکترونیکی بر اساس توان سیگنال ارائه کردند. این رویکرد، مشابه تلاش‌های انجام شده برای طراحی سیستم‌های کم‌هزینه مانند STM32، به شناسایی انواع مختلف جمینگ پرداخته، اما پیچیدگی آن در مقابله با حملات پیشرفته محدودیت‌هایی داشته است. برخلاف این روش‌ها، که اغلب بر روش‌های پردازش پیچیده یا سخت‌افزارهای پرهزینه متکی بودند، در تحقیق حاضر یک سامانه ضدجمینگ مبتنی بر فیلتر وفقی LMS طراحی و آماده پیاده‌سازی شده است که قادر است حملات جمینگ را با کارایی بالا شناسایی و کاهش دهد.

۲. بیان مسئله‌ی اختلال جمینگ

سیگنال‌های ارسالی از ماهواره‌های GPS، پس از طی مسافت طولانی تا رسیدن به گیرنده، با کاهش شدیدی در توان مواجه می‌شوند. این سیگنال‌های ضعیف به‌راحتی می‌توانند در معرض تداخلات عمدی و غیرعمدی قرار گیرند که موجب کاهش دقت یا از کار افتادن کامل سامانه می‌شود و یکی از بزرگترین چالش‌ها در سامانه‌های GPS است. این تداخل‌ها شامل سیگنال‌های ناخواسته RF هستند که از منابع مختلف تولید و توسط گیرنده‌های GPS دریافت می‌شوند [۱۱-۱۳]. برخی از انواع تداخلات و روش‌های جمینگ که می‌توانند عملکرد سامانه GPS را مختل کنند، عبارتند از:

۲,۱. جمینگ موج پیوسته (CW)

این نوع جمینگ شامل ارسال سیگنال با توان بسیار بالاتر از سیگنال ارسالی GPS است و باعث می‌شود گیرنده قادر به دریافت سیگنال‌های اصلی نباشد. این نوع اختلال معمولاً یک سیگنال تک‌تون یا چندتون را به‌صورت مداوم ارسال می‌کند. رابطه این نوع جمینگ به شکل رابطه (۱) است:

$$j(t) = \sum_{k=1}^{K} \sqrt{P_{J_k}}\, exp(j(2\pi f_{J_k} t + \theta_{J_k})) \quad (۱)$$

که در آن، P_{J_k}، f_{J_k} و θ_{J_k} به ترتیب دامنه، فرکانس و فاز تن kام می‌باشند و K تعداد تون‌ها است [۱۲و۱۳].

۲,۲. جمینگ پالس

جمینگ پالس شامل انتقال انفجارهای کوتاه نویز با توان بالا در فواصل زمانی منظم است. این سیگنال‌ها به‌صورت دوره‌ای ارسال می‌شوند و توانایی گیرنده GPS را در تمایز بین سیگنال واقعی و سیگنال‌های جمینگ تحت تأثیر قرار می‌دهند. این نوع جمینگ، مصرف انرژی را بهینه و در عین حال اختلال قابل توجهی در سیگنال ایجاد می‌کند. معادله مربوط به این نوع جمینگ به صورت رابطه (۲) است:

$$j(t) = \sqrt{P_J} p_\tau(t) \otimes \sum_{k=1}^{K} \delta\left(t - \frac{k}{f_{r_k}}\right).exp(j2\pi f_{J_k} t) \quad (۲)$$

که در این رابطه، $p_\tau(t)$ پالس مربعی با عرض (سیکل وظیفه) τ ، f_r فرکانس تکرار پالس، $\delta(t)$ تابع پالس دیراک و $\otimes$ عملگر کانولوشن* است [۱۴].

۲,۳. جمینگ جارویی (رفت و برگشتی)

در این نوع، سیگنال جمینگ به‌طور مداوم در بازه‌ای از فرکانس‌ها تغییر می‌کند و کل باند فرکانسی GPS را تحت پوشش قرار می‌دهد. این نوع جمینگ، به‌ویژه برای گیرنده‌های GPS با فیلترهای باند باریک، بسیار مخرب است. رابطه معادله جمینگ جارویی به شکل رابطه (۳) است:

$$j(t) = \sqrt{P_J} cos(2\pi(f0 + \Delta f \cdot t/Ts)t + \theta j) \quad (۳)$$

به‌طوری‌که در این رابطه، P_J توان جمینگ، $f0$ فرکانس شروع جاروب و Δf بازه فرکانسی جاروب و Ts دوره زمانی جاروب و θj فاز سیگنال است [۱۵و۱۶].

۲,۴. جمینگ چیرپ

جمینگ چیرپ شامل سیگنال‌هایی است که فرکانس آن‌ها به‌صورت خطی در طول زمان تغییر می‌کند. این نوع جمینگ به‌طور خطی فرکانس را در بازه‌ای از فرکانس‌ها جاروب می‌کند. رابطه این نوع جمینگ به شکل رابطه (۴) است:

$$j(t) = \sqrt{P_J}.\exp(j(2\pi f_J t + \pi b(\frac{f_{\max} - f_{\min}}{T_{swp}})t^2 + \theta_J)) \quad (۴)$$
$$= \sqrt{P_J}.\exp(j(f_q(t)t + \theta_J))$$

* Convolution Operator

در این رابطه، P_J توان جمینگ، f_J فرکانس شروع جاروب (در زمان $T_{swp} = 0$)، f_{min} و f_{max} فرکانس کمینه و بیشینه جاروب و T_{swp} دوره زمانی جاروب است که برابر مدت زمانی است که طول می‌کشد تا جمینگ از فرکانس f_{min} تا f_{max} جاروب شود. متغیر $b = \pm 1$ یک متغیر برای مشخص کردن این است که اگر $b = +1$ آنگاه چیرپ بالا و اگر $b = -1$ آنگاه چیرپ پایین داریم [۱۵و۱۶].

۲,۵. جمینگ رگبار

این نوع جمینگ به‌صورت همزمان سیگنال‌های جمینگ را در فرکانس‌های مختلف ارسال می‌کند. این روش مطمئن می‌شود که حتی اگر گیرنده GPS سعی کند فرکانس خود را تغییر دهد، سیگنال جمینگ همچنان موثر است. معادله (۵) نشان‌دهنده جمینگ رگبار می‌باشد.

$$j(t) = \sum_{k=1}^{N} \sqrt{P_{J,K}}\, exp\big(j(2\pi f_{J,K} t + \theta_{J,K})\big) \qquad (۵)$$

که در این رابطه، $P_{J,K}$ توان هر سیگنال جمینگ است و $f_{J,K}$ هر فرکانس فردی که جمینگ شده و N تعداد کل فرکانس‌هایی است که مختل شده‌اند و $\theta_{J,K}$ فاز هر جزء است [۱۳].

۲,۶. جمینگ نقطه‌ای

در این نوع جمینگ، یک فرکانس خاص با سیگنال پرقدرت هدف قرار می‌گیرد. این نوع جمینگ به‌ویژه در برابر گیرنده‌های GPS که تنها به یک باند فرکانسی تکیه دارند، بسیار مؤثر است. معادله این نوع جمینگ به فرم رابطه (۶) است:

$$j(t) = \sum_{k=1}^{N} \sqrt{P_s}\, cos\,(2\pi f_s t + \theta_s) \qquad (۶)$$

که در این رابطه، P_s توان سیگنال جمینگ نقطه‌ای است و f_s آن فرکانس خاصی است که متمرکز شده است و θ_s فاز سیگنال جمینگ است. به طور خلاصه انواعی از حملات جمینگ و خصوصیات آن در جدول (۱) ارائه شده است.

جدول (۱) : خلاصه‌ای از روش‌های جمینگ و ویژگی‌های آن‌ها.

روش‌های جمینگ	فرکانس هدف	بهره‌وری قدرت	تاثیر بر سیگنال GPS
جمینگ موج پیوسته	تک فرکانس	بالا	اختلال مداوم در یک فرکانس خاص
جمینگ پالس	پالس‌های متعدد	متوسط	اختلال متناوب؛ تداخل بحرانی زمان
جمینگ چیرپ	رفت و برگشتی	متوسط	اختلال در محدوده فرکانس وسیع
جمینگ جاروبی	رفت و برگشتی	متوسط رو به بالا	تداخل مداوم در یک باند فرکانس وسیع
جمینگ رگبار	فرکانس‌های چندگانه	پایین	اختلال باند پهن که بر فرکانس‌های GPS متعدد تأثیر می‌گذارد.
جمینگ نقطه‌ای	تک فرکانس	بالا	اختلال متمرکز و با توان بالا در یک فرکانس خاص

خلاصه‌ای از انواع اختلال جمینگ در جدول (۱) نشان داده شده‌اند. این روش‌های جمینگ چالش‌های قابل‌توجهی را برای قابلیت اطمینان و دقت سامانه‌های GPS به‌ویژه در کاربردهای حیاتی که دریافت بی‌وقفه سیگنال ضروری است، ایجاد می‌کند. جمینگ باعث می‌شود گیرنده GPS نتواند تعداد کافی از ماهواره‌ها را برای تعیین موقعیت شناسایی کند. بدون شناسایی حداقل چهار ماهواره، گیرنده GPS قادر به تعیین موقعیت مکانی نخواهد بود. بنابراین، اختلالات جمینگ به‌ویژه جمینگ موج پیوسته می‌توانند عملکرد سامانه‌های ناوبری را به‌طور کامل مختل کنند.

۳. طراحی الگوریتم فیلتر وفقی

فیلترهای وفقی به‌صورت پویا پارامترهای خود را تنظیم می‌کنند تا با سیگنال‌های ورودی سازگار شوند و تداخلات را کاهش دهند. الگوریتم LMS یکی از مهم‌ترین و مؤثرترین روش‌ها برای به‌روزرسانی ضرایب فیلتر در زمان واقعی است.

۳,۱. مدل سیگنال دریافتی

سامانه ضدجمینگ GPS برای کاهش CW های چندتون و در عین حال حفظ کیفیت سیگنال GPS طراحی شده است. مدل سیگنال دریافتی توسط گیرنده GPS در شرایط جمینگ به صورت رابطه (۷) مدل‌سازی می‌شود:

$$y(t)=s(t)+j(t)+w(t) \quad (۷)$$

که در این رابطه، $s(t)$ سیگنال GPS مورد نظر، $w(t)$ نشان دهنده نویز سفید گاوسی افزودنی (AWGN) است و $j(t)$ تداخل موج پیوسته (CW) را نشان می‌دهد [۱۲].

۳,۲. فیلتر وفقی LMS

فیلترهای وفقی برای حذف تداخل از سیگنال‌های اصلی به کار می‌روند. فیلترهای وفقی به‌صورت پویا پارامترهای خود را تنظیم می‌کنند تا با سیگنال‌های ورودی سازگار شوند و تداخلات را کاهش دهند. الگوریتم LMS یکی از مؤثرترین روش‌ها برای به‌روزرسانی ضرایب فیلتر در زمان واقعی است. این الگوریتم به دلیل سادگی و کارایی، یکی از محبوب‌ترین الگوریتم‌ها در این حوزه است. رابطه به‌روزرسانی ضرایب فیلتر LMS به شرح رابطه (۸) است:

$$w(n+1)=w(n)+2\mu e(n)x(n) \quad (۸)$$

که در آن، $w(n)$ وزن‌های فیلتر در لحظه n، $e(n)$ خطای محاسبه‌شده بین سیگنال ورودی و سیگنال مرجع، $x(n)$ ورودی فیلتر و μ نرخ یادگیری است. هدف الگوریتم LMS به حداقل رساندن میانگین مربعات خطا (MSE) است تا تداخلات جمینگ کاهش یابد و سیگنال GPS بازیابی شود [۷].

۳,۳. شبیه‌سازی الگوریتم

برای شبیه‌سازی فیلتر وفقی، از سیگنال‌های جمینگ موج پیوسته (CW) و پالس و سیگنال‌های GPS شبیه‌سازی‌شده استفاده شد. پاسخ فیلتر در محیط MATLAB مورد بررسی قرار گرفت و بهبود در نسبت سیگنال به نویز (SNR) و کاهش میانگین مربعات خطا (MSE) به دست آمد.

۴. ارزیابی عملکرد الگوریتم

برای بررسی عملکرد فیلتر LMS، شبیه‌سازی‌ها در محیط MATLAB انجام شد که شرایط مختلف جمینگ را شامل می‌شد [۹و۱۷]. سیگنال GPS به صورت موج سینوسی با فرکانس معمول سیگنال‌های GPS تولید می‌شود.

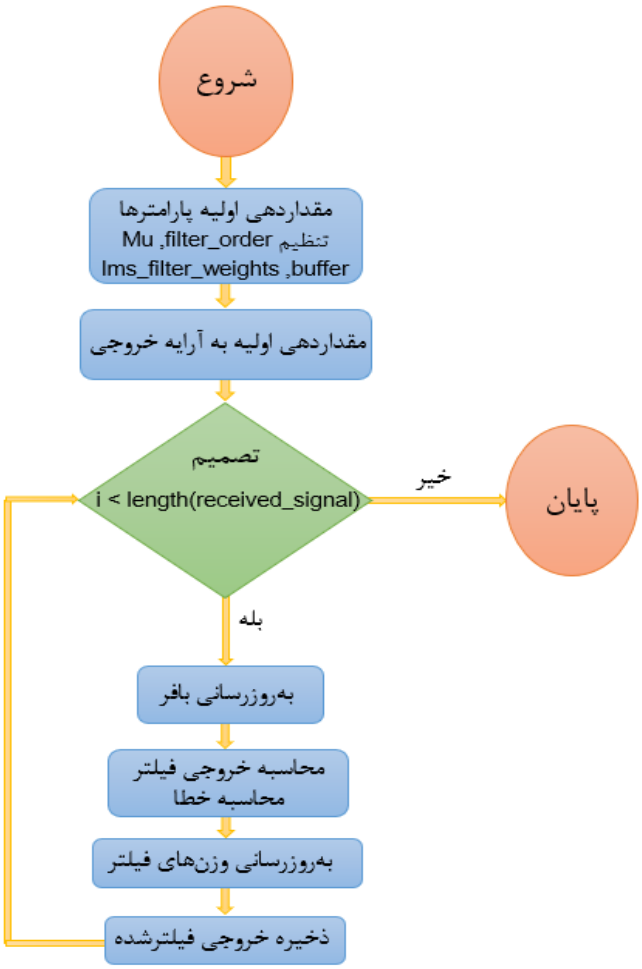
سیگنال‌های جمینگ (موج پیوسته، پالس) به‌طور جداگانه تولید شده و برای ایجاد یک سیگنال ترکیبی (GPS + Jamming) به سیگنال GPS اضافه شدند تا سیگنال ورودی و دریافت‌شده توسط فیلتر را تشکیل دهند. با توجه به اینکه فرکانس L1 برای سیگنال‌های GPS تقریباً ۱,۵۷۵۴۲ گیگاهرتز است، باید نرخ نمونه‌برداری f_s و فرکانس قطع را بر این اساس تنظیم نموده تا فیلتری مناسب برای سیگنال‌های GPS طراحی کنیم. f_s بیشتر از دو برابر فرکانس L1 تنظیم شد تا معیار نایکوئست را برآورده کند و اطمینان حاصل شود که سیگنال به درستی نمونه‌برداری شده است. لازم به ذکر است این بزرگی نیز باید به حدی باشد که بعدا بتواند بر روی ریزپردازنده به درستی اجرا شود. فرکانس قطع کمی کمتر از فرکانس L1 برای فیلتر کردن تداخل فرکانس بالا و در عین حال حفظ سیگنال‌های GPS انتخاب شد. تنظیم نرخ نمونه و فرکانس قطع بر اساس الزامات خاص GPS تضمین می‌کند که فیلتر به گونه‌ای طراحی شده است که به‌طور موثر اختلال جمینگ GPS را فیلتر نماید و در عین حال سیگنال‌های GPS را در محدوده فرکانس مورد نظر حفظ کند [۱۸و۱۹].

فرکانس سیگنال: با مقدار f_sin = 1.405e6 تنظیم شده است. این فرکانس به‌عنوان یک سیگنال سینوسی نماینده سیگنال GPS شبیه‌سازی شده است. کاهش این فرکانس به محدوده ۱,۴۰۵ مگاهرتز امکان شبیه‌سازی دقیق‌تر و کم‌هزینه‌تر از نظر محاسباتی را فراهم می‌کند.

فرکانس جمینگ: در این شبیه‌سازی، سیگنال جمینگ به‌عنوان یک سیگنال موج پیوسته در نظر گرفته شده است و با مقدار f_jam = 1.43e6 تنظیم شده است. این فرکانس به منظور ایجاد تداخل مؤثر با سیگنال GPS انتخاب شده و اختلاف کوچک ۲۵ کیلوهرتز با فرکانس سیگنال GPS دارد. انتخاب این فاصله اندک از فرکانس اصلی GPS، به خوبی ویژگی‌های جمینگ را شبیه‌سازی می‌کند که تداخل فرکانسی بسیار نزدیک به سیگنال اصلی است و نیاز به فیلتر دقیق دارد. برای نوع جمینگ پالس، با استفاده از تابع mod، یک قطار پالس به وجود می‌آوریم که هر پالس به مدت ۰,۰۱ ثانیه فعال است و سپس به مدت ۰,۰۱ ثانیه غیرفعال می‌باشد. سیگنال جمینگ تولید شده و سپس با قطار پالس مدوله می‌شود تا یک سیگنال جمینگ پالسی ایجاد نماید.

فرکانس نمونه‌برداری: این پارامتر Fs = 5.714e6 نرخ نمونه‌برداری سیگنال‌ها را مشخص می‌کند. در هر دو نوع جمینگ، نرخ نمونه‌برداری یکسان نگه داشته شده است تا هم معیار نایکوئیست رعایت شود و هم سیگنال‌های مربوط به GPS و جمینگ به درستی پردازش شوند و قابل مقایسه باشند.

مدت زمان سیگنال: ۰,۱ ثانیه در نظر گرفته شد. بردار زمان، به صورت t = 0:1/Fs:duration-1/Fs تعریف شده است که نحوه توزیع نمونه‌ها را تعیین می‌کند. شکل (۱) فلوچارت مربوط به فیلتر وفقی با الگوریتم LMS را نشان می‌دهد.



شکل (۱) گردش کار مربوط به بخش اعمال فیلتر وفقی LMS.

پارامترهای فیلتر وفقی به صورت زیر تعریف می‌شود:

Mu: نرخ یادگیری فیلتر LMS که تعیین‌کننده سرعت تنظیم ضرایب فیلتر است.

filter_order: مرتبه فیلتر که تعداد ضرایب فیلتر LMS و اندازه بافر را مشخص می‌کند.

lms_filter_weights: ضرایب اولیه فیلتر که در ابتدا به مقدار صفر تنظیم شده‌اند.

buffer: یک بافر برای ذخیره مقادیر نمونه‌های سیگنال ورودی استفاده می‌شود و به ترتیب تاخیر نمونه‌ها را فراهم می‌کند.

ایجاد متغیر filtered_signal: این متغیر به اندازه سیگنال دریافتی (ترکیب سیگنال اصلی و جمینگ) مقدار صفر می‌گیرد تا سیگنال فیلتر شده در آن ذخیره شود.

حلقه اصلی برای اعمال فیلتر LMS: در این حلقه، برای هر نمونه از سیگنال دریافتی، مراحل زیر انجام می‌شود:

الف. به‌روزرسانی بافر: نمونه‌ی جدید از سیگنال دریافتی به ابتدای بافر اضافه می‌شود و سایر نمونه‌ها یک موقعیت به جلو منتقل می‌شوند. این عمل به فیلتر کمک می‌کند تا با داده‌های به‌روز کار کند.

ب. محاسبه خروجی فیلتر (y): خروجی فیلتر با ضرب داخلی بین ضرایب فیلتر (lms_filter_weights) و بافر محاسبه می‌شود. این خروجی تخمینی از سیگنال اصلی GPS است.

ج. محاسبه خطا (error): خطا به عنوان تفاوت بین سیگنال اصلی و خروجی فیلتر محاسبه می‌شود. این خطا به فیلتر LMS کمک می‌کند تا میزان اختلاف را بررسی و ضرایب خود را تنظیم کند.
د. به‌روزرسانی ضرایب فیلتر: ضرایب فیلتر با استفاده از قانون به‌روزرسانی LMS تنظیم می‌شوند. این فرآیند به فیلتر اجازه می‌دهد که به‌طور خودکار خود را با شرایط تغییر یافته‌ی سیگنال وفق دهد و سیگنال جمینگ را کاهش دهد.
ه. ذخیره خروجی فیلتر: مقدار y به عنوان سیگنال فیلترشده در filtered_signal ذخیره می‌شود.
معیارهای ارزیابی شامل بهبود نسبت سیگنال به نویز (SNR) و کاهش میانگین مربعات خطا (MSE) بودند.
SNR در ارزیابی عملکرد فیلتر وفقی، به صورت رابطه (۹) محاسبه شد:

$$SNR\ improvement = \frac{Psignal}{Pnoise} \quad (۹)$$

MSE که یکی از معیارهای مهم در ارزیابی عملکرد فیلتر وفقی است، به صورت رابطه (۱۰) محاسبه شد:

$$MSE = \frac{1}{N}\sum_{n=1}^{N} e_n^2 \quad (۱۰)$$

که در آن، N تعداد نمونه‌ها و e_n خطای هر نمونه است. نمودار شکل (۲) نشان‌دهنده کاهش MSE بعد از اعمال فیلتر است. برای رسم نتایج قبل و بعد از فیلتر کردن از نمودارهای MATLAB استفاده شد. این امکان مقایسه سیگنال اصلی، سیگنال جمینگ، سیگنال ترکیب شده و در انتها سیگنال فیلترشده را در هر دو حوزه زمان و فرکانس فراهم کرد. توان سیگنال‌ها را هم محاسبه و قابل چاپ کرده و از معیارهای عملکرد SNR و JSR قبل و بعد از فیلتر کردن برای کمّی کردن و رویت بهبود (و یا وخامت) کیفیت سیگنال عبوری محاسبه شدند. برای مثال، با Mu=0.001 و مرتبه فیلتر ۳۲ به شرح زیر می‌باشند.

SNR of Received Signal: 6.02 dB
SNR of Filtered Signal: 25.60 dB
JSR of Received Signal: -6.02 dB

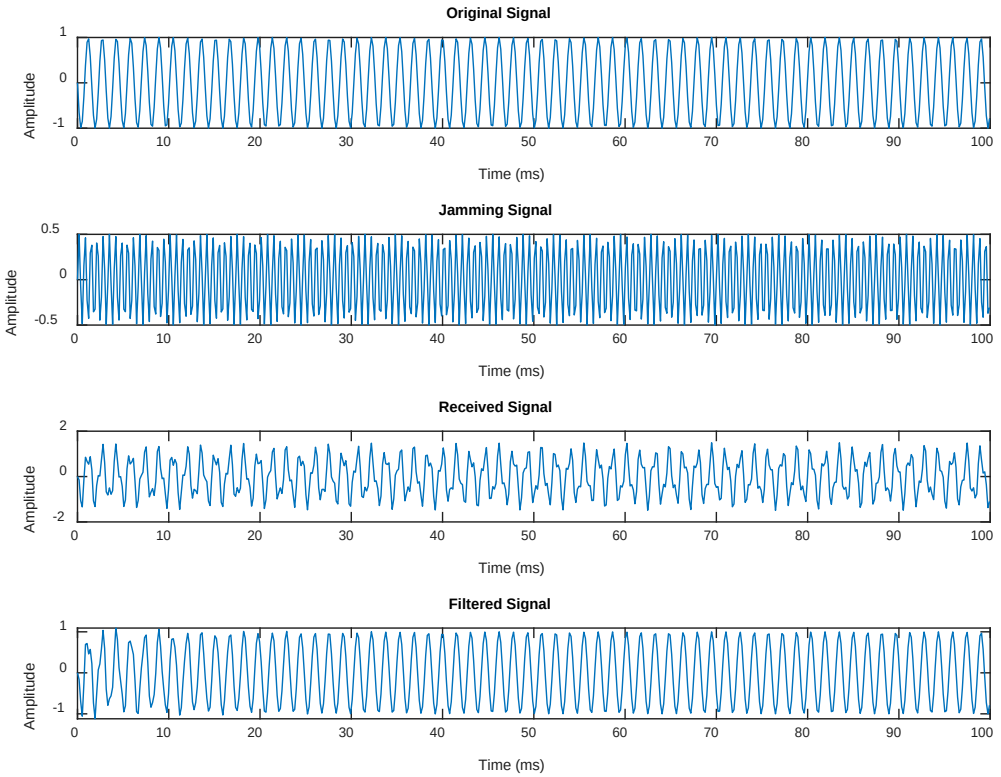
۴،۱. نتایج شبیه‌سازی

همانطور که بیان شد، در محیط MATLAB دو نوع جمینگ شامل جمینگ موج پیوسته (CW) و جمینگ پالس مورد بررسی قرار گرفتند. نتایج نشان داد که فیلتر LMS به طور موثری توانست هر دو نوع جمینگ را حذف و سیگنال تمیز GPS را بازیابی کند. نمودارهای مربوط به نتایج شبیه‌سازی در شکل‌های (۲) تا (۷) آمده‌اند. در جدول (۲) نتایج مربوط به این تنظیمات آمده است.

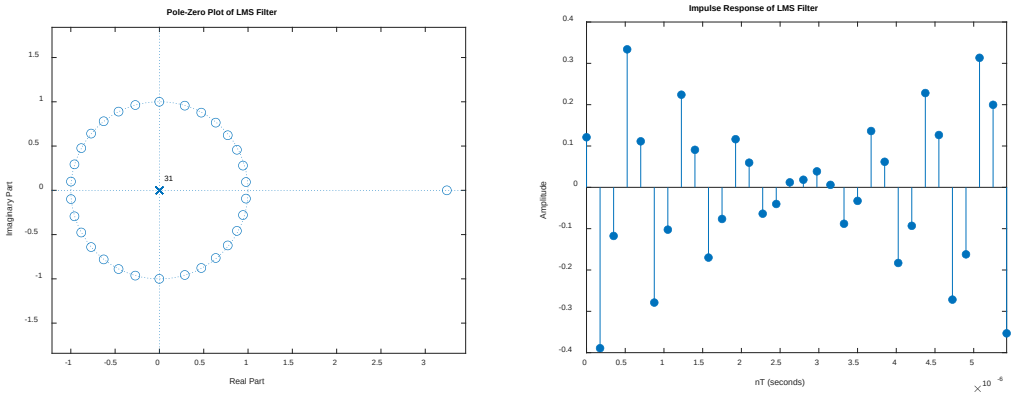
تأثیر داده‌های مختلف روی فیلتر وفقی LMS به چندین عامل مهم بستگی دارد که در ادامه به‌طور کامل بررسی می‌شوند:

۱. نوع سیگنال جمینگ (در اینجا پالس یا موج پیوسته)

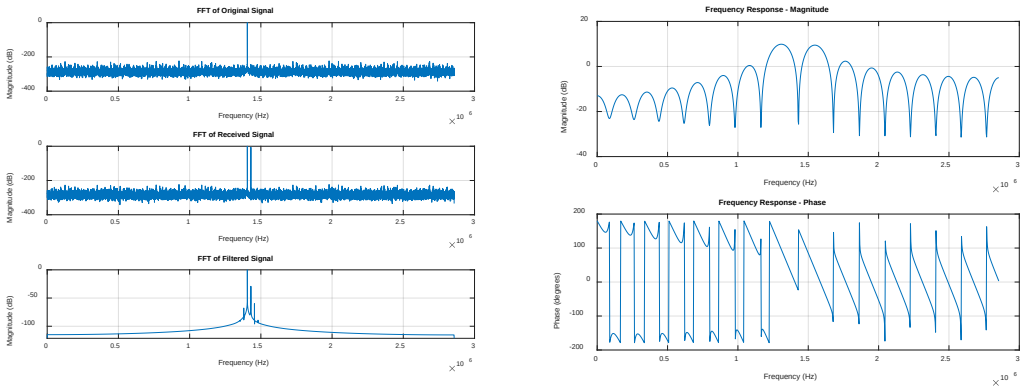
پالس: سیگنال جمینگ پالس شامل تغییرات سریع و ناگهانی در دامنه است. برای فیلترهای وفقی، این نوع سیگنال معمولاً سخت‌تر هستند، زیرا فیلتر باید به سرعت به تغییرات ناگهانی پاسخ دهد. اگر فیلتر نتواند به سرعت وفق پیدا کند، بهبود SNR نسبتاً کمتر خواهد بود.



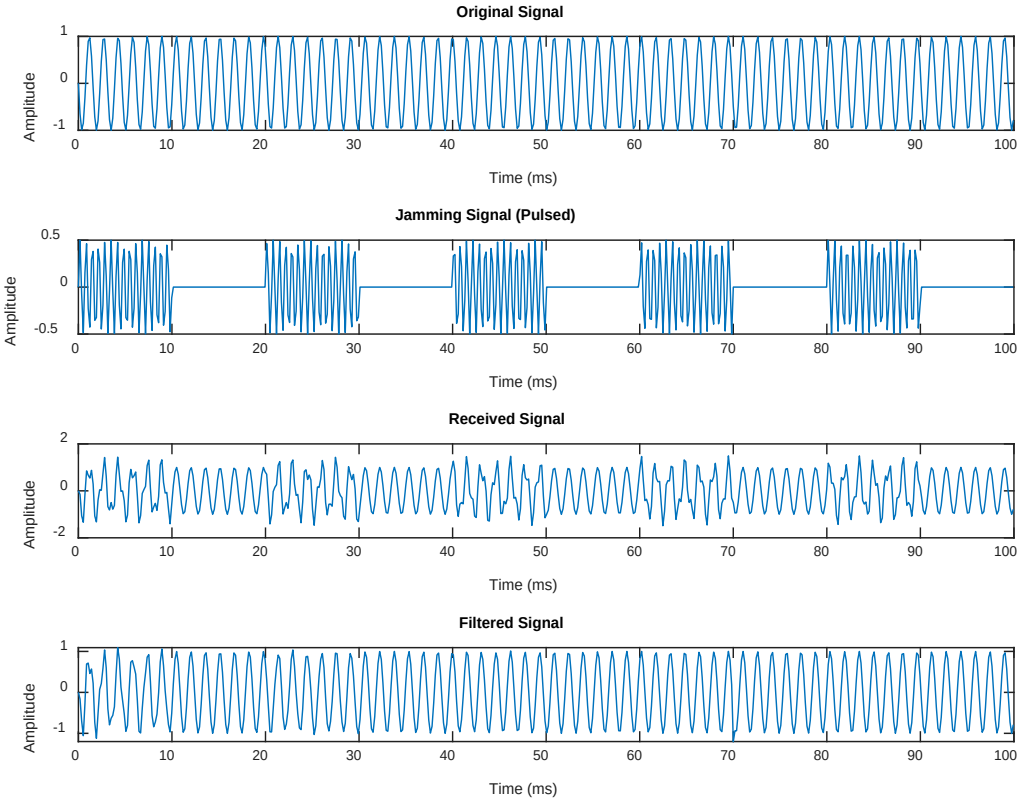
شکل (۲) نمودارها از بالا به پایین: سیگنال اصلی، سیگنال جمینگ، سیگنال ترکیبی و سیگنال فیلترشده درجمینگ CW با فیلتر وفقی LMS، با مرتبه فیلتر ۳۲ و Mu = 0.0001.



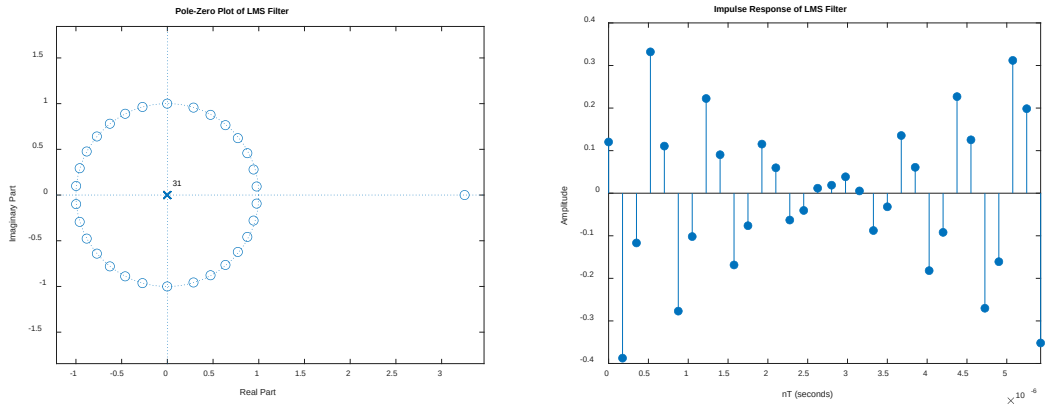
شکل (۳) نمودار سمت راست، پاسخ ضربه و نمودار سمت چپ، قطب-صفر در جمینگ CW با فیلتر وفقی LMS با مرتبه فیلتر ۳۲ و Mu = 0.0001.



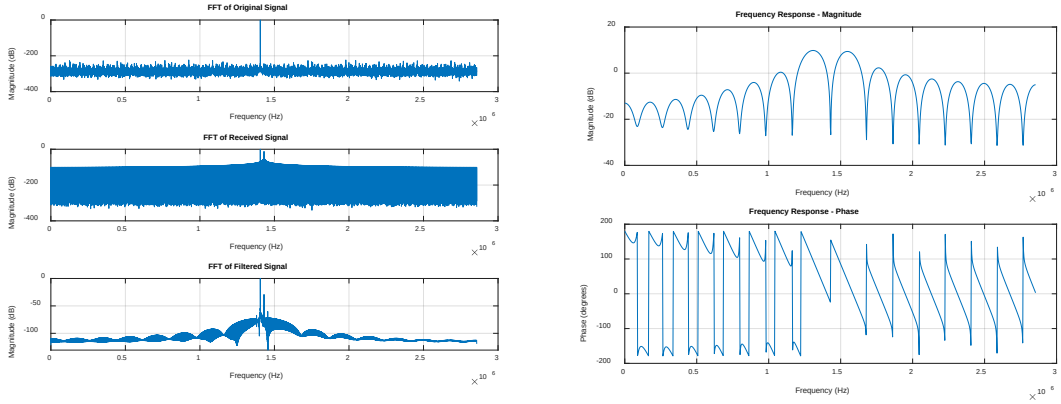
شکل (۴) نمودار سمت راست، اندازه و فاز پاسخ فرکانسی و نمودار سمت چپ، FFT در جمینگ CW با فیلتر وفقی LMS با مرتبه فیلتر ۳۲ و Mu = 0.0001.



شکل (۵) نمودارها از بالا به پایین: سیگنال اصلی، سیگنال جمینگ، سیگنال ترکیبی و سیگنال فیلترشده درجمینگ پالس با فیلتر وفقی LMS، با مرتبه فیلتر ۳۲ و Mu = 0.0001؛



شکل (۶) نمودار سمت راست، پاسخ ضربه و نمودار سمت چپ، قطب-صفر در جمینگ پالس با فیلتر وفقی LMS با مرتبه فیلتر ۳۲ و Mu = 0.0001.



شکل (۷) نمودار سمت راست، اندازه و فاز پاسخ فرکانسی و نمودار سمت چپ، FFT در جمینگ پالس با فیلتر وفقی LMS با مرتبه فیلتر ۳۲ و Mu = 0.0001.

جمینگ موج پیوسته (CW): سیگنال‌های جمینگ CW معمولاً تغییرات آرام و تدریجی دارند که فیلترهای LMS بهتر می‌توانند آن‌ها را مدیریت کنند. بنابراین، فیلترهای LMS معمولاً در حذف نویز از CWها عملکرد بهتری دارند و SNR بیشتری نسبت به فیلتر پالس حاصل می‌کنند.

۲. مقدار Mu

Mu کوچک (در اینجا ۰,۰۰۰۱): با مقدار کوچکMu ، فیلتر LMS به‌آرامی یاد می‌گیرد و تغییرات کمتری در وزن‌های فیلتر اتفاق می‌افتد. این باعث می‌شود فیلتر دقیق‌تر شود، اما مدت بیشتری طول می‌کشد تا به شرایط بهینه برسد. این مورد به‌ویژه برای سیگنال‌هایی که تغییرات کندتری دارند، مناسب است. اما اگر داده‌ها دارای تغییرات ناگهانی باشند، فیلتر با Mu کوچک عملکرد کندتری خواهد داشت و SNR کمتری ایجاد می‌کند.

Mu بزرگ (در اینجا ۰,۰۰۱): مقدار بزرگ Mu، باعث می‌شود فیلتر سریع‌تر به تغییرات پاسخ دهد. این مقدار برای فیلتر کردن سیگنال‌های با تغییرات ناگهانی مناسب‌تر است، اما ممکن است به بی‌ثباتی و نوسانات در فیلتر منجر شود. برای سیگنال‌های CW نیز Mu بزرگ می‌تواند SNR بسیار بیشتری تولید کند، ولی خطر ناپایداری وجود دارد.

۳. مرتبه فیلتر

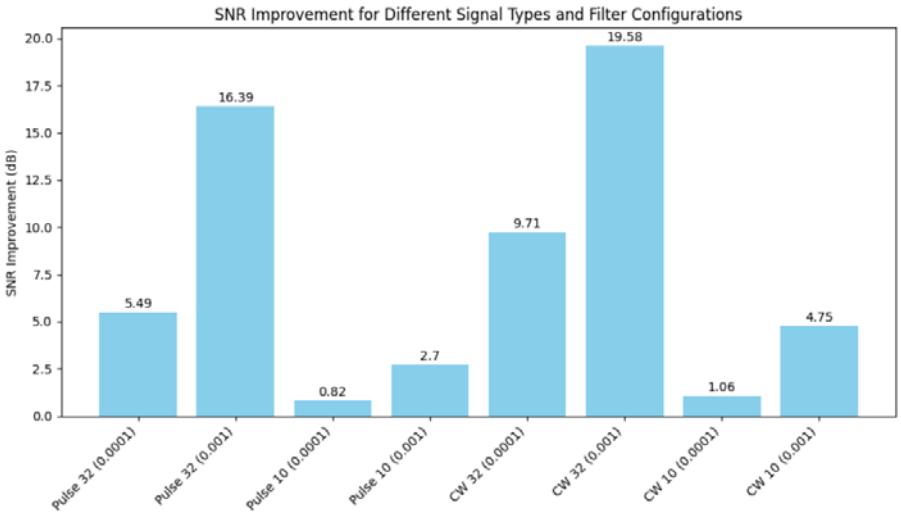
مرتبه بالاتر: فیلترهای با مرتبه بالاتر می‌توانند الگوهای پیچیده‌تری از سیگنال‌ها را تشخیص دهند و بهتر با تداخلات متنوع مقابله کنند. بنابراین، در سیگنال‌های پیچیده‌تر یا نویزهای بیشتر، فیلترهای با مرتبه بالاتر می‌توانند SNR بیشتری ایجاد کنند. اما با افزایش مرتبه، پیچیدگی محاسباتی و مصرف حافظه نیز بیشتر می‌شود که می‌تواند برای ریزپردازنده‌های کم‌قدرت چالش‌برانگیز باشد.

مرتبه پایین‌تر: فیلترهای با مرتبه پایین‌تر محاسبات سریع‌تری دارند و منابع کمتری استفاده می‌کنند، اما قدرت فیلتر کردن سیگنال‌های پیچیده را کاهش می‌دهند. در نتیجه، SNR کمتری به دست می‌آید.

در نهایت، تأثیر داده‌ها بر فیلتر LMS به تعادلی بین این پارامترها بستگی دارد. در جدول (۲) مقایسه‌ای از بررسی تنظیمات متفاوت این سه مورد آورده شد که در ادامه در اختیارتان قرار خواهد گرفت.

جدول (۲) مقایسه بهبود SNR به ازای جمینگ پالس و CW به همراه مشخصات فیلتر ارائه شده.

نوع جمینگ	مرتبه فیلتر	MU	SNR قبل از فیلتر (dB)	SNR بعد از فیلتر (dB)	JSR قبل از فیلتر (dB)	بهبود SNR (dB)
پالس	۳۲	۰,۰۰۰۱	۹,۰۳	۱۴,۵۲	-۹,۰۳	۵,۴۹
پالس	۳۲	۰,۰۰۱	۹,۰۳	۲۵,۴۲	-۹,۰۳	۱۶,۳۹
پالس	۱۰	۰,۰۰۰۱	۹,۰۳	۹,۸۵	-۹,۰۳	۰,۸۲
پالس	۱۰	۰,۰۰۱	۹,۰۳	۱۱,۷۳	-۹,۰۳	۲,۷۰
CW	۳۲	۰,۰۰۰۱	۶,۰۲	۱۵,۷۳	-۶,۰۲	۹,۷۱
CW	۳۲	۰,۰۰۱	۶,۰۲	۲۵,۶۰	-۶,۰۲	۱۹,۵۸
CW	۱۰	۰,۰۰۰۱	۶,۰۲	۷,۰۸	-۶,۰۲	۱,۰۶
CW	۱۰	۰,۰۰۱	۶,۰۲	۱۰,۷۷	-۶,۰۲	۴,۷۵



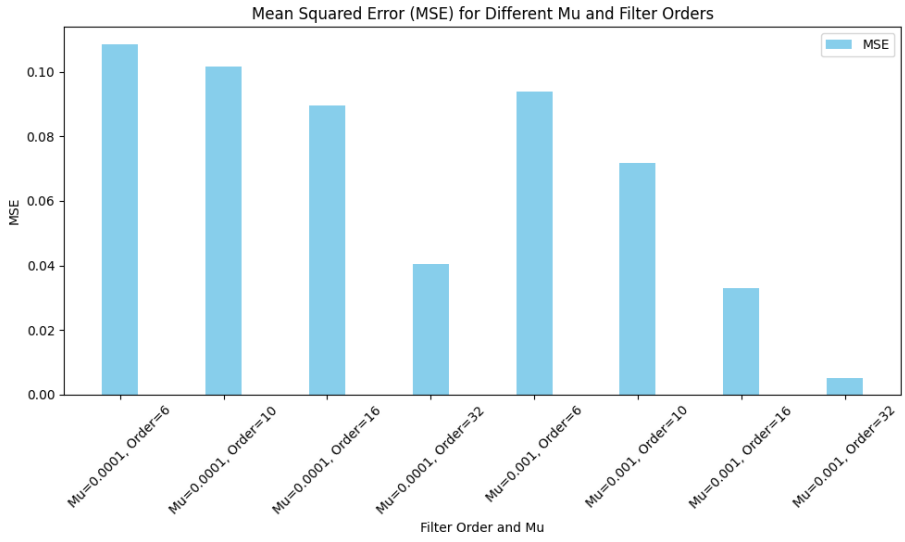
شکل (۸) تحلیل نموداری تاثیر پیکربندی فیلتر روی جمینگ پالس و CW.

همانطور که از شکل (۸) و جدول (۲) قابل استنباط است، اثرات مقادیر مختلف پارامتر μ و مرتبه فیلتر روی SNR، سیگنال‌های پالس و موج پیوسته بررسی شده‌اند. در جمینگ پالس با مرتبه ۳۲ و $\mu = 0.001$ بیشترین بهبود SNR (۱۶٫۳۹ دسی‌بل) را داریم که نشان می‌دهد مقدار μ بالاتر و مرتبه فیلتر بیشتر، اثرات بیشتری روی کاهش جمینگ دارد. مرتبه ۱۰ با $\mu = 0.0001$ کمترین بهبود SNR (۰٫۸۲ دسی‌بل) را داراست که نشان می‌دهد مقدار μ کمتر با مرتبه فیلتر کمتر تاثیر کمتری دارد. همین موضوع را در مورد جمینگ CW نیز، مشاهده می‌کنیم. در مرتبه ۳۲ با $\mu = 0.001$ بهبود SNR به مقدار ۱۹٫۵۸ دسی‌بل رسیده است که نشان‌دهنده تأثیر مثبت مقدار بالای μ و مرتبه بالای فیلتر می‌باشد. فیلتر با مرتبه ۱۰ و $\mu = 0.0001$ کمترین بهبود SNR (۱٫۰۶ دسی‌بل) را دارد. بنابراین، انتخاب مقدار μ و مرتبه فیلتر به شدت به نوع سیگنال و هدف بهینه‌سازی بستگی دارد. در عمل، مقدار Mu اغلب با آزمایش و خطا تعیین می‌شود. با توجه به داده‌ها و عملکرد مدنظر، ابتدا از یک مقدار متوسط شروع شده و سپس آن را تنظیم می‌کنیم تا بهترین عملکرد را داشته باشد. خطای بین سیگنال اصلی و سیگنال فیلترشده برای تمام آن‌ها محاسبه شده است. این مقدار نشان‌دهنده میزان دقت فیلتر LMS در بازسازی سیگنال اصلی است. هر چه این مقدار کمتر باشد، نشان‌دهنده عملکرد بهتر فیلتر است. جدول (۳) مقایسه‌ای بین این اعداد و رابطه‌ی آن‌ها با مرتبه و نرخ یادگیری فیلتر است.

همانطور که از جدول (۳) و شکل (۹) مشاهده می‌شود، فیلترهای با مرتبه بالاتر (مانند ۳۲) نسبت به فیلترهای با مرتبه کمتر (مانند ۶ یا ۱۰) عملکرد بهتری دارند. با افزایش مرتبه فیلتر، دقت فیلتر افزایش می‌یابد و خطای میانگین مربعات کمتر می‌شود. این نشان می‌دهد که فیلترهای پیچیده‌تر توانایی بهتری در مدل‌سازی جمینگ و کاهش آن دارند. با این حال، نرخ یادگیری پایین‌تر (مثل ۰٫۰۰۰۱) عملکرد ضعیف‌تری نسبت به نرخ یادگیری بالاتر (مثل ۰٫۰۰۱) دارد. این نشان می‌دهد که سرعت تنظیم وزن‌های فیلتر در نرخ‌های یادگیری پایین‌تر کندتر است و سامانه دیرتر به خطای کمینه می‌رسد. از طرفی، نرخ یادگیری بالا (۰٫۰۰۱) به دلیل سرعت تنظیم بهتر، به نتایج دقیق‌تری منجر می‌شود. ترکیب مرتبه فیلتر بالا (۳۲) و نرخ یادگیری بالا (۰٫۰۰۱) بهترین نتایج را با کمترین خطای میانگین مربعی ارائه داده است (MSE=0.005013)، درحالی‌که ترکیب مرتبه فیلتر پایین (مرتبه ۶) و نرخ یادگیری پایین فیلتر (۰٫۰۰۰۱) بالاترین خطای میانگین مربعی را نشان می‌دهد (MSE=0.108427). این نتایج نشان‌دهنده آن است که برای کاهش جمینگ و افزایش کیفیت فیلتر، باید بین مرتبه فیلتر و نرخ یادگیری تعادلی مناسب برقرار کرد.

جدول (۳) مقایسه بین میزان MSE در فیلتر با Mu و مرتبه متفاوت.

مرتبه فیلتر	Mu	MSE
۳۲	۰,۰۰۱	۰,۰۰۵۰۱۳
۳۲	۰,۰۰۰۱	۰,۰۴۰۴۱۳
۱۶	۰,۰۰۱	۰,۰۳۳۰۸
۱۶	۰,۰۰۰۱	۰,۰۸۹۴۹۱
۱۰	۰,۰۰۱	۰,۰۷۱۷۰۸
۱۰	۰,۰۰۰۱	۰,۱۰۱۷۲۲
۶	۰,۰۰۱	۰,۰۹۳۷۲۴
۶	۰,۰۰۰۱	۰,۱۰۸۴۲۷



شکل (۹) نمودار میله‌ای نشان‌دهنده MSE در فیلتر وفقی به ازای مرتبه و Mu متفاوت.

۵. نتیجه‌گیری

در این مقاله، یک روش مبتنی بر فیلتر وفقی LMS برای مقابله با جمینگ GPS ارائه شد. نتایج شبیه‌سازی نشان دادند که فیلتر LMS توانست SNR سیگنال GPS را به میزان حداقل ۱۶٫۳۹ دسی‌بل بهبود بخشد و MSE را تا نزدیک به ۶۰ درصد کاهش دهد که یعنی فیلتر LMS می‌تواند تقریبا به‌طور موثر جمینگ را در موقعیت‌های مختلف کاهش دهد و یکپارچگی سیگنال GPS را حفظ کند. پس از اعتبارسنجی الگوریتم فیلتر در محیط MATLAB، سپس بر روی ریزپردازنده برای آزمون عملکرد پیاده‌سازی آماده شدیم. این روش می‌تواند در سامانه‌های ناوبری و کاربردهای امنیتی دیگر مورد استفاده قرار گیرد.

۶. مراجع

[۱] سید محمدرضا موسوی میرکلائی، "پردازش داده‌ها در گیرنده‌های تک فرکانسه GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۸۹.

[۲] سید محمدرضا موسوی میرکلائی، مریم معاضدی، محمدجواد رضایی و امیر طباطبایی،" مقابله با اختلال در گیرنده‌های GPS"، انتشارات دانشگاه علم و صنعت ایران، ۱۳۹۴.

[3] A. Purwar, D. Joshi, and V. K. Chaubey, “GPS Signal Jamming and Anti-jamming Strategy — A Theoretical Analysis,” IEEE Annual India Conference (INDICON), Dec. 2016.

[4] P. Teunissen and O. Montenbruck, Springer Handbook of Global Navigation Satellite Systems, Cham, Switzerland: Springer, 2017.

[5] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, “A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach”, Springer Science & Business Media, 2007.

[6] A. J. Van Dierendonck, "Global Positioning System: Theory and Applications," Progress in Astronautics and Aeronautics, 1996.

[7] D. Borio, "A Multi-State Notch Filter for GNSS Jamming Mitigation," IEEE Conference on Localization and GNSS, pp. 1-6, 2014.

[8] Y. R. Chien, "Design of GPS Anti-Jamming Systems using Adaptive Notch Filters," IEEE Systems Journal, vol. 9, no. 2, pp. 451-460, 2015.

[9] T. Yousif and P. Blunt, "Interference Mitigation for GNSS Receivers using FFT Excision Filtering Implemented on an FPGA," Eng Journal, vol. 3, no. 4, pp. 439-466, 2022.

[10] E. Elezi, G. Çankaya, A. Boyacı and S. Yarkan, "A Detection and Identification Method Based on Signal Power for Different Types of Electronic Jamming Attacks on GPS Signals," IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1-5, 2019.

[11] D. Borio and C. Gioia, "Interference Mitigation: Impact on GNSS Timing," GPS Solutions, vol. 25, pp. 1-18, 2021.

[12] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, ‘‘GPS Vulnerability to Spoofing Threats and Overview of Anti-Spoofing Techniques”, International Journal of Navigation and Observation, pp. 1-16, 2012.

[13] D. Borio, C. O'Driscoll, and J. Fortuny, “GNSS Jammers: Effects and Countermeasures”, IEEE Workshop on Satellite Navigation Technologies (Navitech) & European Workshop on GNSS Signals and Signal Processing, pp. 1-7, 2012.
[14] J. Song, Z. Lu, Z. Xiao, B. Li, and G. Sun, "Optimal Order of Time-Domain Adaptive Filter for Anti-Jamming Navigation Receiver," Sensors, vol. 14, no. 1, pp. 1-15, 2022.
[15] K. Radoš, M. Brki´c, and D. Beguši´c, "Recent Advances on Jamming and Spoofing Detection in GNSS," Sensors, vol. 24, pp. 1-28, 2024.
[16] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen, and Q. Fu, "GNSS Spoofing Jamming Detection Based on Generative Adversarial Network," IEEE Sensors Journal, vol. 21, no. 20, pp. 22823-22832, 2021.
[17] X. Li, L. Chen, Z. Lu, F. Wang, W. Liu, W. Xiao, and P. Liu, "Overview of Jamming Technology for Satellite Navigation," Machines, vol. 11, no. 7, pp. 1-29, 2023.
[18] V. Tiwari, A. Agrawal, M. Sharma, P. Chaturvedi, T. Katiyar, and I. Maheshwari, "Mitigation of Jamming and Spoofing Attack on GNSS Signals using Subspace Projection," IEEE Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET), pp. 1-6, 2023.
[19] D. Borio and C. Gioia, "GNSS Interference Mitigation: A Measurement and Position Domain Assessment," NAVIGATION: Journal of the Institute of Navigation, vol. 68, no. 1, pp. 93-114, 2021.

نهمین کنفرانس بین‌المللی
ترکیبیات، رمزنگاری، علوم کامپیوتر و محاسبات
۵ و ۶ دی ۱۴۰۳

ایده‌آل‌های Q-نرم توسیع‌یافته در نیم‌گروه‌ها

امیر شمالی[۱]
دانشگاه آزاد اسلامی، واحد سنندج، سنندج، ایران

رسول رسولی
دانشگاه پیام نور، تهران، ایران

چکیده

در این مقاله ایده‌آل‌های Q-نرم و ایده‌آل‌های (اول کامل یافته و نیم اول کامل یافته) Q-نرم و همچنین توسیع آنها از نیم‌گروه‌ها را تعریف می‌کنیم و خصوصیات اصلی آن را بیان و اثبات می‌کنیم و ارتباط آنها را با ایده‌ال‌های نیم‌گروه‌ها نشان می‌دهیم.

واژه‌های کلیدی: ایده‌آل‌های Q-نرم، ایده‌آل‌های اول کامل یافته Q-نرم ،مجموعهٔ Q- نرم
[2010]: 20K27, 06B10, 11R44, 12F05

۱ مقدمه

مبحث ایده‌آل‌های Q-نرم را اولین بار مالودسوف در مقاله [۱] بیان کرد و آکتاس و سگمن ساختار جبری از مجموعه‌های نرم را مورد مطالعه قرار دادند[۲]. همچنین نویسندگان این مقاله قبلا ساختارهای اساسی و اصلی زیرگروه‌های Q-نرم را دنبال کرده و نتایج مهمی را به‌دست آورده‌اند [۳،۴،۵،۶]. در این مقاله ساختارهای Q-نرم روی نیم‌گروه‌ها را بررسی می‌کنیم. ابتدا ایده‌آل‌های Q-نرم، ایده‌آل‌های اول کامل یافته Q-نرم و ایده‌آل‌های نیم‌اول کامل یافته Q-نرم را تعریف، سپس نتایج آنها را به‌دست آورده و در مورد توسیع آنها بحث می‌کنیم.

۲ پیش‌نیازها

در این بخش تعاریف مقدماتی که در این مقاله مورد نیاز است را بیان می‌کنیم. برای جزئیات بیشتر به مراجع [۱،۲،۳،۴،۵،۶] مراجعه کنید.

تعریف ۱.۲. فرض کنید I یک زیرمجموعه غیر تهی از نیم‌گروه S باشد، دراین‌صورت اگر $SI \subseteq I$ آنگاه می‌گوییم I یک ایده‌آل چپ و اگر $IS \subseteq I$ آنگاه می‌گوییم I یک ایده‌آل راست از S است. اگر I هم ایده‌آل راست و هم ایده‌آل چپ از S باشد آنگاه I را یک ایدآل دو طرفه یا ایده‌آل از S می‌نامیم.

تعریف ۲.۲. فرض کنید I یک ایده‌آل غیر تهی از نیم‌گروه S و $x, y \in S$ باشد، گوئیم I یک ایده‌آل اول کامل یافته از S است اگر $xy \in I$ ایجاب کند $x \in I$ یا $y \in I$. ایده‌آل I یک ایده‌آل نیم‌اول کامل یافته از S است اگر $x^2 \in I$ ایجاب کند $x \in I$.

تعریف ۳.۲. فرض کنید U یک مجموعهٔ جهانی آغازین و Q یک مجموعهٔ غیر تهی دلخواه باشد. همچنین فرض کنید A نیز یک مجموعهٔ غیر تهی دلخواه باشد، در این‌صورت نگاشت $\mu : A \times Q \longrightarrow P(U)$ را یک مجموعهٔ Q- نرم می‌گوئیم به‌طوری‌که اگر $x \notin A$، $\mu(x, q) = \emptyset$. همچنین می‌توان μ را به‌صورت زیر هم نشان داد:

$$\mu = \{((x, q), \mu(x, q)) \mid (x, q) \in A \times Q, \mu(x, q) \in P(U)\}.$$

[۱] سخنران

تعریف ۴.۲. فرض کنید μ و ν دو زیر مجموعهٔ Q- نرم A باشند، در این‌صورت
الف: μ را تهی گوئیم هرگاه به‌ازای هر $(x,q) \in A \times Q$، $\mu(x,q) = \emptyset$،
ب: μ را جهانی گوئیم هرگاه به‌ازای هر $(x,q) \in A \times Q$، $\mu(x,q) = U$،
ج: تصویر زیرمجموعهٔ μ را به‌صورت زیر تعریف می‌کنیم:

$$Im(\mu) = \{\mu(x,q) \mid (x,q) \in A \times Q\}.$$

د: μ را زیر مجموعهٔ ν گوئیم هرگاه به‌ازای هر $(x,q) \in A \times Q$، $\mu(x,q) \subseteq \nu(x,q)$، و آن را با نماد $\mu \subseteq \nu$ نشان می‌دهیم.
ه: گوئیم $\mu = \nu$ هرگاه به‌ازای هر $(x,q) \in A \times Q$، $\mu(x,q) = \nu(x,q)$،
و: اجتماع μ و ν را با نماد $\mu \cup \nu$ نشان می‌دهیم و به‌ازای هر $(x,q) \in A \times Q$ به‌صورت زیر تعریف می‌شود:

$$(\mu \cup \nu)(x,q) = \mu(x,q) \cup \nu(x,q),$$

ز: اشتراک μ و ν را با نماد $\mu \cap \nu$ نشان می‌دهیم و به‌ازای هر $(x,q) \in A \times Q$ به‌صورت زیر تعریف می‌شود:

$$(\mu \cap \nu)(x,q) = \mu(x,q) \cap \nu(x,q).$$

۳ نتایج اصلی

تعریف ۱.۳. فرض کنید μ یک زیرمجموعه Q-نرم از نیم‌گروه S، $x,y \in S$ و $q \in Q$ باشد، دراین‌صورت اگر $\mu(xy,q) \supseteq \mu(y,q)$ آنگاه می‌گوییم μ یک ایده‌آل چپ Q-نرم و اگر $\mu(xy,q) \supseteq \mu(x,q)$ آنگاه می‌گوییم μ یک ایده‌آل راست Q-نرم از S است. اگر μ هم ایده‌آل راست و هم ایده‌آل چپ Q-نرم از S باشد آنگاه μ را یک ایدآل دو طرفه یا ایده‌آل Q-نرم از S می‌نامیم.

تعریف ۲.۳. فرض کنید μ یک زیرمجموعه Q-نرم از نیم‌گروه S، $x,y \in S$ و $q \in Q$ باشد، در این‌صورت ایده‌آل μ را یک ایده‌آل اول کامل یافتهٔ Q-نرم از S گوئیم هرگاه

$$\mu(xy,q) = \mu(x,q) \cup \mu(y,q).$$

همچنین ایده‌آل μ را یک ایده‌آل نیم اول کامل یافتهٔ Q-نرم از S گوئیم هرگاه

$$\mu(x,q) = \mu(x^2,q).$$

قضیه زیر ارتباط بین ایده‌آل‌های نیم‌گروه S و ایده‌آل‌های Q-نرم از S را نشان می‌دهد.

قضیه ۳.۳. فرض کنید $\emptyset \neq I \subseteq S$ یک زیر مجموعهٔ دلخواه باشد و $\varphi : S \times Q \longrightarrow P(U)$ یک نگاشت با تعریف زیر باشد:

$$\varphi(x,q) = \begin{cases} U & \text{if } x \in I \\ \emptyset & \text{otherwise.} \end{cases}$$

در این‌صورت اگر I یک ایده‌آل یا ایده‌آل اول تکامل یافته یا ایده‌آل نیم اول تکامل یافته از S باشد آنگاه φ نیز یک ایده‌آل Q-نرم یا ایده‌آل اول تکامل یافته Q-نرم یا ایده‌آل نیم اول تکامل یافته Q-نرم از S می‌باشد.

قضیه ۴.۳. فرض کنید μ یک زیرمجموعه Q-نرم از نیم‌گروه S باشد به‌طوری‌که $x,y \in S$، $q \in Q$ و $\alpha \in Im\mu$. قرار می‌دهیم

$$\mu_\alpha = \{x \in S \mid \mu(x,q) \geq \alpha\},$$

در این‌صورت اگر μ_α یک ایده‌آل یا ایده‌آل اول تکامل یافته یا ایده‌آل نیم اول تکامل یافته از S باشد آنگاه μ نیز یک ایده‌آل Q-نرم یا ایده‌آل اول تکامل یافته Q-نرم یا ایده‌آل نیم اول تکامل یافته Q-نرم از S می‌باشد.

تعریف ۵.۳. فرض کنید μ یک زیرمجموعه Q-نرم از نیم‌گروه S و $x \in S$ باشد. نگاشت $\langle x,\mu\rangle : S \times Q \longrightarrow P(U)$ را به‌صورت $\langle x,\mu\rangle(y,q) = \mu(xy,q)$ تعریف می‌کنیم که در آن $y \in S$ و $q \in Q$. در این‌صورت $\langle x,\mu\rangle$ را توسیع μ توسط x می گوئیم.

قضیه ۶.۳. فرض کنید S یک نیم‌گروه تعویض‌پذیر و $x \in S$ باشد. در این‌صورت اگر μ یک ایده‌آل Q-نرم از S باشد آنگاه $\langle x, \mu\rangle$ نیز یک ایده‌آل Q-نرم از S است.

قضیه ۷.۳. فرض کنید μ یک ایده‌آل Q-نرم از نیم‌گروه S و $x \in S$ باشد. در این‌صورت موارد زیر برقرار است:
الف: $\mu \supseteq \langle x, \mu\rangle$،
ب: به‌ازای هر عدد طبیعی n، $\langle x^{n+1}, \mu\rangle \supseteq \langle x^n, \mu\rangle$،
ج: اگر $\mu(x, q)$ غیر تهی باشد در این‌صورت $\langle x, \mu\rangle = S \times Q$.

تعریف ۸.۳. فرض کنید S یک نیم‌گروه و $A \subseteq S$ یک زیرمجموعهٔ غیر تهی دلخواه و $x \in S$ باشد. در این‌صورت $\langle x, A \times Q\rangle$ را به‌صورت زیر تعریف می‌کنیم:

$$\langle x, A \times Q\rangle = \{(y, q) \in S \times Q \mid (xy, q) \in A \times Q\}$$

قضیه ۹.۳. فرض کنید S یک نیم‌گروه تعویض‌پذیر و $x \in S$ باشد. در این‌صورت اگر μ یک ایده‌آل اول کامل یافتهٔ Q-نرم از S باشد آنگاه $\langle x, \mu\rangle$ نیز یک ایده‌آل اول کامل یافتهٔ Q-نرم از S است و به‌خصوص $\langle x, \mu\rangle = \langle x^2, \mu\rangle$.

قضیه ۱۰.۳. فرض کنید S یک نیم‌گروه تعویض‌پذیر و $x \in S$ باشد. در این‌صورت اگر μ یک زیرمجموعهٔ Q-نرم از S باشد به‌طوری‌که $\langle x, \mu\rangle = \mu$ آنگاه μ یک تابع ثابت است.

قضیه ۱۱.۳. فرض کنید S یک نیم‌گروه تعویض‌پذیر و $x \in S$ باشد. در این‌صورت اگر μ یک ایده‌آل نیم‌اول کامل یافتهٔ Q-نرم از S باشد آنگاه $\langle x, \mu\rangle$ نیز یک ایده‌آل نیم‌اول کامل یافتهٔ Q-نرم از S است.

نتیجه ۱۲.۳. فرض کنید S یک نیم‌گروه تعویض‌پذیر و $x \in S$ باشد. در این‌صورت اگر μ_i یک ایده‌آل نیم‌اول کامل یافتهٔ Q-نرم از S باشد آنگاه $\langle x, \bigcap_{i\in I} \mu_i\rangle$ نیز یک ایده‌آل نیم‌اول کامل یافتهٔ Q-نرم از S است.

مراجع

[1] H. Aktas and N. Cagman, *Soft sets and soft groups*, Inform. Sci. 177(2007), 2726-2735.

[2] D. A. Molodtsov, *Soft set theory-First results*, Computers and Mathematics With Applications, 37 (4) (1999), 19-31.

[3] R. Rasuli, *Q-Soft Normal Subgroups*, Journal of New Theory, 26 (2019), 13-22.

[4] R. Rasuli, *Anti Q-Soft Normal Subgroups*,The Jounal of Fuzzy Mathematicse Los Angles America, 28(1) (2020), 237-248.

[5] R. Rasuli, *Q-soft coset, characteistic Q-soft and Q-level subsets of Q-soft subgroups*, International Congerence on combinatorics, Crytography, Computer Science and computing held by Iran University of Science and Technology, Iran,Tehran, during November 16-17,2022.

[6] R. Rasuli and A. Shomali, *Algebraic Structures of Q-soft and anti Q-soft normal subgroups*, 11^{th} National Mathematics Conference of Payame Noor University, 16-17 October, Yazd, Iran.

پست الکترونیکی: rasulirasul@yahoo.com
پست الکترونیکی: shomali.math@gmail.com

مساله برنامه‌ریزی دو سطحی خطی با پارامترهای خاکستری

فرید پورافقی *
۱- استادیار گروه ریاضی، دانشگاه پیام نور، گروه ریاضی، تهران، ایران

چکیده

برنامه‌ریزی دو سطحی یکی از مسایل پرکاربرد می‌باشدکه در آن دو تصمیم‌گیرنده در یک ساختار سلسله مراتبی بترتیب تصمیم می‌گیرند. از جمله کاربردهای آن در ترافیک، حمل و نقل و اقتصاد می‌باشد که از اهمیت خاصی برخوردار است. بیشتر مسائل برنامه‌ریزی دوسطحی در محیط‌های قطعی با پارامترهای ثابت مورد مطالعه قرار گرفته است و روش‌های رایج برای حل آنها تبدیل مساله برنامه‌ریزی دوسطحی به یک مساله برنامه‌ریزی تک سطحی می‌باشد. در این مقاله، مساله برنامه‌ریزی دو سطحی خطی در محیط عدم قطعیت با پارامترهای خاکستری مورد بررسی قرار می‌گیرد. و یک روش برای حل آن ارائه می‌شود. برای اثبات کارایی روش ارائه شده یک مثال عددی حل شده است.

کلمات کلیدی: مساله برنامه‌ریزی دوسطحی، برنامه‌ریزی دو سطحی خطی خاکستری، روش شمارش ضمنی

۱. مقدمه

مساله برنامه‌ریزی خطی دو سطحی، یک سیستم تصمیم نامتمرکز و غیر مشارکتی با ساختار سلسله مراتبی می‌باشد. در این مسائل، تصمیم‌گیرنده سطح یک را رهبر و سطح دو را پیرو می‌گوییم، هر تصمیم‌گیرنده تلاش می‌کند تابع هدف خود را بدون در نظر گرفتن تابع هدف سطح دیگر بهینه کند. اما تصمیم هر سطح بر مقدار تابع هدف و فضای تصمیم‌گیری سطح دیگر اثر می‌گذارد[۱]. بدلیل کاربردهای زیاد آن در عمل روش‌های متعددی برای حل آن ارائه شده است [۲]. اغلب بدلیل وجود اطلاعات ناقص و نادقیق در مورد مسائل زندگی روزمره واقعی، تصمیم‌گیری‌ها همواره در یک بستر دقیق انجام نمی‌شود. در چنین مسائلی می‌توان برای بیان ضرایب نادقیق از نظریه‌های عدم قطعیت مانند، نظریه خاکستری استفاده کرد. نظریه خاکستری یکی از نظریه‌های مقابله با عدم قطعیت است که شامل موضوعاتی می‌شود که دامنه مشخص و ماهیت نامشخص دارند. این نظریه اولین بار توسط پروفسور دنگ، در سال ۱۹۸۲ معرفی شد [۳]. با توجه به مزیت‌های این نظریه نسبت به سایر روش‌های مقابله با سیستم‌های دارای عدم قطعیت، کاربرد آن در سال های اخیر در حال گسترش است[۴و۵]. در این مقاله، حالت خاصی از یک مساله برنامه ریزی خطی دو تراز در نظر گرفته شده است که ضرایب توابع هدف آن اعداد خاکستری می‌باشند. برای حل این مساله از روش ضمنی و تبدیل مساله به یک مساله تک سطحی استفاده شده است.

* **Corresponding author:** فرید پورافقی، استادیار گروه ریاضی، دانشگاه پیام نور، گروه ریاضی، تهران، ایران
Email: f_pourofoghi@pnu.ac.ir

۲. سیستم خاکستری [۴]

این نظریه، روشی جدید برای مطالعه مسائلی است که به دلیل داده‌های اندک و اطلاعات محدود، عدم دقت بالایی دارند. عدد خاکستری بازه‌ای عددی است که کران بالا و پایین آن مشخص است. اما مکان آن بین کران بالا و پایین نامشخص است. $\otimes x \in [\underline{x}, \bar{x}]$

تعریف۱: برای عدد خاکستری $\otimes x \in [\underline{x}, \bar{x}]$:

۱. مرکز آن را با نماد $\otimes x_c$ نشان داده و به صورت زیر تعریف می‌شود:

$$\otimes x_c = \frac{\underline{x} + \bar{x}}{2}$$

۲. طول عدد خاکستری $\otimes x \in [\underline{x}, \bar{x}]$ را با نماد $\ell(\otimes x)$ نمایش داده و به صورت زیر تعریف می‌کنیم.

$$\ell(\otimes x) = |\bar{x} - \underline{x}|$$

۳. درجه عدد خاکستری $\otimes x \in [\underline{x}, \bar{x}]$ را با نماد $g^\circ(\otimes x)$ نمایش داده و به صورت زیر تعریف می‌کنیم.

$$g^\circ(\otimes x) = \frac{\ell(\otimes x)}{\otimes x_c}\ ,\ \otimes x_c \neq 0$$

تعریف۲: فرض کنید $\otimes x_1 \in [\underline{x}_1, \bar{x}_1]$ و $\otimes x_2 \in [\underline{x}_2, \bar{x}_2]$دو عدد خاکستری باشند. می‌توان مفاهیم مربوط به روابط بین اعداد خاکستری را برای اعداد خاکستری بازه‌ای به‌صورت زیر بیان نمود:

$$\otimes x_1 + \otimes x_2 = [\underline{x}_1 + \underline{x}_2, \bar{x}_1 + \bar{x}_2]$$

$$\otimes x_1 - \otimes x_2 = \otimes x_1 + (-\otimes x_2) = [\underline{x}_1 - \bar{x}_2, \bar{x}_1 - \underline{x}_2]$$

$$\otimes x_1 \times \otimes x_2 = \left[\min\{\underline{x}_1\underline{x}_2, \bar{x}_1\bar{x}_2, \bar{x}_1\underline{x}_2, \underline{x}_1\bar{x}_2\}, \max\{\underline{x}_1\underline{x}_2, \bar{x}_1\bar{x}_2, \bar{x}_1\underline{x}_2, \underline{x}_1\bar{x}_2\}\right]$$

$$\frac{\otimes x_1}{\otimes x_2} = \otimes x_1 \times \otimes x_2^{-1} = \left[\min\left\{\frac{\underline{x}_1}{\underline{x}_2}, \frac{\underline{x}_1}{\bar{x}_2}, \frac{\bar{x}_1}{\underline{x}_2}, \frac{\bar{x}_1}{\bar{x}_2}\right\}, \max\left\{\frac{\underline{x}_1}{\underline{x}_2}, \frac{\underline{x}_1}{\bar{x}_2}, \frac{\bar{x}_1}{\underline{x}_2}, \frac{\bar{x}_1}{\bar{x}_2}\right\}\right] \qquad 0 \notin [\underline{x}_2, \bar{x}_2]$$

$$k.\otimes x \in \begin{cases} [k\underline{x}, k\bar{x}] & k > 0 \\ [k\bar{x}, k\underline{x}] & k < 0 \end{cases}$$

تعریف۳: برای مقایسه دو عدد خاکستری $\otimes x_1 \in [\underline{x}_1, \bar{x}_1]$ و $\otimes x_2 \in [\underline{x}_2, \bar{x}_2]$ به صورت زیر عمل می‌کنیم:

i) $\otimes \hat{x}_1 < \otimes \hat{x}_2 \Rightarrow \otimes x_1 <_G \otimes x_2$

ii) $\otimes \hat{x}_1 = \otimes \hat{x}_2 \Rightarrow \begin{cases} g^\circ(\otimes x_1) = g^\circ(\otimes x_2) \Rightarrow \otimes x_1 =_G \otimes x_2 \\ g^\circ(\otimes x_1) < g^\circ(\otimes x_2) \Rightarrow \otimes x_1 >_G \otimes x_2 \\ g^\circ(\otimes x_1) > g^\circ(\otimes x_2) \Rightarrow \otimes x_1 <_G \otimes x_2 \end{cases}$

۳. مدل برنامه‌ریزی خطی دو تراز

مدل‌های برنامه‌ریزی خطی و غیر خطی دو تراز مختلفی وجود دارد که در این مقاله مدل زیر را به عنوان مدل برنامه‌ریزی خطی دو تراز معرفی می‌کنیم[۱].

$$\begin{aligned} &\min_{x} F_1(x,y) = a^T x + b^T y \\ &\min_{y} F_2(x,y) = c^T x + d^T y \\ &s.t \quad Ax + By \le r \\ &\qquad x, y \ge 0 \end{aligned} \tag{۱}$$

به طوریکه:

$$a,c,x \in R^{n_1} \ , \ b,d,y \in R^{n_2} \ , \ A \in R^{m \times n_1} \ , \ B \in R^{m \times n_2} \ , \ y \in R^{n_2} \tag{۲}$$

تعریف۴: مجموعه محدودیت‌ها

$$S = \{(x,y) | Ax + By \le r \ , x, y \ge 0\}$$

تعریف۵: تصویر S بر فضای سطح اول

$$S(x) = \{y | By \le r - Ax \ , x, y \ge 0\}$$

تعریف۶: مجموعه شدنی مساله

$$T = \{(x,y) \in S \ , \ y = y(x)\}$$

که $y(x)$ جواب بهینه مساله سطح دوم به ازای مقدار ثابت x است و $(x,y) \in T$ را یک نقطه شدنی می‌گوییم.

تعریف۷: (x^*, y^*) جواب بهینه مساله است هرگاه داشته باشیم:

$$F_1(x^*, y^*) \le F_1(x,y) \qquad \forall (x,y) \in T$$

۴. مدل برنامه‌ریزی خطی دو تراز خاکستری

مدل‌های برنامه‌ریزی خطی دو تراز خاکستری یک مساله خطی دو تراز در محیط عدم قطعیت می‌باشد که فرم کلی آن به صورت زیر می‌باشد.

$$\min_{x} \otimes F_1(x,y) =_G \otimes\left[\underline{a},\bar{a}\right]x + \otimes\left[\underline{b},\bar{b}\right]y$$
$$\min_{y} \otimes F_2(x,y) =_G \otimes\left[\underline{c},\bar{c}\right]x + \otimes\left[\underline{d},\bar{d}\right]y \qquad (۳)$$
$$s.t \quad Ax + By \le r$$
$$x, y \ge 0$$

که در آن $\underline{a},\bar{a}$ و $\underline{b},\bar{b}$ و $\underline{c},\bar{c}$ و $\underline{d},\bar{d}$ اعداد حقیقی مثبت و $A \in R^{m\times n_1}$, $B \in R^{m\times n_2}$ می‌باشند.

تعریف۸: (x,y) جواب موجه مساله برنامه‌ریزی خطی دو ترازه خاکستری می‌باشد هرگاه در معادلات بالا صدق کند.

تعریف۹: $\left(x^*,y^*\right)$ جواب بهینه مساله است هرگاه داشته باشیم:

$$\otimes F_1(x^*,y^*) \le_G \otimes F_1(x,y) \qquad \forall (x,y)$$

۵. روش شمارش ضمنی

قرار می‌دهیم

$$\otimes Z =_G \otimes\left[\underline{c},\bar{c}\right]x + \otimes\left[\underline{d},\bar{d}\right]y$$

چون در مساله سطح دوم x مقدار ثابت در نظر گرفته شده و توسط سطح اول تعیین می‌گردد. بنابراین تنها متغییر سطح دوم y است در این صورت داریم: $y = \frac{1}{\otimes\left[\underline{d},\bar{d}\right]}\left(\otimes Z - \otimes\left[\underline{c},\bar{c}\right]x\right)$

با جایگذاری رابطه بدست آمده در مساله (3)، مساله برنامه‌ریزی دو سطحی تبدیل به مساله یک سطحی زیر می‌شود

$$\min_{x} \otimes F_1(x,y) =_G \otimes\left[\underline{a},\bar{a}\right]x + \frac{\otimes\left[\underline{b},\bar{b}\right]}{\otimes\left[\underline{d},\bar{d}\right]}\left(\otimes Z - \otimes\left[\underline{c},\bar{c}\right]x\right)$$
$$s.t \quad Ax + \frac{B}{\otimes\left[\underline{d},\bar{d}\right]}\left(\otimes Z - \otimes\left[\underline{c},\bar{c}\right]x\right) \le r$$
$$x \ge 0$$

مساله بالا یک مساله برنامه‌ریزی یک سطحی خطی خاکستری است. با توجه به اینکه نقطه بهینه مساله برنامه‌ریزی خطی یکی از نقاط راسی است، بنابراین برای حل مساله کافی است که نقاط راسی با روش شمارش ضمنی بدست آورده شود.

تعریف۱۰: هرگاه یک یا چند محدودیت از محدودیت‌های یک مساله برنامه‌ریزی ریاضی را حذف کنیم یک فرم آزاد شده از آن مساله به دست می‌آید.

قضیه۱: [۱] فرض کنید که X مجموعه‌ای ناتهی، بسته و کران‌دار است. قرار می‌دهیم

$$a = \sup(X)\ ,\ b = \inf(X)$$

آنگاه،

الف) $a \in X$ **ب)** $b \in X$

۶. الگوریتم

۱. با در نظر گرفتن تابع هدف سطح دوم به عنوان یک متغییر جدید و جایگزین کردن آن در تابع هدف مساله سطح اول و محدودیت‌های دیگر، یک مساله برنامه ریزی خطی تک سطحی خاکستری حاصل می‌شود.
۲. نقاط راسی شدنی مساله حاصل را پیدا می‌کنیم.
۳. بنا بر قضیه ۱ هر نقطه راسی $(x, z) \in X$ یک نقطه راسی S برای مساله مینیمم‌سازی است اگر و تنها اگر داشته باشیم:

$$\forall \varepsilon > 0 \Rightarrow (x, z - \varepsilon) \notin X$$

۴. مقدار تابع هدف مساله را در نقاط راسی شدنی بدست آمده مقایسه کرده و جواب بهینه تعیین می‌شود.

برای نشان دادن کارایی روش یک مثال عددی حل شده است.

۷. مثال

مساله برنامه‌ریزی دو سطحی خطی خاکستری زیر را حل کنید.

$$\min_{x} \otimes F_1(x, y) =_G \otimes[1,3]x - \otimes[7,8]z$$
$$\min_{y} \otimes F_2(x, y) =_G \otimes[1,1]y$$
$$s.t \quad \begin{aligned} x + y &\geq 3 \\ -2x + y &\leq 0 \\ 2x + y &\leq 12 \\ 3x - 2y &\leq 4 \\ x, y &\geq 0 \end{aligned}$$

حل:

تابع هدف مساله سطح دوم را به عنوان یک متغییر جدید در نظر می‌گیریم.

$$\otimes z =_G \otimes[1,1] y$$

در این صورت مساله بالا به فرم زیر تبدیل می‌شود.

$$\min \otimes F_1(x,y) =_G \otimes[1,3] x - \otimes[7,8] z$$

$$\begin{aligned} s.t \qquad x + z &\geq 3 \\ -2x + z &\leq 0 \\ 2x + z &\leq 12 \\ 3x - 2z &\leq 4 \\ x &\geq 0 \end{aligned}$$

نقاط شدنی راسی مساله بالا عبارتند از:

$$\left.\begin{aligned} x + z &= 3 \\ -2x + z &= 0 \end{aligned}\right\} \Rightarrow (x,z) = (1,2) \quad , \quad \left.\begin{aligned} 2x + z &= 12 \\ -2x + z &= 0 \end{aligned}\right\} \Rightarrow (x,z) = (3,6)$$

$$\left.\begin{aligned} x + z &= 3 \\ 3x - 2z &= 4 \end{aligned}\right\} \Rightarrow (x,z) = (2,1) \quad , \quad \left.\begin{aligned} 2x + z &= 12 \\ 3x - 2z &= 4 \end{aligned}\right\} \Rightarrow (x,z) = (4,4)$$

طبق قاعده ارائه شده در گام ۴ برخی از نقاط راسی ممکن است حذف شوند.

$$(1,2-\varepsilon) \notin X \quad , \quad (2,1-\varepsilon) \notin X \quad , \quad (4,4-\varepsilon) \notin X \quad , \quad (3,6-\varepsilon) \in X$$

بنا بر قضیه ۱، نقطه $(3,6)$ نشدنی است. بنابراین تنها نقاط شدنی راسی مساله سه نقطه زیر می‌باشند.

$$(1,2) \quad , \quad (2,1) \quad , \quad (4,4)$$

مقدار تابع هدف را در نقاط شدنی محاسبه می‌کنیم.

$$(1,2) \Rightarrow \otimes F_1(1,2) =_G \otimes[1,3] \times 1 - \otimes[7,8] \times 2 =_G - \otimes[11,15]$$
$$(2,1) \Rightarrow \otimes F_1(2,1) =_G \otimes[1,3] \times 2 - \otimes[7,8] \times 1 =_G - \otimes[1,6]$$
$$(4,4) \Rightarrow \otimes F_1(4,4) =_G \otimes[1,3] \times 4 - \otimes[7,8] \times 4 =_G - \otimes[16,28]$$

با استفاده از تعریف ۳ و مقایسه مقدار تابع هدف در نقاط شدنی، نقطه شدنی $(4,4)$ ، به عنوان نقطه بهینه انتخاب می‌شود.

۸. نتیجه‌گیری

در این مقاله مساله برنامه‌ریزی خطی دو سطحی خاکستری معرفی گردید. برای حل این مساله از تبدیل مساله برنامه‌ریزی خطی دو سطحی خاکستری به یک مساله تک سطحی استفاده گردید. برای این منظور تابع هدف مساله سطح دوم به عنوان یک متغییر جدید به مساله اضافه می‌گردد و به این ترتیب یک مساله برنامه‌ریزی تک سطحی خاکستری خواهیم داشت. بنابراین با محاسبه نقاط شدنی و استفاده از روش شمارش ضمنی جواب بهینه مساله معرفی می‌گردد.

۹. مراجع

[۱] حسینی، ا. و نخعی، ع. و فتحی، م، "توسعه روش‌های حل مساله برنامه‌ریزی دو سطحی خطی بر اساس روش شمارش ضمنی و روش دوگان،" مجله مدل‌سازی پیشرفته ریاضی، دوره ۴، شماره ۱، ۱۳۹۳.

[2] J.F. Bard, "Some properties of the bi-level linear programming," *Journal of Optimization Theory and Applications*, vol. 68, pp. 371-373, 1991.

[3] J.L. Deng, "The control problems of grey systems," *Systems and Control Letters*, vol. 5, no. 1, pp. 288- 294, 1982.

[4] F. Pourofoghi, D. Darvishi, and J. Saffar Ardabili, "A New Approach to Finding the Answer of Transportation Problems with Grey Parameters," *Operational Research and Its Applications*, vol. 18. No. 2, pp. 59-73, 2021.

[5] F. Pourofoghi and D. Darvishi, "Applying Duality Results to Solve the Linear Programming Problems with Grey Parameters," *Control and Optimization in Applied Mathematics (COAM)*, vol. 5. No. 1, pp. 15-28, 2021.

زمان‌بندی کارها در محیط محاسبات ابری با استفاده از الگوریتم کلونی مورچه و الگوریتم ترکیبی جستجوی ابرکروی مبتنی‌بر نظریه آشوب و ژنتیک

رضا محمدی [*۱]، سکینه سهرابی [۲]، محمد نصیری [۳]، مهدی سخایی نیا [۴]

۱- استادیار، دانشکده فنی و مهندسی، دانشگاه بوعلی، همدان

۲- دانشجو دکتری، دانشکده فنی و مهندسی، دانشگاه بوعلی، همدان

۳- دانشیار، دانشکده فنی و مهندسی، دانشگاه بوعلی، همدان

۴- استادیار، دانشکده فنی و مهندسی، دانشگاه بوعلی، همدان

چکیده

مساله زمان‌بندی وظایف در محیط ابری موضوع مورد توجه در تحقیقات فعلی می‌باشد. زمان‌بندی مؤثر وظایف در محیط ابری برای افزایش رقابت‌پذیری بین شرکت‌ها و بهبود منافع اقتصادی آنها از اهمیت زیادی برخوردار است. در مواجهه با نیاز فوری به یک استراتژی زمان‌بندی کارآمد در دنیای واقعی، این مقاله فرآیند زمان‌بندی وظایف ابری را تحلیل کرده و سپس الگوریتمی برای زمان‌بندی کارها در محیط ابری ارائه می‌کند. روش پیشنهادی بر پایه الگوریتم کلونی مورچه و همچنین الگوریتم ترکیبی جستجوی ابرکروی مبتنی بر نظریه آشوب و ژنتیک استوار است. در الگوریتم جستجوی ابرکروی مبتنی بر نظریه آشوب و ژنتیک برای بهبود عملکرد سیستم از یک استراتژی جستجو متناسب با میزان اهمیت معیارهایی مشخص بهره گرفته شده است. این معیارها عبارت‌اند از بارکاری ماشین‌های مجازی، هزینه، مدت زمان انتظار و مدت زمان انجام کارهای وارد شده به سیستم. پس از پیاده‌سازی سناریو و تجزیه‌وتحلیل، نتایج حاصل از شبیه‌سازی بیانگر آن است که الگوریتم پیشنهادی با توجه به معیارهای مذکور، عملکرد بهتری نسبت به الگوریتم جستجوی ابرکروی مبتنی‌بر نظریه آشوب، الگوریتم ترکیبی جستجوی ابرکروی مبتنی‌بر نظریه آشوب و ژنتیک، الگوریتم‌های مبتنی بر ژنتیک و کلونی مورچه و دیگر الگوریتم‌های زمان‌بندی کار نظیر الگوریتم ترکیبی بهینه‌سازی ازدحام ذرات و ژنتیک دارد.

کلمات کلیدی: زمان‌بندی کار، الگوریتم بهینه‌سازی ترکیبی، الگوریتم ژنتیک، الگوریتم جستجوی ابرکروی مبتنی بر نظریه آشوب، الگوریتم بهینه‌سازی کلونی مورچه، محاسبات ابری

[*] **Corresponding author:** رضا محمدی
Email: r.mohammadi@basu.ac.ir

۱. مقدمه

در سال‌های اخیر، مفهوم محاسبات ابری برای فراهم کردن دسترسی فزاینده پویا به منابع محاسباتی مشترک (نرم‌افزار و سخت‌افزار) از طریق اینترنت مورد توجه قرار گرفته است. بسیاری از برنامه‌های کاربردی مبتنی بر فناوری توسط این محیط ارائه می‌شود که از طریق اینترنت توزیع شده‌اند. محاسبات ابری تغییرات فوق العاده‌ای را در دنیای فناوری اطلاعات تسهیل می‌کند [۲,۱]. محیط مذکور به عنوان یک فناوری جدید، به دلیل ارزش تجاری بسیار زیاد، به طور گسترده توسط شرکت‌ها مورد استفاده قرار گرفته است. محاسبات ابری لایه‌ای از انتزاع را بین جزئیات فنی‌اش و کاربران به وجود می‌آورد که این جزئیات را از دید کاربران پنهان می‌سازد، به همین خاطر از واژه‌ی ابر برای این محیط استفاده شده است. این محاسبات مدلی بر پایه‌ی شبکه‌های بزرگ کامپیوتری مانند اینترنت است که قادر به رفع نیازهای مطرح در فناوری اطلاعات می‌باشد. با کاربرد گسترده محاسبات ابری، تعداد کاربران ابری و تعداد وظایف وارد شده به محیط ابری به سرعت در حال رشد هستند. این مساله محیط ابری را با چالش‌های جدی روبرو کرده است. ظهور محاسبات ابری منجبر به تعریف دوباره الگوهای محاسبات و خدمات شده است. ماهیت این محیط یک تجمع بزرگ ازمنابع ذخیره سازی در مقیاس بزرگ را فراهم می‌کند که منابع داده و منابع محاسباتی را ادغام می‌کند. هم شرکت‌ها و هم افراد می‌توانند منابع مورد نیاز را با توجه به نیاز واقعی خود به دست آورند و این منابع می‌توانند به سرعت توسط ارائه دهندگان خدمات تهیه و تحویل داده شوند [۳]. محبوبیت محاسبات ابری از توانایی آن در ارائه خدمات جهانی فناوری اطلاعات مانند زیرساخت‌های اصلی، پلتفرم‌ها و برنامه‌های کاربردی به مشتریان ابری از طریق وب ناشی می‌شود. و می‌توان آن را به سه سطح تقسیم کرد: به دست آوردن استفاده از زیرساخت از طریق شبکه (IaaS)، پلت فرم به عنوان سرویس (PaaS) و نرم افزار به عنوان سرویس.(SaaS) [۴].

یکی از دلایل محبوبیت این محیط این است که منابع محاسباتی به عنوان سرویس‌های استاندارد در سطح شبکه ارائه می‌شوند. از سوی دیگر کاربران به کمک تکنیک‌های مجازی‌سازی قادر به استفاده از منابع به صورت نامحدود هستند. این مدل را آخرین پیشرفت محاسبات توزیع شده، محاسبات گرید و پردازش موازی می‌دانند. مسئله زمان‌بندی کارها در محیط ابر یکی از مسائل چالش برانگیز و اساسی می‌باشد. زمان‌بندی جریان کار را می‌توان پردازش مناسب کارها به نحوی که کارها بتوانند طبق معیار مورد نظر تکمیل شوند، تعریف کرد. امروزه اهمیت مسئله‌ی زمان‌بندی کارها در محیط ابر با توجه به سیستم‌هایی که از این محیط استفاده می‌کنند، قابل درک است. برای مثال می‌توان به سیستم‌های تصمیم‌یار هوشمند برای دستورالعمل‌های اضطراری شهر در محیط ابر و سیستم تصمیم‌گیری بلادرنگ برای سیستم تخلیه اضطراری هنگام آتش‌سوزی [۵] اشاره کرد. معیارهای مختلفی می‌تواند در بررسی عملکرد یک سیستم مدنظر باشد و این معیارها را می‌توان برای مقایسه و بررسی عملکرد الگوریتم‌های زمان‌بندی مورد استفاده قرار داد [۶]. عمده معیارهای مطرح برای کاربران این محیط شامل هزینه، مدت زمان اجرا، مدت زمان انجام کار، تعادل بارکاری درسیستم، سطح کیفیت خدمت و سطح رضایت کاربر می‌شود [۷]. یک نگرانی مهم عملکرد در محیط‌های غیرمتمرکز توزیع‌شده، مانند ابرها، این است که چگونه تضمین کنیم که کارها در زمان‌های تکمیل تخمینی با استفاده از پهنای باند منابع موجود به طور منصفانه و کارآمد و در عین حال در نظر گرفتن تغییرات عملکرد منابع، اجرای خود را کامل می‌کنند. روش‌هایی که برای زمان‌بندی کارها در محیط محاسبات ابر مورد استفاده قرار می‌گیرند از منظر این معیارها با هم متفاوتند. لازم به ذکر است که یک الگوریتم زمان‌بندی نامناسب می‌تواند باعث ناکارآمدی محیط ابر شود و انتخاب الگوریتم زمان‌بندی مناسب تأثیر زیادی در عملکرد این محیط دارد [۸]. با افزایش تعداد کاربران و مشاغل، مسئله زمان‌بندی کارها در محیط به یک فرآیند سخت تبدیل شده و از جمله مسائل چالش‌برانگیز در این محیط می‌باشد که مطالعات و تحقیقات انجام شده در این زمینه همچنان ادامه دارد زیرا یک مسئله NP-کامل است. به منظور ارضای نیاز مشتری به کیفیت خدمات یافتن یک استراتژی زمان‌بندی کارآمد و بسیار ضروری است [۹].

در سال‌های اخیر، الگوریتم‌های اکتشافی طبیعی برای زمان‌بندی وظایف به کار گرفته شده‌اند و عملکرد آنها بهتر از الگوریتم‌های سنتی است. به طور کلی، تکنیک ها و الگوریتم های بهینه سازی به دو دسته اصلی تقسیم می شوند: الگوریتم

های دقیق و الگوریتم‌های تقریبی. الگوریتم‌های دقیق می‌توانند به طور دقیق راه حل بهینه را تعیین کنند. با این حال، هنگامی که با مسائل بهینه‌سازی پیچیده مواجه می‌شوند، کارایی ندارند و باعث می‌شوند زمان اجرای آنها به صورت تصاعدی با ابعاد مسئله افزایش یابد. الگوریتم‌های تقریبی می‌توانند به سرعت راه‌حل‌های موثر برای مسائل چالش برانگیز بهینه‌سازی را شناسایی کنند. الگوریتم‌های تقریبی به سه نوع تقسیم می شوند: الگوریتم‌های اکتشافی، فراابتکاری و فوق‌ابتکاری [i]. دو مسئله اصلی با الگوریتم‌های اکتشافی، تمایل آن‌ها به به دام افتادن در راه‌حل‌های بهینه محلی و همگرایی اولیه آن‌ها با این راه‌حل‌ها است. الگوریتم‌های فراابتکاری برای رسیدگی به مسائلی که الگوریتم‌های اکتشافی با آن مواجه هستند معرفی می‌شوند. در واقع، الگوریتم‌های فراابتکاری دسته‌ای از الگوریتم‌های بهینه‌سازی تقریبی را نشان می‌دهند که استراتژی‌های خروج از نقاط بهینه محلی را ارائه می‌دهند. استانداردهای مختلفی را می توان برای دسته‌بندی الگوریتم‌های فراابتکاری استفاده کرد. در یکی از دسته‌بندی‌های ارائه شده، الگوریتم‌ها به دو گروه طبقه‌بندی شده اند: الگوریتم‌هایی که بر یک پاسخ تکیه دارند و الگوریتم‌هایی که بر یک جامعه تکیه دارند. تعدادی از الگوریتم‌های مبتنی بر جمعیت که در این مقاله به آنها اشاره شده است در زیر فهرست شده اند.

به عنوان مثال، الگوریتم ازدحام ذرات و الگوریتم ژنتیک انواعی از الگوریتم‌های فراابتکاری رایج هستند که مبتنی‌بر جمعیت می‌باشند. پس از آن، چندین الگوریتم زمان‌بندی هوشمند اکتشافی که از بهینه‌سازی پیشرفته مشتق شده‌اند ظاهر شدند. الگوریتم ژنتیک به عنوان یک روش بهینه‌سازی قدرتمند شناخته می‌شود [۱۰]. در این الگوریتم اطلاعات گذشته با توجه به موروثی بودن الگوریتم، استخراج شده و در روند جستجو مورد استفاده قرار می‌گیرند. الگوریتم ژنتیک یک رویکرد مناسب برای حل مسئله زمان‌بندی کارها در محیط محاسبات ابر می‌باشد. الگوریتم ژنتیک بهبود یافته (IGA) [۱۱] بر اساس الگوریتم ژنتیک (GA) با ترکیب یک "روش انتخاب سه مرحله ای" و شباهت متقابل منطقه‌ای ایجاد می‌شود، که شانس به دام افتادن الگوریتم ژنتیک در یک بهینه محلی را کاهش می‌دهد. الگوریتم ژنتیک پیشرفته (PGA) با الهام از فاگوسیتوز معرفی شده است [۱۲]. این الگوریتم بر اساس آن، یک الگوریتم ژنتیکی چند گروهی (MPHC_GA) را توسعه داده است. در الگوریتم مذکور از روش Min-Min برای ایجاد زیرجمعیت‌های چندگانه اولیه استفاده شده است، سپس به صورت جداگانه از طریق الگوریتم ژنتیک استاندارد (GA) و الگوریتم ژنتیک بهبود یافته مبتنی بر فاگوسیتوز (PGA) تکامل یافته است. الگوریتم بهینه‌سازی کلونی مورچه یکی دیگر از الگوریتم‌های مبتنی‌بر جمعیت می‌باشد. در این روش مورچه‌های مصنوعی به وسیله‌ی حرکت بر روی گراف مسئله، همچون مورچه‌های واقعی در مسیر حرکت خود نشانه‌هایی به نام فرومون باقی می‌گذارند که باعث می‌شود مورچه‌های بعدی بتوانند راه حل‌های بهتری را برای مسئله فراهم نمایند. این الگوریتم در حل بسیاری از مسائل بهینه‌سازی ترکیبی سخت موفق بوده و نتایج قابل قبولی را ارائه نموده است. امروزه توجه به بسط‌های مختلف این الگوریتم از اهمیت ویژه‌ای برخوردار است. الگوریتم کلونی مورچه یک نمونه‌ی موفق از سیستم‌های هوشمند گروهی بوده و یک راه حل مناسب برای حل مسئله زمان‌بندی کارها در محیط ابر ارائه می‌نماید. الگوریتم بهینه‌سازی ازدحام ذرات پیشرفته یکی دیگر از الگوریتم‌های مبتنی‌بر جمعیت استفاده شده در محیط ابری می‌باشد [۱۳]. در روش مذکور از یک استراتژی اثربخش استفاده شده است. الگوریتم عنکبوت اجتماعی پر هرج و مرج [۱۴] از الگوریتم عنکبوت اجتماعی مشتق شده است و برای رسیدگی به مسئله زمان‌بندی کار در ماشین‌های مجازی ناهمگن مختلف در محیط ابر معرفی شده است.

در این مقاله یک روش برای زمان‌بندی کارها در محیط محاسبات ابر ارائه می‌شود. زمان‌بندی کارها با استفاده از الگوریتم پیشنهادی که بر پایه الگوریتم کلونی مورچه و الگوریتم ترکیبی جستجوی ابرکروی مبتنی‌بر نظریه آشوب و ژنتیک استوار است، انجام می‌شود. در الگوریتم پیشنهادی از یک استراتژی جستجو براساس میزان اهمیت معیارهای موردنظر در ارزیابی سیستم ابر، کمک گرفته شده است. این استراتژی با توجه به معیارهای مدنظر می‌تواند متفاوت باشد و این امر منجر به بهبود عملکرد سیستم می‌شود. بررسی نتایج بدست آمده بیانگر آن است که الگوریتم پیشنهادی عملکرد بهتری نسبت به برخی از الگوریتم‌های زمان‌بندی نظیر الگوریتم ژنتیک، بهینه‌سازی کلونی مورچه، الگوریتم جستجوی ابرکروی مبتنی‌بر

نظریه آشوب [۱۵]، الگوریتم ترکیبی بهینه‌سازی ازدحام و ژنتیک [۱۶،۱۵]، الگوریتم ترکیبی با استفاده از الگوریتم ژنتیک و جستجوی ابرکروی مبتنی‌بر نظریه آشوب برای زمان‌بندی کارها در محیط ابر [۱۷] و همچنین دیگر الگوریتم‌های زمان‌بندی کار نظیر الگوریتم ترکیبی بهینه‌سازی ازدحام ذرات و ژنتیک دارد.

ادامه مقاله به صورت زیر سازماندهی شده است: از آنجایی که الگوریتم پیشنهادی در این مقاله بر پایه الگوریتم کلونی مورچه و الگوریتم ترکیبی جستجوی ابرکروی مبتنی بر نظریه آشوب و ژنتیک استوار است، در بخش دوم به توضیح الگوریتم‌های مورد استفاده در الگوریتم مذکور پرداخته می‌شود. در بخش سوم الگوریتم‌های پیشنهادی شرح داده می‌شوند. در بخش چهارم نتایج آزمایشات و شبیه‌سازی‌ها آورده می‌شود و در بخش پنجم نتایج حاصل از اجرای الگوریتم بررسی می‌شود.

۲. مروری بر الگوریتم‌های مورد استفاده در این مقاله

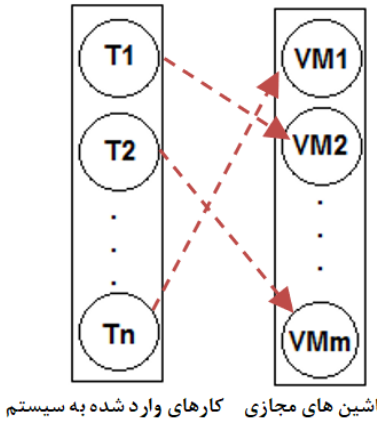
در این بخش به توضیح الگوریتم‌های مورد استفاده در الگوریتم پیشنهادی پرداخته می‌شود. روش پیشنهادی برای زمان‌بندی کارها در محیط ابر در بخش ۳ ارائه خواهد شد. این الگوریتم بر پایه الگوریتم کلونی مورچه و الگوریتم ترکیبی جستجوی ابرکروی مبتنی بر نظریه آشوب و ژنتیک استوار است. در ادامه هر یک از الگوریتم‌های مذکور توضیح داده می‌شود.

۲-۱. الگوریتم بهینه‌سازی کلونی مورچه (ACO)

در این بخش به توضیح الگوریتم کلونی مورچه[۱۸] مورد استفاده برای زمان‌بندی کارها در محیط محاسبات ابر پرداخته می‌شود. از مفروضات در نظر گرفته شده در این مقاله می‌توان به موارد زیر اشاره کرد:

- ✓ کارها به صورت دسته‌ای به سیستم وارد می‌شوند.
- ✓ کارها مستقل از هم می‌باشند.

برای نمایش مسئله پیش‌رو از گراف $G = (N, E)$ که در شکل (۱) آورده شده است، استفاده می‌شود. در این گراف گره‌ها به دو دسته تقسیم‌بندی می‌شوند. گره‌های موجود در دسته‌ی سمت چپ بیانگرکارهای وارد شده به سیستم و گره‌های موجود در دسته‌ی راست بیانگر ماشین‌های مجازی موجود در سیستم می‌باشد. یال‌های بین دو دسته‌ی مذکور نشان‌دهنده‌ی نحوه‌ی اختصاص کارها بر روی ماشین‌های‌مجازی می‌باشند. الگوریتم کلونی مورچه از سه گام که در ادامه به اختصار توضیح داده می‌شود، تشکیل شده است.



شکل ۱ – سرعت نمایش مسئله زمان‌بندی کارها با استفاده از الگوریتم ACO

۲-۱-۱. مقداردهی اولیه

در این مرحله ابتدا پارامترهای اولیه الگوریتم از جمله تعداد تکرار و تعداد مورچه مصنوعی موجود در سیستم مقداردهی می‌شوند. سپس به تعداد تعیین شده در ابتدای الگوریتم، مورچه‌ی مصنوعی ایجاد می‌شود. روند اجرای کلونی مورچه به این صورت است که در هر تکرار از اجرای الگوریتم، مورچه‌های مصنوعی توسط حرکت خود بر روی گراف مسئله یک مسیر را طی می‌کنند. مسیر طی شده بیانگر نحوه‌ی اختصاص کارها به ماشین‌های مجازی می‌باشد و به عنوان یک راه‌حل برای مسئله‌ی پیش‌رو در نظر گرفته می‌شود. برای هر مورچه‌ی ساخته شده در الگوریتم، یک ماشین مجازی به صورت تصادفی انتخاب شده که نقطه‌ی شروع مسیر حرکت مورچه را تعیین می‌کند. سپس اولین کار وارد شده به سیستم به ماشین‌مجازی انتخاب شده، اختصاص می‌یابد. در ادامه هر مورچه با استفاده از قانون انتخاب ماشین‌مجازی (در بخش ۲-۱-۲ توضیح داده می‌شود)، مجددا یک ماشین‌مجازی را برای ادامه‌ی حرکت خود انتخاب کرده و دومین کار وارد شده به سیستم به آن ماشین‌مجازی، اختصاص می‌یابد. برای اختصاص دیگر کارهای وارد شده به سیستم مستلزم حرکت مورچه بر روی گراف مسئله هستیم. این روند تا اختصاص تمامی کارهای وارد شده به سیستم ادامه می‌یابد. مسیریابی مورچه‌ها در قانون انتخاب ماشین‌مجازی با استفاده از میزان فرومون انباشته شده بر روی هر مسیر انجام می‌شود. میزان فرومون اولیه برای هر مسیر در زمان صفر با استفاده از رابطه (۱) محاسبه می‌شود.

$$\tau_i(0) = pe_num_i \times pe_mips_i + vm_bw_i \qquad (۱)$$

در رابطه (۱) متغیرهای vm_bw_i ، pe_num_i و pe_mips_i به ترتیب نشان‌دهنده پهنای باند، تعداد پردازنده و نرخ اجرای دستورالعمل‌ها توسط هر پردازنده در ماشین‌مجازی j ام، Vm_j می‌باشند.

۲-۱-۲. قانون انتخاب ماشین مجازی برای کار بعدی

برای اختصاص دیگر کارهای وارد شده به سیستم مستلزم حرکت مورچه بر روی گراف مسئله هستیم. هر مورچه با استفاده از قانون انتخاب ماشین‌مجازی یک ماشین‌مجازی را برای ادامه‌ی حرکت خود انتخاب کرده و کار وارد شده به سیستم به آن ماشین‌مجازی، اختصاص می‌یابد. این روند تا اختصاص تمامی کارهای وارد شده به سیستم ادامه می‌یابد. هر مورچه برای حرکت بین ماشین‌های مجازی از تابع احتمالی که در رابطه (۲) آورده شده است، استفاده می‌کند.

$$P_{ij}^{\,k}(t) = \begin{cases} \dfrac{\left[\tau_{ij}(t)\right]^{\alpha}\left[\eta_{ij}(t)\right]^{\beta}\left[LB_{ij}(t)\right]^{\gamma}}{\sum_{s \in allowed_k} \left[\tau_{is}(t)\right]^{\alpha}\left[\eta_{is}(t)\right]^{\beta}\left[LB_{is}(t)\right]^{\gamma}} & \\ 0, & otherwise \end{cases} \qquad (۲)$$

ر رابطه (۲)، متغیر $\tau_{ij}(t)$ میزان غلظت فرومون را در مسیر بین Vm_j و $Task_i$ در زمان t نشان می‌دهد. متغیر $\eta_{ij}(t)$ نشان‌دهنده اطلاعات اکتشافی می‌باشد که با استفاده از رابطه (۳) محاسبه می‌شود.

$$\eta_{ij}(t) = \frac{1}{d_{ij}} \qquad (۳)$$

در رابطه (۳) متغیر d_{ij} برابر است با مجموع زمان اجرا و زمان انتقال $Task_i$ به Vm_j که با استفاده از رابطه (۴) محاسبه می‌شود.

$$d_{ij} = \frac{TL_Task_i}{pe_num_j \times pe_mips_j_Vm_j} + \frac{InputFileSize}{Vm_bw_j} \qquad (۴)$$

در رابطه (۴) متغیرهای TL_Task_i، $InputFileSize$، Vm_bw_j، pe_num_j و $pe_mips_j_Vm_j$ به ترتیب نشان‌دهنده طول کار (برحسب تعداد دستورالعمل‌ها) ارسال شده به Vm_j، اندازه کار موردنظر، پهنای باند، تعداد پردازنده و نرخ اجرای دستورالعمل‌ها توسط هر پردازنده در Vm_j می‌باشند.

متغیر LB_{ij} نشان‌دهنده بارکاری ماشین‌های مجازی موجود در سیستم بوده و با استفاده از رابطه (۵) بدست می‌آید.

$$LB_{ij} = 1 - \frac{res_j - LastAver_res}{res_j + LastAver_res} \qquad (۵)$$

در رابطه (۵) متغیر $LastAver_res$ بیانگر میانگین زمان اجرای ماشین‌های مجازی در بهترین مسیر ایجاد شده توسط مورچه‌ها، در آخرین تکرار از اجرای الگوریتم می‌باشد. در این رابطه متغیر res_j نشان‌دهنده‌ی زمان اجرای کارها در Vm_j است که توسط رابطه (۶) محاسبه می‌شود.

$$res_j = \sum_{m \in total_task} d_{mj} \qquad (۶)$$

در رابطه (۶) متغیر $total_task$ بیانگر لیست کارهای اختصاص داده شده به Vm_j است و متغیر برابر است با مجموع زمان اجرا و زمان انتقال $Task_j$ به Vm_j که توسط رابطه (۴) محاسبه می‌شود.

در رابطه (۲) باید توجه داشت که $s \in allowed_k$ می‌باشد و همچنین $allowed_k = \{1,2,...,m\} - tabu_k$ است. متغیر $tabu_k$ بیانگر لیست ماشین‌های مجازی طی شده توسط مورچه kام است. درواقع $allowed_k$ نشان‌دهنده‌ی لیست ماشین‌های مجازی مجاز برای عبور مورچه kام است.

در رابطه (۲) از متغیرهای β, α و γ به ترتیب برای تنظیم میزان اهمیت پارامترهای $\tau_{ij}(t)$ ، $\eta_{ij}(t)$ و $LB_{ij}(t)$ استفاده شده است.

پس از آنکه هر مورچه‌ی موجود در سیستم با استفاده از رابطه (۲) یک مسیر را طی کرد، مقداری فرومون بر روی مسیر حرکت خود به جای می‌گذارد که این مقدار با استفاده از رابطه‌ی (۷) محاسبه می‌شود.

$$\Delta\tau_{ij}(t) = \begin{cases} \dfrac{Q}{L^k(t)} & if\ (i,j) \in T^k(t) \\ 0, & if\ (i,j) \notin T^k(t) \end{cases} \qquad (۷)$$

در رابطه (۷) متغیر $T^k(t)$ نشان‌دهنده‌ی مسیر ایجاد شده توسط مورچه kام در زمان t می‌باشد. متغیر $L^k(t)$ بیانگر طول مسیر طی شده توسط مورچه kام در زمان t می‌باشد. در این مقاله مسیر ایجاد شده توسط هر مورچه به عنوان یک راه‌حل برای مسئله پیش‌رو درنظر گرفته می‌شود که بیانگر نحوه‌ی اختصاص کارها به ماشین‌های مجازی می‌باشد. برای محاسبه‌ی طول هر مسیر ابتدا با استفاده از مسیر پیشنهادی توسط هر مورچه شبیه‌سازی انجام می‌شود، سپس کارایی سیستم محاسبه شده و به عنوان طول مسیر مورد بررسی، درنظر گرفته می‌شود. لازم به ذکر است که متغیر Q یک پارامتر قابل تطبیق می‌باشد. معیارهای موردنظر در این مقاله و میزان اهمیت هر یک در جدول (۱) آورده شده است.

جدول ۱- معیارهای مدنظر در شبیه‌سازی

معیارها	متغیر	میزان اهمیت(ضریب)
مدت زمان انتظار	Wait	۰/۰۰۱
هزینه	Cost	۰/۰۰۲
مدت زمان انجام کار	Makespane	۰/۰۰۳
درجه عدم تعادل بارکاری در ماشین‌های مجازی	Dimb	۰/۰۰۴

متغیر $L^k(t)$ با استفاده رابطه (۸) بدست می‌آید. در این رابطه مقدار $Dimb$ بیانگر درجه عدم تعادل بارکاری در ماشین‌های مجازی بوده و با استفاده از رابطه (۹) محاسبه می‌شود.

$$L^k(t) = 0.004 \times Dimb + 0.003 \times Makespane + 0.002 \times Cost + 0.001 \times Wait \quad (۸)$$

$$Dimb = \frac{T_{Max} + T_{Min}}{T_{Avg}} \quad (۹)$$

$$T_i = \frac{Total_tasklength_j}{pe_num_j \times pe_mips_j} \quad (۱۰)$$

در رابطه (۹) متغیرهای T_{Min}، T_{Max} و T_{Avg} به ترتیب بیانگر بیشترین، کمترین و میانگین مقدار متغیر T_i در میان ماشین‌های مجازی می‌باشند. مقدار T_i با استفاده از رابطه (۹) محاسبه می‌شود که در این رابطه متغیرهای $Total_tasklength_j$، pe_num_j و pe_mips_j به ترتیب بیانگر مجموع طول وظایف اجرا شده توسط Vm_j، تعداد پردازنده‌ها و نرخ اجرای دستورالعمل‌ها توسط هر پردازنده در Vm_j می‌باشند.

۲-۱-۳. بهنگام سازی فرومون انباشته شده بر روی مسیرها

در این بخش میزان فرومون انباشته شده بر روی مسیرها بهنگام می‌شود. بهنگام‌سازی شامل دو مرحله‌ی بهنگام‌سازی محلی و سراسری می‌شود که در ادامه به توضیح هر یک پرداخته شده است.

۱. بهنگام‌سازی محلی: پس از آنکه هر مورچه یک دور را طی کرد، یک راه‌حل ایجاد می‌شود. سپس میزان فرومون انباشته شده بر روی مسیر طی شده توسط همان مورچه به صورت محلی بهنگام می‌شود. در کلونی مورچه‌ها این عمل با کاهش مقدار فرمون توسط یک فاکتور ثابت (ضریب تبخیر) انجام می‌شود. ضریب تبخیر فرومون برای اجتناب از انباشته شدن بی‌حد دنباله فرومون درنظر گرفته شده است که الگوریتم را قادر می‌سازد تا تصمیم بدی را که قبلا گرفته است، فراموش کند. میزان فرومون انباشته شده بر روی یال‌هایی که توسط مورچه‌ها انتخاب نشده‌اند، با افزایش تعداد تکرار الگوریتم به صورت نمایی کاهش می‌یابد. برای بهنگام‌سازی محلی از رابطه (۱۱) استفاده می‌شود.

$$\tau_{ij}(t) = (1-\rho)\tau_{ij}(t) + \Delta\tau_{ij}(t) \quad (۱۱)$$

در رابطه (۱۱) متغیر ρ ضریب تبخیر فرومون می‌باشد که $0 < \rho < 1$ است. متغیر $\Delta\tau_{ij}(t)$ بیانگر میزان فرومون انباشته شده بر روی مسیر بین Vm_j و $Task_i$ است که برای محاسبه‌ی آن باید مجموع مقدار فرمون به جا گذاشته شده توسط هر مورچه را بر روی مسیر مورد بررسی محاسبه کرد. برای این منظور از رابطه (۱۲) استفاده می‌شود.

$$\Delta\tau_{ij}(t) = \sum_{k=1}^{m} \Delta\tau_{ij}^{k}(t)(t) \quad (۱۲)$$

در رابطه (۱۲) متغیر m نشان‌دهنده‌ی تعداد مورچه‌های موجود در سیستم بوده و متغیر $\Delta\tau_{ij}(t)$ بیانگر میزان فرومون انباشته شده توسط هر مورچه بر روی مسیر مورد بررسی می‌باشد.

۲. بهنگام‌سازی سراسری: پس از آنکه تمامی مورچه‌ها یک دور را طی کردند، بر اساس اندازه طول بهترین مسیر طی شده توسط مورچه‌ها که در متغیر T^+ نگهداری می‌شود، میزان فرومون انباشته شده بر روی یال‌ها با استفاده از رابطه (۱۳) به صورت سراسری بهنگام می‌شود.

$$\tau_{ij}(t) = \tau_{ij}(t) + \frac{Q}{L^+}, \quad if\,(i,j) \in T^+ \qquad (۱۳)$$

در رابطه (۱۳) متغیر Q یک پارامتر قابل تطبیق می‌باشد، متغیر L^+ بیانگر طول بهترین مسیر طی شده توسط مورچه‌ها می‌باشد. همان‌طور که پیش‌تر گفته شد، برای محاسبه‌ی مقدار L^+ ابتدا برای مسیرهای ساخته شده، شبیه‌سازی انجام می‌شود و طول هر مسیر با استفاده از رابطه (۸) محاسبه می‌شود و کمترین آن‌ها به عنوان طول بهترین مسیر طی شده، انتخاب می‌شود.

۲-۲. الگوریتم بهینه‌سازی ترکیبی با استفاده از الگوریتم ژنتیک و جستجوی ابرکروی مبتنی بر نظریه آشوب برای زمان‌بندی کارها در محیط محاسبات ابر (CHSS_GA)

در این قسمت الگوریتم بهینه‌سازی ترکیبی با استفاده از الگوریتم ژنتیک و جستجوی ابرکروی مبتنی بر نظریه آشوب برای زمان‌بندی کارها در محیط محاسبات ابر شرح داده می‌شود. در الگوریتم مذکور علاوه بر استفاده از الگوریتم ژنتیک [۱۶] که به عنوان یک روش بهینه‌سازی قدرتمند شناخته می‌شود، از الگوریتم جستجوی ابرکروی مبتنی‌بر نظریه آشوب نیز استفاده شده است. الگوریتم جستجوی ابرکروی مبتنی‌بر نظریه آشوب نسخه جدیدی از الگوریتم جستجوی ابرکروی استاندارد [۱۵] با استفاده از نظریه آشوب می‌باشد که ضعف الگوریتم جستجوی ابرکروی استاندارد مبنی‌بر سرعت همگرایی و زیاد بودن تعداد تکرار اجرای الگوریتم برای رسیدن به جواب بهینه را برطرف می‌نماید. در الگوریتم جستجوی ابرکروی استاندارد همانند اکثر الگوریتم‌های فرابتکاری با اجزای تصادفی، تابع توزیع احتمال استفاده شده تابع توزیع احتمال گاوسی یا یکنواخت می‌باشد اما درالگوریتم جستجوی ابرکروی مبتنی‌بر نظریه آشوب مقادیر حاصل از نگاشت آشوب جایگزین این مقادیر تصادفی می‌شوند. از آنجایی که نظریه آشوب با قطعیت همراه است، می‌توان به قطعی بودن نتایج حاصل اطمینان داشت. الگوریتم مذکور از پنج گام که در ادامه به اختصار توضیح داده شده است، تشکیل می‌شود.

۲-۲-۱. مقداردهی اولیه و تولید ذرات

در این گام ابتدا پارامترهای اولیه الگوریتم از جمله تعداد مراکز کره، اندازه شعاع کره، تعداد ذرات جدیدی که در هر تکرار اضافه می‌شوند و تعداد جمعیت اولیه مقداردهی می‌شوند. سپس به کمک نگاشت لیبویتچ که در رابطه (۱۳) آورده شده است، جمعیت اولیه تولید می‌شود. جمعیت اولیه شامل ذراتی می‌باشد که هر ذره یک راه‌حل برای مسئله پیش‌رو است. هر ذره دارای دو قسمت متغیرها و مقدار تابع هدف است. متغیرهای یک ذره نشان‌دهنده‌ی نحوه‌ی اختصاص کارها به ماشین‌های مجازی می‌باشند و مقدار تابع هدف یک ذره بیانگر کارایی سیستم برای راه‌حل ارائه شده توسط متغیرها می‌باشد. برای هر ذره ابتدا با استفاده از متغیرهای آن ذره، شبیه‌سازی انجام می‌شود، سپس کارایی سیستم محاسبه شده و به عنوان مقدار تابع هدف آن ذره درنظر گرفته می‌شود.

$$x_{k+1} = \begin{cases} \alpha x_k, & 0 < x_k < p_1 \\ \dfrac{p_2 - x_k}{p_2 - p_1}, & p_1 < x_k < p_2 \\ 1 - \beta(1 - x_k), & p_1 < x_k < 1 \end{cases} \qquad (۱۳)$$

در ادامه به تعداد معین که در ابتدای الگوریتم مشخص شده است، بهترین ذرات (ذراتی که دارای کمترین مقدار تابع هدف هستند) از بین ذرات تولید شده، به عنوان مراکز کره انتخاب می‌شوند و مابقی ذرات توسط معیار غلبه‌ی مراکز کره که از رابطه (۱۴) بدست می‌آید حول مراکز ذرات قرار خواهند گرفت.

$$D_{SC} = \left| \left(\frac{OFD_{SC}}{\sum_{i=1}^{N_{SC}} OFD_i} \right) \right| \qquad (۱۴)$$

در رابطه‌ی (۱۴) OFD برای هر مرکز کره برابر است با اختلاف تابع هدف آن مرکز با بیشینه مقدار تابع هدف از بین همه‌ی مراکز کره‌ها که با استفاده از رابطه (۱۵) محاسبه می‌شود.

$$OFD_{sc} = f_{sc} - \max_{sc}\{f\} \qquad (۱۵)$$

در رابطه (۱۵) f_{sc} عبارت است از مقدار تابع هدف مرکز کره‌ی مورد بررسی و SC_s بیانگر مجموعه‌ی مراکز کره‌ها می‌باشد.

۲-۲-۲. جستجو

در این گام با استفاده از استراتژی جستجوی متناسب با معیارها و بر اساس میزان اهمیت (ضریب) هر یک از معیارها، یک ذره در فضای محدود شده به وسیله‌ی یک کره به دنبال پاسخ بهتر می‌گردد. لازم به ذکر است که با توجه به معیارهای مدنظر و ضرایب هر یک که در جدول (۱) آورده شده است، مدت زمان انجام کار و درجه عدم تعادل بارکاری ماشین‌های مجازی دو معیار مطرح می‌باشند زیرا نسبت به سایر معیارهای در نظر گرفته شده از اهمیت بیشتری برخوردار هستند. بنابراین در گام جستجو ابتدا تابع $Sort_VmAndClds$ که به معیار درجه عدم تعادل بارکاری ماشین‌های مجازی می‌پردازد، برای تمامی ذرات اجرا شده و در ادامه تابع $Find_MaxForMin$ که به معیار مدت زمان انجام کار می‌پردازد، برای تمامی مراکز کره اجرا می‌شود. هر یک از توابع مذکور یک ذره و لیست ماشین‌های مجازی موجود در سیستم را به عنوان ورودی دریافت می‌کند و پس از اجرا، یک ذره را به عنوان خروجی به الگوریتم برمی‌گرداند. در صورتی که پس از اجرای هر یک از توابع مذکور در نتیجه بهبود حاصل نشود، ذره ورودی به عنوان خروجی به الگوریتم برگردانده می‌شود. روند اجرای تابع $Sort_VmAndClds$ در شکل (۲) آورده شده است که به اختصار توضیح داده می‌شود.

Function Sort_VmAndClds

Input: A Particle (Solution) and List Of *VMs*

Output: *Best_Particle*

Steps:

1. Set *Best_Particle* = null, *New_Particle* =null, *Old_Particle* = *Particle*

2. Set *Chance_Array* (*VMs* Chance)

3. Sort *Chance_Array* (Dessending)

4. Set N_tasks_Array (Number of Task that submit to each *VM*)

5. Foreach *VM* in List of *VMs*

If exsit *VM* with more chances and fewer task

Set *New_Particle* with swap number of tasks of Two *VMs*

End Foreach

6. Run Simulation with *New_Particle*

7. If Result of simulation of *New_Particle* is less than Result of *Old_Particle*

Best_Particle = *New_Particle* else *Best_Particle* = *Old_Particle*

8. Return *Best_Particle*

شکل ۲– تابع Sort_VmAndClds

در گام اول الگوریتم جستجوی ابرکروی مبتنی بر نظریه آشوب، برای تولید جمعیت اولیه از مقادیر حاصل از نگاشت لیبویتچ استفاده شده است و در اختصاص کارها به ماشین‌های مجازی به ظرفیت، سرعت و پهنای باند ماشین‌های مجازی توجه نشده است، از این رو در تابع $Sort_VmAndClds$ ابتدا به کمک رابطه (۱۶) شانس انتخاب هر ماشین مجازی محاسبه شده و در آرایه $Chance_Array$ نگهداری می‌شود.

$$Ch_i = pe_num_i \times pe_mips_i _Vm + vm_bw_i \quad (۱۶)$$

در رابطه (۱۶) مقدار متغیرهای vm_bw_i، pe_mips_i و pe_num_i به ترتیب برابر با پهنای باند، تعداد پردازنده‌ها و نرخ اجرای دستورالعمل‌ها توسط هر پردازنده در ماشین مجازی j ام، Vm_j می‌باشند. آنگاه با استفاده از قسمت متغیرها در ذره‌ی وارد شده به تابع که بیانگر نحوه‌ی اختصاص کارها به ماشین‌های مجازی می‌باشد، تعداد کار اختصاص داده شده به هر ماشین مجازی محاسبه شده و این اطلاعات در آرایه N_tasks_Array ذخیره می‌گردد. آرایه $Chance_Array$ که شامل شانس انتخاب هر یک از ماشین‌مجازی‌های موجود در سیستم برای اجرای $task_i$ می‌باشد، به صورت نزولی مرتب می‌شود. آنگاه اگر ماشین مجازی با شانس بیشتر و تعداد کار کمتر نسبت به ماشین مجازی دیگری با شانس کمتر و تعداد کار بیشتر در سیستم وجود داشت، در آرایه N_tasks_Array تعداد کارهای ارسال شده به دو ماشین مجازی مذکور با هم جابه جا می‌شوند، در واقع هدف از اجرای تابع $Sort_VmAndClds$ اختصاص تعداد کار بیشتر به ماشین‌مجازی با شانس بیشتر نسبت به ماشین‌مجازی با شانس کمتر است. سپس با استفاده از لیست کارهای وارد شده به سیستم، به هر یک از ماشین‌های مجازی بر اساس تعداد تعیین شده در آرایه N_tasks_Array، از ابتدای لیست کارهای وارد شده به سیستم، کار برای اجرا اختصاص می‌یابد. پس از آنکه برای تمامی ذرات تابع $Sort_VmAndClds$ اجرا شد، تابع $Find_MaxForMin$ برای تمامی مراکز کره اجرا می‌شود. روند اجرای تابع $Find_MaxForMin$ در شکل (۳) آورده شده است که در ادامه به اختصار توضیح داده می‌شود.

Function Find_MaxForMin

Input: A *SC* (Solution) and *List Of VMs*

Output: Best_Sc

Steps:

1. Set $Best_Sc = null$, $New_SC = null$, $Old_SC = SC$

2. Set $Makespane_Array$ (Makespane of VMs)

3. Sort $Makespane_Array$ (Dessending)

4. Set $Max_Makespane_VM$ and Set $Min_Makespane_VM$

5. Set New_SC : First Cloudlet that submited to $Max_Makespane_VM$, Submit to $Min_Makespane_VM$

6. If Result of simulation of New_SC is less than Result of $Old_Particle$ $Best_SC = New_SC$ else $Best_SC = Old_SC$

7. Return $Best_SC$

شکل ۳– تابع Find_MaxForMin

با توجه به شکل (۴) در تابع $Find_MaxForMin$ ابتدا مدت زمان انجام کارها روی هر ماشین مجازی محاسبه شده و در آرایه Makespane_Array نگهداری می‌شود. سپس آرایه را به صورت صعودی مرتب کرده و دو متغیر $Max_Makespane_VM$ و $Min_Makespane_VM$ با استفاده از شناسه‌ی مربوط به ماشین‌های مجازی که به ترتیب بیشترین و کمترین مقدار مدت زمان انجام کار را دارا هستند، مقداردهی می‌شوند. در ادامه اولین وظیفه از لیست

کارهای ارسال شده به ماشین مجازی با شناسه برابر با $Max_Makespane_VM$ یعنی ماشین مجازی که بیشترین مدت زمان انجام کار را دارا هست، حذف شده و به ماشین مجازی با شناسه‌ای برابر با $Min_Makespane_VM$ ارسال می‌شود. در این بخش مقدار تابع هدف (همانند بخش ۲-۱) به کمک رابطه (۸) بدست می‌آید.

۲-۲-۳. تغییر فضای جستجوی نامناسب

همان‌طور که پیش‌تر گفته شد در گام اول الگوریتم، مراکز کره و همچنین ذرات متعلق به هر کره تعیین می‌شوند. آنگاه در گام جستجو هر ذره در کره‌ی مربوط به خود به دنبال پاسخ بهتر می‌گردد. در این بخش دو نکته حائز اهمیت است:

۱. بعد از انجام گام جستجو درصورتی که یک ذره به موقعیتی با مقدار تابع هدف کم‌تر از مرکز کره متناظر با خود برسد، ذره مورد نظر به عنوان مرکز کره شناخته شده و مرکز کره قبلی به عنوان ذره، حول مرکز کره جدید فضا را جستجو می‌کند.
۲. بعضی ذرات در مجموعه‌ای که به آن تعلق گرفته‌اند دارای مقدار تابع هدف نامناسبی هستند، بنابراین انتظار نمی‌رود که این ذرات با جستجو در فضایی که به آن تعلق گرفته‌اند بتوانند به مقدار مطلوب برای تابع هدف مورد بررسی برسند. درنتیجه، فضای جستجوی آن‌ها باید تغییر یابد تا بتوانند فضای مناسب‌تری را جستجو نمایند. این ذرات شناسایی شده و به کره‌های دیگر اختصاص می‌یابند.

۲-۲-۴. تولید ذرات جدید

برای جستجوی بهتر فضا و منعطف‌تر نمودن الگوریتم، در هر تکرار یک تعداد معین از بدترین ذرات (ذراتی که دارای مقدار تابع هدف بیشتری می‌باشند) حذف شده و به همان تعداد ذرات جدید تولید شده و جایگزین این ذرات می‌شوند. تعداد تعیین شده برای تولید ذرات جدید در هر تکرار از اجرای الگوریتم، نباید زیاد باشد و این تعداد در ابتدای الگوریتم تعیین می‌شود. ذرات جدید به سه روش با احتمال انتخاب برابر که در ادامه آورده شده است، تولید می‌شوند.

۱. ذرات مانند گام اول الگوریتم به کمک مقادیر حاصل از نگاشت لیبویتچ که در رابطه (۱۳) آورده شده است، تولید می‌شوند.
۲. ذرات تولید شده در گام اول الگوریتم، به عنوان جمعیت اولیه به الگوریتم ژنتیک داده می‌شود و سپس الگوریتم ژنتیک یک بار و m مرتبه (m برابر با تعداد ذرات جدید است) تکرار می‌شود. در ادامه m ذره، از بین بهترین ذرات یعنی ذراتی که دارای مقدار تابع هدف کمتری هستند انتخاب شده و به عنوان ذرات جدید به الگوریتم داده می‌شوند.
۳. برای تولید ذرات جدید از عملگر پیشنهادی استفاده می‌شود. در معرفی عملگر پیشنهادی از عملگر آمیزش الگوریتم ژنتیک ایده گرفته شده است. برای این منظور به تعداد m مرتبه عملگر پیشنهادی را اجرا کرده و نتیجه‌ی حاصل از هربار اجرای این عملگر، تولید یک ذره با استفاده از بهترین ذرات موجود در سیستم می‌باشد. این عملگر به جای عمل بر روی زوج کروموزوم (ذره)، بر روی بهترین کروموزوم‌ها عمل می‌کند. به این صورت که برای تعیین مقدار ژن (متغیر) اول، یک کروموزوم را از بین بهترین کروموزوم‌ها به صورت تصادفی انتخاب کرده و محتوای ژن مدنظر در کروموزوم جدید را برابر محتوای ژن متناظر در کروموزوم انتخابی قرار می‌دهد و این عمل را به تعداد ژن‌های کروموزوم تکرار می‌کند.

۲-۲-۵. آزمون همگرایی

الگوریتم با رسیدن به یکی از شرایط زیر خاتمه می‌یابد:
الف) تعداد تکرار اجرای الگوریتم به یک تعداد معین برسد.
ب) اختلاف تابع هدف بهترین کره از بین کره‌های موجود در دو تکرار متوالی کمتر از مقدار آستانه تعیین شده، شود. روند اجرای الگوریتم بهینه‌سازی ترکیبی با استفاده از الگوریتم ژنتیک و جستجوی ابرکروی مبتنی بر نظریه آشوب در شکل (۴) آورده شده است.

Function CHSS_GA

Input: (*num _ pop* , *num _ SC* , *cloudlet _ list* , *Vm _ list*)

Output: *Optimal _ Solution*

Steps 1:

- *Optimal _ Solution* =null
- Initialize the particles With Liebovitch Map

Steps 2:

- Move the particles toward their corresponding *SC* With
  1. Run mutation operator of Genetic Algorithm
  2. Run *Sort _ VmAndClds* Function
  3. Run *Find _ MaxForMin* Function

  If (any particle‘ *objective function* < *SC* ‘objective function)
  { Exchange the *SC* with particle; }

Steps 3:

- Compute the total objective function
- Dummy particle(s) selection
- The particle looking for the new *SC* based on AP of the SC_s
- If (Is there any *SC* with no particles)
  { Changes this *SC* to a particle;
  The particle looking for the new *SC* based on AP of the SC_s ; }

Steps 4:

- Choose new *SCs* and their particles
- Create New Particles with:
  1. Run Genetic Algorithm
  2. Run the proposed operator
  3. Using Liebovitch Map

Steps 5:

- *Optimal _ Solution* = Best of Particles
- If (termination condition reached?)
  { Go to Step 2; }

Return *Optimal _ Solution* **;**

شکل ۴– روند اجرای عملگر الگوریتم CHSS_GA

۳. الگوریتم‌های پیشنهادی برای زمان‌بندی کارها در محیط محاسبات ابر

در این بخش به توضیح دو روش پیشنهادی برای زمان‌بندی کارها که بر پایه الگوریتم کلونی مورچه و الگوریتم ترکیبی جستجوی ابرکروی مبتنی بر نظریه آشوب و ژنتیک استوار هستند، پرداخته می‌شود. در ادامه هر یک از روش‌های مذکور توضیح داده می‌شود.

همان‌طور که در بخش ۲-۲ توضیح داده شده است، در الگوریتم CHSS_GA جمعیت اولیه‌ی الگوریتم با استفاده از مقادیر حاصل از نگاشت لیبویتچ که در رابطه (۱۳) آورده شده است، تولید می‌شود که در واقع برای تولید ذرات اولیه‌ی الگوریتم به ظرفیت و توان ماشین‌های مجازی توجه نمی‌شود و اختصاص کارها تنها با توجه به مقادیر حاصل از نگاشت لیبویتچ که یک رابطه‌ی ریاضی می‌باشد، صورت می‌گیرد. هر ذره موجود در جمعیت اولیه، یک راه حل ارائه شده برای مسئله پیش‌رو می‌باشد که بیانگر نحوه اختصاص کارها به ماشین‌های مجازی می‌باشد. در گام جستجوی الگوریتم مذکور از استراتژی جستجو متناسب با میزان اهمیت معیارهای مطرح در شبیه‌سازی استفاده می‌شود و این امر به اختصاص بهتر کارها به ماشین‌های مجازی کمک می‌کند. با توجه به آنچه بیان شد، الگوریتم پیشنهادی اول برای برطرف کردن ضعف الگوریتم CHSS_GA مبنی بر عدم توجه به ظرفیت ماشین‌های مجازی برای اختصاص کارها ارائه می‌شود. همان‌طور که پیش‌تر گفته شد، در الگوریتم ACO مورچه‌های مصنوعی توسط فرومون انباشته شده بر روی یال‌ها مسیریابی می‌کنند و با توجه به تابع احتمال آورده شده در رابطه (۲)، یال با فرومون بیشتر را انتخاب می‌کنند. به همین دلیل پس از مدتی اکثر یا تقریبا همه مورچه‌ها مسیر کوتاه تر را طی خواهند کرد، از این رو در گام اول الگوریتم CHSS_GA که به تولید جمعیت اولیه می‌پردازد، الگوریتم ACO اجرا شده و راه‌حل‌های ایجاد شده در آخرین تکرار از الگوریتم ACO به عنوان جمعیت اولیه به الگوریتم CHSS_GA داده می‌شود.

همان‌طور که در بخش ۲-۱ توضیح داده شده است، در ابتدای الگوریتم ACO به دلیل اینکه میزان فرومون موجود بر روی یال‌ها صفر یا ثابت درنظر گرفته می‌شود، انتخاب مسیر کاملا تصادفی است. سپس در تکرارهای بعدی از اجرای الگوریتم با حرکت مورچه‌های مصنوعی بر روی گراف مسئله، میزان فرومون انباشته شده بر روی یال‌ها بهنگام شده و این امر به مسیریابی بهتر مورچه‌های کمک می‌کند. الگوریتم پیشنهادی دوم برای برطرف کردن ضعف الگوریتم ACO مبنی‌بر عدم تخمین درست میزان فرومون اولیه‌ی موجود بر روی یال‌ها در شروع الگوریتم ارائه می‌شود. این الگوریتم به مسیریابی بهتر مورچه‌ها کمک کرده و باعث می‌شود مورچه‌ها در تعداد تکرار کمتری نسبت به حالت قبل به سمت مسیر کوتاه‌تر همگرا شوند. این امر به این شکل محقق می‌شود که قبل از اجرای الگوریتم ACO، الگوریتم CHSS_GA اجرا شده و به کمک راه‌حل‌های ایجاد شده توسط الگوریتم CHSS_GA، میزان فرومون انباشته شده بر روی یال‌ها تخمین زده می‌شود. این امر منجر به بهبود سرعت همگرایی شده و به مسیریابی بهتر مورچه‌ها کمک می‌کند. در ادامه هر یک از الگوریتم‌های پیشنهادی توضیح داده خواهد شد.

۳-۱. الگوریتم پیشنهادی اول ACO_CHSS_GA (F1)

الگوریتم پیشنهادی اول (F1) همانند الگوریتم CHSS_GA که در بخش ۲-۲ توضیح داده شد، از پنج گام تشکیل می‌شود، با این تفاوت که جمعیت اولیه‌ی الگوریتم $F1$ توسط الگوریتم ACO تولید می‌شود. روند الگوریتم $F1$ به این صورت است که در گام اول الگوریتم پس از مقداردهی به پارامترهای اولیه، جمعیت اولیه توسط اجرای الگوریتم ACO تولید می‌شود. برای این منظور در الگوریتم ACO به تعداد تعیین شده برای جمعیت اولیه در الگوریتم CHSS_GA، مورچه مصنوعی ایجاد می‌شود. هر مورچه با استفاده از تابع احتمال آورده شده در رابطه (۲) به انتخاب مسیر حرکت خود می‌پردازد. در ادامه مسیرهایی که توسط مورچه‌ها در آخرین تکرار از اجرای الگوریتم ACO ساخته شده‌اند، به عنوان جمعیت اولیه به الگوریتم CHSS_GA داده می‌شوند. روند اجرای الگوریتم پیشنهادی $F1$ در شکل (۵) آورده شده است.

Function ACO_CHSS_GA

1. Initialization

2. Run ACO

Input: ($num_particles$, $cloudlet_list$, Vm_list)

Output: Particles

3. Set $array_pop$ =array(Particles);

4. Run CHSS_GA

Input: $array_pop$

Output: $Best_Particle$

Set $t = 1$

Steps:

while($t < t_{MAX}$)

1. Set hyper-spheres and Particles distribution among hyper-spheres

2. Searching

3. Dummy particles recovery

4. Determining new SCs and particles

5. Convergence testing and

set Best_Particle with best of particles

End while

5. Return $Best_Particle$

شکل ۵– روند اجرای الگوریتم F1

۳-۲. الگوریتم پیشنهادی دوم CHSS_GA_ACO (F2)

در این بخش به توضیح الگوریتم پیشنهادی دوم (F2) پرداخته می‌شود. روند اجرای الگوریتم $F2$ همانند الگوریتم ACO که در بخش ۲-۱ توضیح داده شده است، می‌باشد. با این تفاوت که قبل از اجرای الگوریتم ACO، ابتدا الگوریتم CHSS_GA اجرا می‌شود تا بر اساس ذرات تولید شده در الگوریتم مذکور بتوان میزان فرومون موجود بر روی یال‌ها را تخمین زد. برای این منظور بهترین ذرات (ذراتی که دارای کمترین مقدار تابع هدف هستند) از بین ذرات ساخته شده در الگوریتم CHSS_GA انتخاب شده و به عنوان ورودی به الگوریتم ACO داده می‌شوند. همان‌طور که پیش‌تر گفته شد هر ذره دارای دو قسمت متغیرها و مقدار تابع هدف است. متغیرهای یک ذره نشان‌دهنده‌ی نحوه‌ی اختصاص کارها به ماشین‌های مجازی می‌باشند و مقدار تابع هدف یک ذره بیانگر کارایی سیستم برای راه‌حل مورد بررسی می‌باشد، به ازای هر ذره که به الگوریتم ACO داده می‌شود، یک مورچه مصنوعی ساخته می‌شود. سپس متغیرهای ذره مورد بررسی، به عنوان مسیر ساخته شده توسط مورچه درنظر گرفته می‌شود. همچنین مقدار تابع هدف ذره به عنوان طول مسیر مورچه، درنظر گرفته می‌شود. با ساخت مسیر طی شده توسط هر مورچه، نوبت به بهنگام‌سازی محلی فرومون می‌رسد. برای بهنگام‌سازی محلی فرومون انباشته شده بر روی مسیر حرکت هر مورچه، از رابطه (۱۱) استفاده می‌شود. پس از آنکه تمامی ذرات (مسیرها) تولید شده توسط الگورتیم CHSS_GA بررسی شدند و برای هر کدام یک مورچه‌ی مصنوعی ساخته شد، میزان فرومون انباشته شده بر ۱۲رساد، بدین منظور با استفاده از رابطه (می‌سازی ساراساری فرومونشاد، نوبت به بهنگام روی یال‌ها به صورت سراسری بهنگام می‌شود. پس از تخمین میزان فرومون انباشته شده بر روی یال‌ها، مورچه‌هایی که از

قبل ایجاد شده‌اند حذف شده و به تعداد تعیین شده در ابتدای الگوریتم ACO، مورچه مصنوعی ایجاد می‌شود. مورچه‌ها به صورت تصادفی بر روی ماشین‌های مجازی قرار می‌گیرند و توسط فرومون انباشته شده بر روی یال‌ها مسیریابی می‌کنند. از آنجایی که مسیریابی مورچه‌ها توسط تابع احتمال آورده شده در رابطه (۲) انجام می‌شود، همواره یال با فرومون بیشتر را انتخاب می‌کنند و پس از مدتی اکثر یا تقریبا همه مورچه‌ها مسیر کوتاه‌تر را طی خواهند کرد. روند الگوریتم پیشنهادی $F2$ در شکل (۶) آورده شده است.

Function CHSS_GA_ACO

1. Initialization
2. Run CHSS_GA
Input: ($num_particles$, $cloudlet_list$, Vm_list)
Output: Scs (hyper-spheres)
3. Set $array_pop$ =array(SCs);
4. Run ACO
Input: ($array_pop$, $cloudlet_list$, Vm_list)
Output: Best of Particles
Steps:
1. for all SCs in $array_pop$
make ant add to ant_lists
Set ant_tour = SCs
Set L_tour = Cost function of SCs
update the real-time pheromone intensity locally
End for
2. update the real-time pheromone intensity globally
3. clear(ant_lists)
4. while($t < t_{MAX}$)
for i=1 to num_ants
make ant add to ant_lists cloudlet_list
compute $P_{ij}^{k}(t)$ for taski and vmj
select max of $P_{ij}^{k}(t)$
assign taski to vmj
update the real-time pheromone intensity locally
End for
update the real-time pheromone intensity globally
Set Best_Particle = Best of ant

End while
5. Return Best_Particle

شکل ۶– روند اجرای الگوریتم F2

۴. نتایج آزمایشات و شبیه‌سازی‌ها

در این بخش کارایی الگوریتم‌های پیشنهادی $F1$ و $F2$ مورد بررسی و ارزیابی قرار می‌گیرد. برای این منظور با استفاده از الگوریتم‌های مورد بررسی به زمان‌بندی کارها برای اجرا بر روی ماشین‌های مجازی پرداخته می‌شود. شرایط درنظر گرفته شده برای انجام شبیه‌سازی از جمله تعداد مرکز داده، تعداد کارهای وارد شده به سیستم و تعداد ماشین‌های مجازی موجود در سیستم در جدول (۲) آورده شده است. شبیه‌سازی و ارزیابی الگوریتم‌های مورد بررسی در چند مرحله و با توجه به اطلاعات آورده شده در جدول (۲) انجام شده است. به منظور بررسی بهتر الگوریتم‌های پیشنهادی، در هر مرحله از شبیه‌سازی تعداد وظایف وارد شده به سیستم و تعداد ماشین مجازی موجود در سیستم، متفاوت در نظر گرفته شده است. برای شبیه‌سازی محیط محاسبات ابر از نرم‌افزار اکلیپس [ii] استفاده شده است.

جدول ۲- شرایط مدنظر برای انجام شبیه‌سازی

نوع موجودیت	پارامترها	مقدار
وظیفه	اندازه وظیفه	۳۰
	تعداد وظایف	۵۰-۱۰۰۰
ماشین مجازی	تعداد ماشین مجازی	۱۰-۳۰
	پهنای باند	۱۰۰۰
	تعداد دستور اجرا شده در هر ثانیه توسط پردازنده(MIPS)	۵۰۰-۱۰۰۰
	اندازه حافظه ماشین مجازی	۵۰۰
	تعداد پردازنده در هر ماشین مجازی	۱-۲
مرکز داده	تعداد مرکز داده	۳۰
	تعداد منابع موجود (Host)	۳
	طریقه زمانبندی ماشین‌های مجازی بر روی منابع	زمان‌بندی نوبت گردشی [iii]

شرایط درنظر گرفته شده برای الگوریتم‌های پیشنهادی و دیگر الگوریتم‌های مورد بررسی در جدول (۳) آورده شده است و می‌توان مشاهده کرد که تعداد تکرار درنظر گرفته شده در الگوریتم‌های پیشنهادی $F1$ و $F2$ که از ترکیب الگوریتم‌های CHSS و GA و ACO به دست آمده‌اند، نسبت به سایر الگوریتم‌ها مورد بررسی کمتر می‌باشد.

برای مثال در الگوریتم پیشنهادی F1 (ACO_ CHSS_GA) ابتدا الگوریتم ACO به تعداد تکرار ۵ بار اجرا شده، سپس الگوریتم CHSS_GA اجرا می‌شود. در الگوریتم مذکور ابتدا CHSS به تعداد تکرار برابر با ۵ اجرا شده و در هر بار اجرای الگوریتم CHSS، برای تولید ذرات جدید، الگوریتم GA به تعداد ذرات جدید اجرا می‌شود. لازم به ذکر است که در الگوریتم CHSS نرخ ایجاد ذرات جدید در گام چهارم (تولید ذرات جدید) برابر با ۰.۰۵ در نظر گرفته شده است و با توجه به آنکه تعداد جمعیت اولیه در الگوریتم برابر با ۱۰۰ است، این تعداد برابر با ۵ خواهد بود. در شبیه‌سازی‌های انجام شده مقدار آستانه (اختلاف بین بهترین کره از بین کره‌های موجود در دو تکرار متوالی برای خاتمه الگوریتم) در الگوریتم‌های CHSS، CHSS_GA، $(F1)$ و $(F2)$ برابر با 10^{-3} در نظر گرفته شده است. نتایج حاصل از شبیه‌سازی‌ها توسط الگوریتم‌های مورد بررسی در جدول (۴) آورده شده است.

جدول ۳- شرایط درنظر گرفته شده برای انجام شبیه‌سازی با استفاده از الگوریتم‌های مورد بررسی

شرایط	نام تابع	الگوریتم F1	الگوریتم F2	CHSS_GA	CHSS	GA	ACO
CHSS	تعداد جمعیت اولیه	۱۰۰	۱۰۰	۱۰۰	۱۰۰	-	-
	تعداد مراکز کره	۳۰	۳۰	۳۰	۳۰		
	تعداد تکرار الگوریتم	۵	۵	۱۰	۱۰		
GA	تعداد جمعیت اولیه	۱۰۰	۱۰۰	۱۰۰	-	۱۰۰	-
	تعداد تکرار الگوریتم	۵	۵	۵		۱۰۰	
	احتمال جهش	۰.۶	۰.۶	۰.۶		۰.۶	
ACO	تعداد مورچه	۱۰۰	۱۰	-	-	-	۲۰
	تعداد تکرار الگوریتم	۵	۵				۲۰
	ضریب وزن‌دهی (β)	۱	۱				۱
	ضریب تبخیر فرومون (ρ)	۰.۴	۰.۴				۰.۴
	ضریب وزن‌دهی فرومون (α)	۱	۱				۱
	ضریب وزن‌دهی تعادل بارکاری ماشین مجازی (γ)	۰.۳	۰.۳				۰.۳

جدول ۴- نتایج حاصل از زمان‌بندی کارها با استفاده از الگوریتم‌های مورد بررسی

N_Cloudlets / N_VMs	F2	F1	PSO_PGA	CHSS_GA	CHSS	ACO	GA
۵۰ / ۱۰	**۱/۱۵**	۱/۷۰	۱/۶۱	۱/۱۶	۱/۱۶	۱/۹۷	۱/۷۰
۱۰۰ / ۲۰	**۲/۱۹**	۳/۲۳	**۲/۱۹**	۲/۲۶	۳/۰۳	۳/۵۸	۳/۳۳
۵۰۰ / ۳۰	۱۰/۸۹	۱۵/۷۹	۱۱/۷۷	**۱۰/۷۲**	۱۲/۷۸	۱۶/۳۵	۱۵/۸۹
۶۰۰ / ۳۰	**۱۸/۰۸**	۱۹/۱۹	۱۸/۵۵	۱۹/۰۵	۱۹/۲۴	۱۹/۵۷	۱۹/۳۳
۷۰۰ / ۲۵	**۱۹/۶۸**	۲۲/۰۵	۱۹/۷۰	۱۸/۷۵	۱۹/۷۹	۲۱/۲۷	۲۲/۰۲
۸۰۰ / ۲۵	**۲۱/۴۶**	۲۵/۱۰	۲۱/۵۵	۲۲/۰۰	۲۲/۵۳	۲۴/۱۴	۲۵/۰۹
۱۰۰۰ / ۳۰	**۲۶/۱۶**	۳۲/۹۱	۲۶/۸۵	۲۸/۳۱	۳۰/۵۸	۳۲/۵۷	31.60

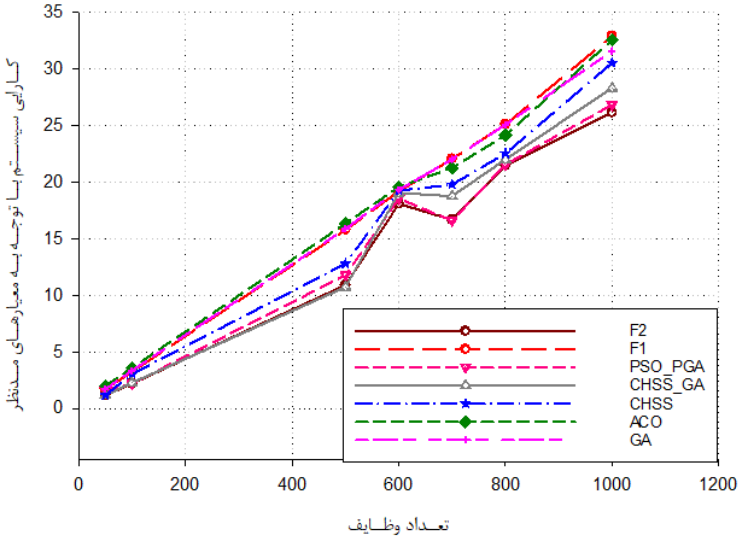
در هر مرحله از شبیه‌سازی (هر سطر از جدول (۴) به زمان‌بندی کارهای وارد شده به سیستم توسط الگوریتم‌های مورد بررسی پرداخته شده است. لازم به ذکر است که در هر یک از شبیه‌سازی‌های انجام شده، تعداد کارهای وارد شده به سیستم و همچنین تعداد ماشین‌های مجازی موجود در سیستم متفاوت در نظر گرفته شده است. برای مثال در سطر اول از جدول مذکور تعداد کارهای وارد شده به سیستم برابر با ۵۰ و تعداد ماشین‌های مجازی موجود در سیستم برابر با ۱۰ درنظر گرفته شده است. سپس شبیه‌سازی برای هر یک از الگوریتم‌های مورد بررسی انجام شده و با استفاده از رابطه‌ی (۸) کارایی سیستم محاسبه می‌شود.

به کمک بررسی نتایج حاصل از شبیه‌سازی که در جدول (۴) آورده شده است، می‌توان مشاهده کرد که:

۱. الگوریتم پیشنهادی ACO_CHSS_GA ($F1$)در مقایسه با الگوریتم‌های ژنتیک و بهینه‌سازی کلونی مورچه که برای زمان‌بندی کارها در محیط محاسبات ابر مورد استفاده قرار گرفته‌اند، عملکرد بهتری دارد.

۲. الگوریتم پیشنهادی CHSS_GA_ ($F2$) در مقایسه با الگوریتم‌های بهینه‌سازی کلونی مورچه، ژنتیک، الگوریتم جستجوی ابرکروی مبتنی بر نظریه آشوب، الگوریتم بهینه‌سازی ترکیبی با استفاده از الگوریتم ژنتیک و جستجوی ابرکروی مبتنی بر نظریه آشوب و همچنین الگوریتم پیشنهادی ACO_CHSS_GA ($F1$) نتایج بهتری را دارا می‌باشد.

نمودار شکل (۹) برای بررسی بهتر نتایج آورده شده در جدول (۴)، ترسیم شده است. بررسی نمودار آورده شده در شکل (۷) بیانگر آن است که الگوریتم پیشنهادی F2 نسبت به سایر الگوریتم‌های مورد برسی دارای عملکرد بهتری می‌باشد.



شکل ۷– نمودار نتایج حاصل از شبیه‌سازی با استفاده از الگوریتم‌های مورد بررسی

مدت زمان انجام برخی از شبیه‌سازی‌های انجام شده توسط الگوریتم‌های مورد بررسی در جدول (۵) آورد شده است. برای مثال اعداد آورده شده در ستون اول از جدول (۵) نشان‌دهنده‌ی مدت زمان اجرای الگوریتم‌های مورد بررسی برای زمان‌بندی کارهای وارد شده به سیستم است که در آن تعداد کارهای وارد شده به سیستم برابر با ۵۰ و تعداد ماشین‌های مجازی موجود در سیستم برابر با ۱۰ درنظر گرفته شده است. بررسی نتایج آورده شده در جدول (۵) بیانگر آن است که مقدار کمینه‌ی مدت زمان اجرای الگوریتم از میان الگوریتم‌های مورد بررسی متعلق به الگوریتم جستجوی ابرکروی مبتنی‌بر نظریه آشوب می‌باشد. مدت زمان اجرای الگوریتم پیشنهادی F2 تفاوت قابل ملاحظه‌ای با مقدار کمینه مدت زمان اجرا نداشته و در بدترین حالت این تفاوت حدود ۹۰ ثانیه می‌باشد. این در حالی است که با توجه به نتایج آورده شده در جدول (۴) می‌توان مشاهده کرد که الگوریتم پیشنهادی F2 برای زمان‌بندی کارها نسبت به سایر الگوریتم‌های مورد بررسی دارای عملکرد بهتری می‌باشد. در جدول‌های (۳)، (۴) و (۵) کمینه نتایج به صورت پررنگ نمایش داده شده است.

جدول ۵- مدت زمان انجام شبیه‌سازی (برحسب میلی‌ثانیه) با استفاده از الگوریتم‌های مورد بررسی

N_Cloudlet / N_VMs	۵۰ / ۱۰	۱۰۰ / ۲۰	۵۰۰ / ۳۰
CHSS_GA	۴۸۰۶۱	۶۸۹۸۰	۳۲۲۲۸۸
CHSS	**۱۱۸۴۵**	**۱۶۹۶۵**	**۹۷۲۵۸**
GA	۸۴۶۷۰	۷۹۵۰۶۰	۸۸۷۲۷۶
ACO	۲۶۱۷۸	۳۶۹۰۴۸	۱۴۵۴۰۵۸
PSO_PGA	۴۸۰۶۸	۶۸۹۸۲	۳۲۲۲۹۴
F1	۳۲۵۷۹	۴۵۶۶۳	۳۱۰۷۷۷
F2	۱۸۳۸۹	۲۶۱۰۰	۱۸۷۷۶۴

۵. نتیجه‌گیری

در این مقاله الگوریتمی برای زمان‌بندی کارها در محیط ابر ارائه می‌شود. روش پیشنهادی بر پایه الگوریتم کلونی مورچه و الگوریتم ترکیبی جستجوی ابرکروی مبتنی‌بر نظریه آشوب و ژنتیک استوار است. الگوریتم کلونی مورچه یکی از نمونه‌های موفق از سیستم‌های هوشمند گروهی می‌باشد و امروزه توجه به بسط‌های مختلف این الگوریتم از اهمیت ویژه‌ای برخوردار است. از سوی دیگر در الگوریتم جستجوی ابرکروی مبتنی‌بر نظریه آشوب و ژنتیک برای استفاده کارآمد از سیستم و بهبود عملکرد سیستم از یک استراتژی جستجو متناسب با میزان اهمیت معیارهای مدنظر بهره گرفته شده است. معیارهای مطرح برای زمان‌بندی کارها شامل بارکاری ماشین‌های مجازی، هزینه، مدت زمان انتظار و مدت زمان انجام کار می‌شود. نتایج حاصل از شبیه‌سازی بیانگر آن است که الگوریتم پیشنهادی F2 از سرعت همگرایی (تعداد تکرار کمتر) و نتایج (کارایی سیستم) بهتری نسبت به الگوریتم‌های ژنتیک، کلونی مورچه، جستجوی ابرکروی مبتنی‌بر نظریه آشوب، الگوریتم ترکیبی با استفاده از الگوریتم ژنتیک و جستجوی ابرکروی مبتنی‌بر نظریه آشوب و همچنین الگوریتم پیشنهادی F1 که برای زمان‌بندی کارها در محیط ابر مورد بررسی قرار گرفته‌اند، برخوردار است.

۶. مراجع

[1] S. A. Murad, A. J. M. Muzahid, Z. R. M. Azmi, M. I. Hoque, and M. Kowsher, "A review on job scheduling technique in cloud computing and priority rule based intelligent framework," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 2309–2331, Jun. 2022.

[2] K. Sutha and G. M. K. Nawaz, "Research perspective of job scheduling in cloud computing," *2016 Eighth International Conference on Advanced Computing (ICoAC)*, pp. 61–66, Jan. 2017.

[3] Ibrahim Attiya, Tapio Seppänen, and S. Xiong, "Job Scheduling in Cloud Computing Using a Modified Harris Hawks Optimization and Simulated Annealing Algorithm," vol. 2020, pp. 1–17, Mar. 2020.

[4] E. I. Djebbar, G. Belalem, and M. Benadda, "Task scheduling strategy based on data replication in scientific Cloud workflows," *Multiagent and Grid Systems*, vol. 12, no. 1, pp. 55–67, Mar. 2016.

[5] J. A. J. Sujana, T. Revathi, T. S. S. Priya, and K. Muneeswaran, "Smart PSO-based secured scheduling approaches for scientific workflows in cloud computing," *Soft Computing*, vol. 23, no. 5, pp. 1745–1765, Nov. 2017.

[6] N. L. Chu and N. S.-J. Wu, "A real-time decision support with cloud computing based fire evacuation system," Oct. 2011.

[7] M. A. Alsaih, Rohaya Latip, A. Abdullah, S. K. Subramaniam, and Kamal Ali Alezabi, "Dynamic Job Scheduling Strategy Using Jobs Characteristics in Cloud Computing," *Symmetry*, vol. 12, no. 10, pp. 1638–1638, Oct. 2020.

[8] N. Mansouri and M. M. Javidi, "Cost-based job scheduling strategy in cloud computing environments," *Distributed and Parallel Databases*, Jul. 2019.

[9] C.-W. Tsai and J. J. P. C. Rodrigues, "Metaheuristic Scheduling for Cloud: A Survey," *IEEE Systems Journal*, vol. 8, no. 1, pp. 279–291, Mar. 2014.

[10] Q. Liao, S. Jiang, Q. Hei, T. Li, and Y. Yang, "Scheduling Stochastic Tasks with Precedence Constrain on Cluster Systems with Heterogenous Communication Architecture," *Lecture notes in computer science*, pp. 85–99, Jan. 2015.

[11] Pinal Salot, "A SURVEY OF VARIOUS SCHEDULING ALGORITHM IN CLOUD COMPUTING ENVIRONMENT," *International Journal of Research in Engineering and Technology*, vol. 02, no. 02, pp. 131–135, Feb. 2013.

[12] H. Yao, "Cloud Task Scheduling Algorithm based on Improved Genetic Algorithm," *International Journal of Performability Engineering*, 2017.

[13] Y. Sun, J. Li, X. Fu, H. Wang, and H. Li, "Application research based on improved genetic algorithm in cloud task scheduling," *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 1, pp. 239–246, Jan. 2020.

[14] X. Huang, C. Li, H. Chen, and D. An, "Task scheduling in cloud computing using particle swarm optimization with time varying inertia weight strategies," *Cluster Computing*, vol. 23, no. 2, pp. 1137–1147, Sep. 2019.

[15] V. M. Arul Xavier and S. Annadurai, "Chaotic social spider algorithm for load balance aware task scheduling in cloud computing," *Cluster Computing*, vol. 22, no. S1, pp. 287–297, Jan. 2018.

[16] H. Karami, M. J. Sanjari, and G. B. Gharehpetian, "Hyper-Spherical Search (HSS) algorithm: a novel meta-heuristic algorithm to optimize nonlinear functions," *Neural Computing and Applications*, vol. 25, no. 6, pp. 1455–1465, Jun. 2014.

[17] X. Fu, Y. Sun, H. Wang, and H. Li, "Task scheduling of cloud computing based on hybrid particle swarm algorithm and genetic algorithm," *Cluster Computing*, vol. 26, no. 5, pp. 2479–2488, May 2021.

[18] M. A. Tawfeek, A. El-Sisi, A. E. Keshk, and F. A. Torkey, "Cloud task scheduling based on ant colony optimization," *IEEE Xplore*, Nov. 01, 2013.

[i] Hyper Heuristic
[ii] Eclipse
[iii] Round Robin

بررسی و ارزیابی معماری های شبکه های نرم افزار محور و چالش های امنیتی آنها

حامد نجفی [*۱]، رضا ابراهیمی آتانی [۲]

۱- دانشجوی دکتری شبکه، گروه مهندسی کامپیوتر، دانشکده فنی، دانشگاه گیلان

۲-دانشیار گروه مهندسی کامپیوتر، دانشکده فنی، دانشگاه گیلان

چکیده

شبکه های نرم افزار محور از دسته شبکه های نسل آینده بود که توسط گوگل و سیسکو پشتیبانی توسعه و می شود و بر پایه جداسازی فیزیکی لایه کنترل از لایه داده تعریف میگردد. به طور خاص، لایه کنترل بر روی یک کنترل کننده مرکزی اختصاصی اجرا می شود تا آن را از تمام ساختارهای اساسی شبکه جدا کند. لذا، کنترل کننده کل گراف شبکه را نظارت و مدیریت می نماید. لایه داده که شامل تجهیزات شبکه می شود وظیفه انتقال ترافیک شبکه را بر اساس قوانین حمل و نقل در جداول جریان برعهده دارد. اگر هیچ قانون متناظر برای یک بسته شبکه وجود نداشته باشد، بسته به عنوان یک پیام به کمک دستور PacketIn به کنترل کننده هدایت می شود. قوانین حمل و نقل توسط برنامه های کاربردی در حال اجرا در بالای کنترل کننده یا ماژول ها در داخل کنترل کننده تعریف می شود. در نتیجه، شبکه های نرم افزار محور یک رابط برنامه نویسی را ارائه می دهد که در آن لایه داده می تواند توسط برنامه های خارجی مدیریت شود. در این مقاله سعی داریم شرح مختصری بر شبکه های نرم افزار محور شامل پیشینه، ساختار و نحوه عملکرد آن داشته باشیم سپس شرح مختصری بر معماری آن و روشهای مختلف پیاده سازی های آن (متمرکز ، غیر متمرکز و ترکیبی) ارایه خواهد شد و همچنین چالشهای پیش روی هر یک از این معماری ها بررسی خواهد شد، سپس ساختار امنیتی این شبکه ها بررسی و چالشهای پیش روی آنها مورد بحث قرار خواهد گرفت.

کلمات کلیدی: SDN، Open Flow، Any API's ، پروتکل های ارتباطی ، صفحه کنترل ، صفحه ارسال.

۱. مقدمه

شبکه‌های نرم‌افزار محور (SDN [۱]) یک معماری شبکه است که از تجهیزات سخت‌افزاری جداگانه برای کنترل ترافیک داده‌ها و مدیریت شبکه استفاده می‌کند. در این معماری، کنترل شبکه به صورت مرکزی انجام شده و از طریق نرم‌افزارها و الگوریتم‌های خاص صورت می‌گیرد. این رویکرد امکان ایجاد شبکه‌های انعطاف‌پذیر، قابل برنامه‌ریزی و قابل تنظیم را فراهم می‌کند. SDN توسط پروتکل ارتباطی OpenFlow و همچنین نرم‌افزارهای کنترل‌کننده دیگری مانند Floodlight یا OpenDaylight پشتیبانی می‌شود. این فناوری امکانات بسیاری را از جمله توزیع دینامیک ترافیک، افزایش امنیت شبکه، افزایش کارایی و کاهش هزینه‌ها را برای مدیریت شبکه فراهم می‌کند. با استفاده ازSDN، شرکت‌ها و سازمان‌ها قادر به اجرای سرویس‌های شبکه مختلف با سرعت و انعطاف‌پذیری بالا هستند. همچنین، SDN امکانات بسیاری را برای افزایش کارایی شبکه و بهینه‌سازی مصرف منابع شبکه فراهم می‌کند همچنین با توجه به مزایای بسیاری که SDN ارائه می‌دهد، استفاده از این فناوری در صنعت شبکه و ارتباطات به سرعت در حال گسترش است و در آینده نقش مهمی در توسعه شبکه‌های هوشمند و پویا خواهد داشت.

۲. معرفی مفهومی شبکه های نرم افزار محور

* **Corresponding author:** حامد نجفی دانشجوی دکتری شبکه گروه مهندسی کامپیوتر دانشگاه گیلان

[1] Software Defined Networking

شبکه های SDN قابلیت های کنترل بر شبکه های سنتی را به کمک اجرای ساختار مبتنی بر جریان در لایه داده افزایش داده اند. بطوریکه چندین فیلد سرآیند مشخص می کند که چگونه بسته ها باید در شبکه حرکت کنند. درمقابل در شبکه های کلاسیک مبتنی بر TCP/IP آدرس IP مقصدنقش کلیدی و تعیین کننده ای در مسیریابی ها دارد. بنابراین، کنترل کنندهSDN می تواند تمایز ترافیکی بهتری را بر اساس چندین فیلد سرآیند انجام دهد.

یکی دیگر از ویژگی هایی که SDN را از شبکه های سنتی متمایز می کند این واقعیت است که شامل تکنیک های خود بازپیکربندی است. به عنوان مثال، قوانین شرطی را می توان بر روی سوئیچ ها توسط کنترل کننده اجرا نمود که اگر شرایط خاصی برآورده شود، فعال گردد. این قوانین مشروط مربوط به آمار جمع آوری شده توسط سوئیچ ها است و بیان می کند زمانی که شرایط مشخص شده مواجه می شود سوئیچ چگونه باید واکنش نشان دهد. واکنش می تواند رها کردن بسته ها یا هدایت آنها باشد و انعطاف پذیری خودکار در برابر حملات را فراهم کند. این جوانب مثبت امنیتی در جدول (۱) خلاصه شده است. یکی از مزایای اصلی SDN ها کاربرد این شبکه ها در مدیریت مراکز داده می باشد [۱]. در دیدگاه اول مدل SDN باعث می شود تغییرات سیاست های شبکه کمتر مستعد خطا باشد، زیرا کلیه فرآیندها مبتنی بر توسعه های نرم افزاری است. علاوه بر این برنامه کنترل می تواند به طور خودکار به هر گونه تغییر در وضعیت شبکه واکنش نشان دهد و در انتها توسعه توابع پیچیده شبکه را بصورت ساده شده اجرایی نماید.

جدول(۱):برتری های شبکه های SDN نسبت به شبکه های سنتی

ویژگی های SDN	بهبود وضعیت شبکه	بهبود امنیتی
ایجاد دید کلی از شبکه	در اختیار داشتن داده های آماری مفید شبکه	قابلیت تشخیص نفوذ خودکار در سراسر شبکه
تواناییهای کنترلی بهتر	ارسال بسته مبتنی بر جریان	کنترل دسترسی
توانایی خود ترمیمی	وجود قوانین شرطی ، وجود آمارهای آنی در سویچ ها	امکان Redirect و Drop بسته ها

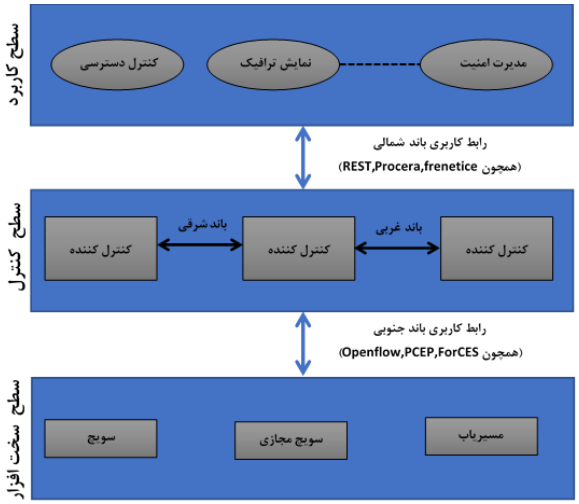
اما یکی از چالش های مهم و جنبه منفی شبکه‌های SDN به ارث بردن بیشتر آسیب‌پذیری‌های شبکه‌های با ساختار مدیریت سنتی یا اینترنتی است. علاوه بر این، SDN تحت تاثیر آسیب‌پذیری‌های جدیدی نیز از طریق معماری منحصربه‌فرد و پیاده‌سازی پروتکل جنوب/شمال[۲] خود خواهد بود. نمونه‌هایی از آسیب‌پذیری‌ها شامل موارد مربوط به سیستم‌عاملی است که کنترل‌کننده را اجرا می‌کند، جعل قوانین جریان باز [۲،۳] و ناهنجاری های حاصل از عدم بکارگیری IPSec [۳]، و DoS/Spoofing/Hacking کنترل‌کننده‌ها خواهد بود که در ادامه تشریح خواهد شد. علاوه بر این، API باند شمالی (northbound API) در صورتی که به درستی ایمن نشود یک خطر جدی امنیتی به شمار می روند. کلیه این عوامل با عدم تجربه توسعه دهندگان و کاربران در این دامنه همراه خواهد شد که احتمال پیکربندی اشتباه را نیز افزایش می دهد. علاوه بر این، SDN به دلیل کنترل متمرکز و قابلیت برنامه‌ریزی، امنیت فیزیکی محدود و تهدیدات ناشی از گره‌های در معرض خطر در داخل شبکه، خود را در معرض حمله های جدیدی نیز در مقایسه با توپولوژی‌های شبکه سنتی قرار می‌دهد. تمرکز اصلی در این مقاله ارائه مروری بر انواع مختلف نگرانی‌ها و فرصت‌های امنیتی در شبکه های مبتنی بر نرم افزار و بررسی تهدیدات پیرامون این شبکه خواهد بود.

۳. معماری کلی شبکه های SDN

در شکل (۱)، طرحی از معماری SDN، لایه های مختلف و پروتکل های ارتباطی ارایه شده است که پایه هر شبکه SDN بر آن استوار است. هر یک از صفحات داده و کنترل [۳]در این معماری وظیفه جداگانه ای را بر عهده دارند و توسط چندین ماژول کاربردی روی کنترل متمرکز متمرکز می شوند. ممکن است بیش از یک کنترل کننده به خصوص در شبکه های بزرگ وجود

[2] North/South Band Protocol
[3] Data & Control Plane

داشته باشد. این کنترلرها وظایف خود را از طریق API های شرق/غرب [۴]همگام می کنند. صفحه داده از طریق API باند جنوب به صفحه کنترل متصل می شود.



شکل(۱) : معماری شبکه های مبتنی بر نرم افزار

۳-۱. شبکه های قابل برنامه ریزی

زمانی که اینترنت برای اولین بار معرفی شد، منشأ آن در شبکه‌سازی فعال[۵] بود و هدف ازآن، از اواسط دهه ۱۹۹۰ تا اوایل دهه ۲۰۰۰، معرفی یک API شبکه بود که به مدیران شبکه اجازه می‌داد منابع موجود در دستگاه‌های شبکه، مانند سوئیچ‌ها و روترها را کنترل کنند. شبکه‌سازی فعال به دو مدل برنامه‌ریزی تبدیل شد:

(۱) مدل روتر/سوئیچ قابل برنامه‌ریزی: که در آن یک برنامه نرم افزاری خاص بر روی گره‌های شبکه و طریق مکانیسم‌های خارج از باند اجرا شده و تبادل اطلاعات مینماید [۴]. (هوش توزیع شده)

(۲) حالت کپسوله : که در آن کد اجرایی گره های شبکه از طریق بسته های داده حمل می شود [۵].(هوش متمرکز)

آنچه که انگیزه ظهور شبکه‌های برنامه ریزی شده بود، تکثیر جعبه‌های میانی[۶] بود که به طور جداگانه مستقر شدند و بر اساس هر تامین کننده تجهیزات شبکه (Vendor) به‌طور متفاوتی برنامه‌ریزی شوند.

۳-۲. تاریخچه تحولات SDN :

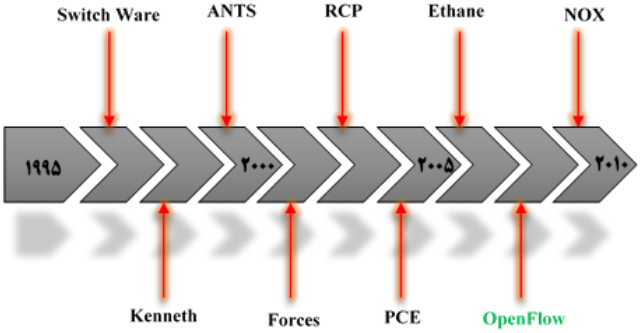
OpenFlow و سیستم عامل شبکه (NOS) آخرین نوآوری هایی بودند که منجر به تولد SDN شد که از سال ۲۰۰۷ تا ۲۰۱۰ ادامه یافت. SDN با پروژه ۴ بعدی (4D)[۶] شروع شد که از چهار لایه زیر تشکیل شده است:

- صفحه داده[۷] که ترافیک را بر اساس قوانین حمل و نقل خاص خود هدایت میکند.
- صفحه کشف[۸] برای جمع آوری آمار ترافیک شبکه و اطلاعات توپولوژی شبکه.
- صفحه انتشار [۹]برای نصب قوانین مدیریت ترافیک؛

[4] east/west-bound API
[5] Active Networks
[6] middle-box
[7] data plane
[8] discovery plane
[9] Plane disemination

- صفحه تصمیم [10] که نشان دهنده کنترل کننده متمرکز شبکه است.

SANE [۶] و Ethane [۷] با استفاده از معماری سطح بالای معرفی شده توسط پروژه 4D و اعمال آن در عملکردهایی غیر از مسیریابی مانند کنترل دسترسی، گامی فراتر به سوی معرفی OpenFlow API و سوئیچ ها برداشتند. تاثیر فوری معرفی OpenFlow نوآوری کنترل کننده های متمرکز به نام سیستم های عامل شبکه بود که امکان توسعه برنامه های کاربردی کنترلی را فراهم کرد. OpenFlow استقرار سوئیچ را ساده کرد و به دلیل ماهیت قابل برنامه ریزی سوئیچ ها در مقایسه با سوئیچ های سنتی، منجر به پذیرش آن در تحقیقات دانشگاهی و صنعت شد. شکل (۲) جدول زمانی تاریخچه شبکه قابل برنامه ریزی را از سال ۱۹۹۵ تا ۲۰۱۰ نشان می دهد.



شکل (۲) : ارایه روند تکاملی شبکه های قابل برنامه ریزی

۳-۳. تاریخچه Openflow

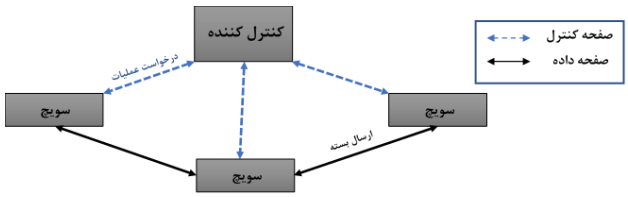
OpenFlow در اولین استاندارد SDN منتشر شده بود و قبل از اینکه به طور گسترده توسط توسعه دهندگان شبکه به کار گرفته شود، چندین تجدید نظر را پشت سر گذاشته است. در این بخش تاریخچه شبکه های قابل برنامه ریزی قبل از OpenFlow را به اختصار توضیح می دهیم. از اواسط دهه ۱۹۹۰ تا اوایل دهه ۲۰۰۰، شبکه های فعال برای گنجاندن توابع قابل برنامه ریزی در شبکه برای حمایت از نوآوری بهتر ارائه شدند. از سال ۲۰۰۱ تا ۲۰۰۷، تلاش های مختلفی برای جداسازی صفحات داده و کنترل با ایجاد یک رابط باز بین آنها انجام شد. در اواسط دهه ۲۰۰۰، آزمایش شبکه در مقیاس بالاتر برای به کارگیری ایده جداسازی صفحه کنترل از داده با معرفی OpenFlow API و سیستم‌های عامل شبکه ظاهر شد. در مارس ۲۰۰۸، مفهوم اصلی OpenFlow در یک مقاله سفید[11] از تیم تحقیقاتی Clean State از دانشگاه استنفورد ارائه شد. یک ماه بعد، با توجه به اهمیت کار، مقاله به عنوان یک یادداشت سرمقاله در ACM SIGCOMM Computer Communication Review ظاهر شد. طراحی OpenFlow API [۱۲] با ایجاد پلتفرم‌های کنترل‌کننده مانند NOX [۱۰] دنبال شد که امکان ایجاد چندین برنامه کنترلی را فراهم کرد. مستقیماً پس از معرفی اولین مشخصات سوئیچ OpenFlow در دسامبر ۲۰۰۹، علاقه بیشتری بنسبت به آن در بازار شبکه بوجود آمد. در آوریل ۲۰۰۹، NEC اولین سوئیچ تجاری با پشتیبانی داخلی OpenFlow را راهی بازار کرد. علاوه بر این، شرکت هایی مانند Big Switch، Vello، Plexxi و Pica8 شروع به ارائه راه حل های آماده برای SDN کردند. در سال ۲۰۱۱، گوگل اعلام کرد که از SDN در ستون فقرات[12] خود استفاده می کند. در همان سال، بنیاد شبکه‌های باز Open Networking Foundation (ONF) [۱۴] توسط دویچه تلکام، مایکروسافت، گوگل، فیس‌بوک، ورایزون و یاهو تأسیس شد تا مفهوم و عملکرد شبکه‌های مبتنی بر SDN و

[10] decision plane
[11] White Paper
[12] Backbone

OpenFlow را با استانداردسازی OpenFlow ترویج کند. در حال حاضر، ONF بیش از ۹۵ عضو از جمله فروشندگان عمده تجهیزات شبکه دارد.

٤. معماری و اجزای SDN

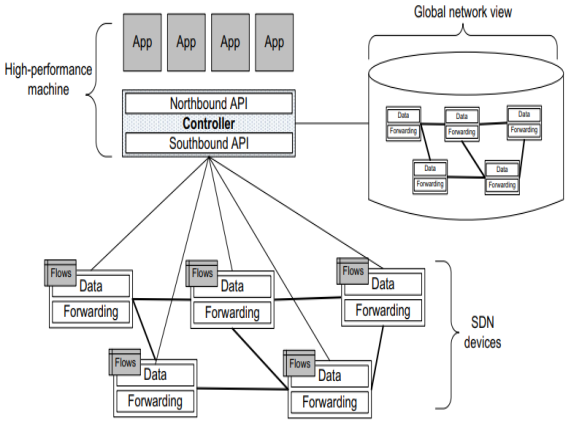
با توجه به ONF معماری SDN شامل دو صفحه با رابط های مربوطه است[۱۵] که در شکل (۳) نشان داده شده است. لایه Application شامل برنامه ها و خدمات متنوعی مانند متعادل کننده بار، بازرسی عمیق بسته (DPI)[۱۳] کنترل های دسترسی سیستم تشخیص (IDS) و سیستم پیشگیری از نفوذ (IPS) است. این لایه از طریق یک رابط برنامه نویسی کاربردی API (ارتباط شمالی)[۱۴] [۱۶] با لایه کنترل ارتباط برقرار می کند. لایه کنترل که به لایه مرکزی نیز معروف است از کنترل کننده ها تشکیل شده است و مغز SDN ها محسوب می شود و وظیفه ایجاد و خاتمه جریان ها، نظارت بر شبکه و برنامه ریزی رفتار تجهیزات فیزیکی را بر عهده دارد. لایه صفحه داده به عنوان لایه زیرساخت شناخته می شود شامل تجهیزات حمل و نقل مانند سوئیچ ها، روترها و سایر تجهیزات خواهد بود . این لایه عملیات مدیریت کنترل کننده ها را از طریق سوئیچ های فعال SDN برای هدایت داده ها، جمع اوری اطلاعات شبکه و ارسال ان به کنترل کننده اجرا می کند. لایه داده با لایه کنترل از طریق رابط جنوبی[۱۵] متصل می شود [۱۶]. شایان ذکر است که ارتباطات جنوب را می توان در دو سناریوی مختلف در نظر گرفت: (۱) درون باند که در این مورد، ارتباط بین کنترل کننده و رابط فیزیکی بستگی به قوانین جریان یا همان نقشه ترافیکی کل سیستم دارد. (۲) خارج از باند که ارتباطات جنوب از طریق مسیری که تحت تاثیر قوانین جریان SDN قرار نمی گیرد، اما از طریق پیکربندی VLAN دستگاه های شبکه را بدون قوانین OpenFlow همانطور که در شکل (۳) نشان داده شده است از یکدیگر تفکیک می کند.



شکل(۳) :معماری لایه ها در SDN

پذیرش این معماری لایه ای مزایای بسیاری را ارائه می دهد، ابتدا جداسازی صفحه ها انعطاف پذیری مورد نظر را برای ترکیب مزایای مجازی سازی سیستم و محاسبات ابری فراهم می کند. دوم، تمرکز اطلاعات اجازه می دهد تا یک دیدگاه کامل از شبکه ایجاد گردد که در تصمیم گیری و بهبود مدیریت شبکه بسیار اثر بخش خواهد بود. در نتیجه، SDN می تواند یک راه حل برای سرویس های متنوع امنیتی باشد که در کل میتواند از سیستم اطلاعاتی محافظت می کنند. در شکل (۴) شمای کلی اتفاقات رخ داده در یک شبکه SDN را در نمای کلی مشاهده مینمایید.

[13] deep packet inspection
[14] Northbound communication
[15] Southbound interface



شکل(۴) :نمای کلی ارتباطات درSDN

۵. پروتکلهای ارتباطی (API) لایه ها

رابط های جنوبی

OpenFlow و OpFlex اولین پروتکل های SDN هستند که ارتباط بین لایه کنترل و لایه های نرم افزار و لایه داد را تعریف کردند. تفاوت کلیدی بین این دو پروتکل این است که OpenFlow در مقایسه با OpFlex که نیاز به نصب عامل ها[۱۶] دارد، بدون عامل است. همانطور که در شکل (۱) مشاهده مینمایید OpenFlow ارتباط بین یک یا چند سرور کنترل را با سوئیچ تعریف می کند همچنین OpenFlow استاندارد بالفعل برای SDN است که توسط بنیاد شبکه باز (ONF) Open Networking Foundation استاندارد شده است [۱۴] و از انواع API های نوع جنوبی است. کنترلر از طریق یک API شمالی به برنامه ها (به عنوان مثال برنامه های مدیریت SDN) متصل می شود. ONF یک گروه کاری رابط Northbound راه اندازی کرده است اما هیچ API استاندارد شده واقعی از نوع شمالی برای آن وجود ندارد. قوانین راه اندازی شده روی سوئیچ OpenFlow توسط یک برنامه کنترل کننده، رفتار سوئیچ را به عنوان سوئیچ، روتر، مترجم آدرس شبکه، فایروال و غیره تعریف می کند. سوئیچ OpenFlow دارای یک یا چند جدول از قوانین مدیریت بسته است. هر قانون دارای یک الگو، لیستی از اقدامات (به عنوان مثال حذف، سیل، ارسال، اصلاح یک فیلد سرصفحه، یا ارسال بسته به کنترل کننده) و اولویت برای تمایز بین قوانین با الگوهای همپوشانی است. هنگامی که یک سوئیچ OpenFlow یک بسته را دریافت می کند، قانون تطبیق با بالاترین اولویت را شناسایی می کند، اقدامات مربوطه را انجام می دهد و شمارنده ها را افزایش می دهد.

پروتکل OpenFlow شامل سه نوع مختلف پیام است:

پیام هایی که توسط کنترلر به سوییچ ارسال می شود (دست دادن[۱۷]، پیکربندی جدول جریان، پیکربندی سوئیچ و غیره)

پیام های ناهمزمان ارسال شده توسط سوئیچ به کنترل کننده (packet-in) (مثل پیام وضعیت پورت، پیام حذف جریان)

پیام‌های متقارن را می‌توان توسط کنترل‌کننده یا سوئیچ ارسال کرد (Echo Request/reply، Hello، Experimenter)

یکی دیگر از جایگزین‌های رابط جنوبی، ForCES [۱۸] است[۱۷و۱۸] که توسط IETF استاندارد شده است. ForCES عملکردهای جداگانه کنترل و صفحه داده را تعریف می کند و در قالب های قدرتمندتر و انعطاف پذیرتر از OpenFlow به کمک مدیریت مکانیسم های پیچیده حمل و نقل ، ارائه مینماید. همچنین SoftRouter [۱۹] می تواند نقش رابط جنوبی را ایفا نموده و اقدام به جداسازی صفحه داده و سطوح کنترل نماید و اتصالات دینامیکی بین عناصر داده و

[16] Agents
[17] handshake
[18] Forwarding and Control Element Separation

عناصر صفحه کنترل را فراهم نماید. استانداردهای دیگر عبارتند از پروتکل پیکربندی شبکه (NetConf)، Locator/ID Separation Protocol (Lisp) که توسط ONF استاندارد شده و Path Computation Element(PCE) .

رابط های شمالی

بطور کلی یک API جهانی استاندارد شده Northbound بین کنترل‌کننده و برنامه‌های کاربردی تجاری وجود ندارد زیرا به شکل و فراوانی اطلاعات مبادله شده بین شبکه و برنامه های کاربردی بستگی دارد و بنابراین API های جهانی استاندارد شده مفیدی برای نوع شمالی وجود ندارد. در جدول (۲) رابط های اصلی SDN را خلاصه می کند.

جدول (۲): رابط های اصلی SDN

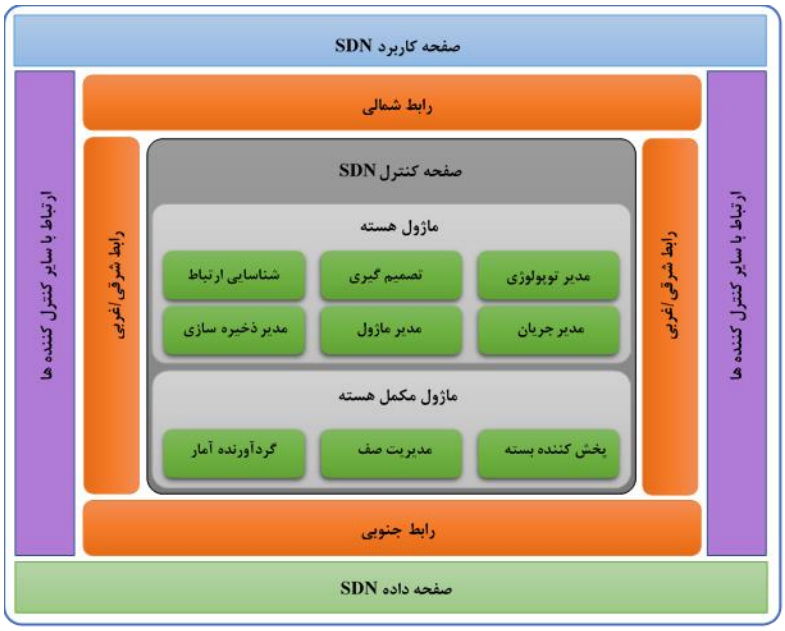
رابط ها	مشروح عملکرد	نمونه ها
رابطهای کاربری شمالی	این رابط های کاربری دارای قابلیت برنامه ریزی بوده و برای ارتباط بین کنترل کننده SDN و لایه کاربرد بکار میروند	Floodlight rest , OpenStack , Vyatta
رابط های کاربری جنوبی	این رابط های کاربردی برای ارتباط بین کنترل کننده لایه کنترل و لایه سخت افزار کاربرد داشته و به دو صورت عمومی و اختصاصی عمل خواهد نمود.	OpenFlow,ForCES,NetConf,LIPS,PCE
رابط های کاربری شرقی	این رابط ها تجمیع بین IP های شبکه های تجاری و شبکه SDN کابرد دارد	ALTO
رابط های کاربری غربی	این رابط ها معماری توزیع شده SDN را مدیریت نموده و برای ارتباط بین دو کنترل کننده SDN در دو دامنه مختلف بکار خواهند رفت	Hyperflow

صفحه کنترل در SDN

در این بخش، به شرح مختصری از لایه کنترل SDN، معماری های لایه کنترل و پارامترهای عملکرد از جمله مقیاس‌پذیری، قابلیت اطمینان، سازگاری و امنیت مورد استفاده برای ارزیابی کنترل‌کننده‌های مختلف SDN پرداخته خواهد شد.

ساختار لایه کنترل

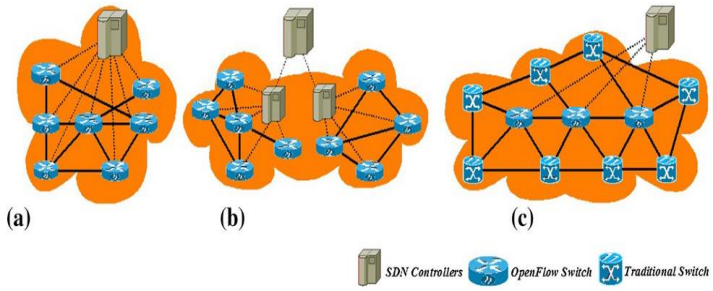
لایه کنترل SDN به عنوان یک لایه رابط بین مدیریت و صفحه داده عمل می کند و نقش مهمی در کنترل و نظارت بر شبکه دارد. کنترل شبکه شامل برنامه ریزی دستگاه های ارسال کننده (تجهیزات شبکه) به کمک دستورالعمل های سیاستی تعریف شده توسط برنامه های کاربردی در سطح مدیریت است. همچنین، در نظارت بر شبکه، صفحه کنترل اطلاعات آمار جریان ترافیک را از تجهیزات صفحه داده بازیابی می کند که می تواند توسط برنامه های مختلف قابل استفاده در صفحه مدیریت، مانند مهندسی ترافیک، امنیت و غیره تجزیه و تحلیل شود. غالباً صفحه کنترل شامل یک سخت افزار عمومی است که یک سیستم عامل شبکه (NOS) را اجرا می کند که متشکل از نرم افزارهای کنترلی اساسی است که برای راه اندازی و مدیریت یک شبکه ضروری است و یک نمایش کلی از تمام شبکه را برای برنامه ها فراهم می کندو همچنین برنامه نویسی شبکه را با پنهان کردن جزئیات پیاده سازی و منطق کنترل پیچیده آن، مانند سیستم عامل یک رایانه شخصی، ساده می کند. برخی از ماژول های اصلی که معمولا در NOS های مختلف یافت می شوند در شکل (۵) نشان داده شده اند.



شکل(۵) : معماری ماژولار نرم افزار های شبکه ای (NOS)

مدلهای مختلف SDN بر اساس صفحه کنترل(Hybrid SDN)

به طور خلاصه، کنترلر SDN قابلیت برنامه ریزی، مجازی سازی، نظارت متمرکز و کنترل پویا شبکه را فراهم می کند. ارائه تمام عملکردها در یک نقطه مرکزی واحد، کار یک اپراتور شبکه را ساده می کند و مدیریت کارآمد شبکه را ممکن می سازد. با این حال، در شبکه‌های چند دامنه‌ای یا در شبکه‌های مقیاس بزرگ، یک کنترل‌کننده ممکن است با مشکلات مقیاس‌پذیری و کنترل تاخیر مواجه شود. در چنین حوزه هایی، به جای یک صفحه کنترل SDN متمرکز، از یک صفحه کنترل SDN متمرکز به صورت فیزیکی توزیع شده اما منطقاً متمرکز استفاده می شود. علاوه بر این، پیاده سازی پارادایم های SDN با تعداد زیاد دستگاه قدیمی(سنتی و عدم پشتیبانی از SDN در آنها) که در سطح جهانی مستقر شده‌اند و شرکت‌های اختصاصی که به دلیل هزینه و محدودیت‌های فنی به سختی حاضر به تغییر ساختار محصولات خود میشوند ، غیرممکن به نظر می‌رسد. این عوامل ما رامجبور به استفاده از یک رویکرد جدید برای معرفی امکان برنامه‌پذیربودن شبکه و یا استفاده از دستگاه‌هایی که از پروتکل OpenFlow پشتیبانی کنند در یک شبکه سنتی (TN) می‌شوند. چنین سناریوی شبکه‌ای که در آن مجموعه ای ترکیبی از دستگاه‌های قدیمی و پشتیبانی کننده از OpenFlow وجود دارد، به عنوان Hybrid SDN یا SDN انتقالی و کنترل‌کننده‌ای که برای مدیریت چنین شبکه‌ای استفاده می‌شود، به عنوان کنترل‌کننده SDN ترکیبی نام برده میشود [۲۱، ۲۲]. بنابراین، در SDN ، می‌توانیم یک کنترل‌کننده SDN متمرکز واحد، کنترل‌کننده‌های SDN با توزیع فیزیکی اما منطقی متمرکز یا کنترل‌کننده SDN هیبریدی داشته باشیم که در شکل(۶) نشان داده شده است.



شکل (۶) : انواع SDN از لحاظ نوع لایه کنترل : a : صفحه کنترل متمرکز b : صفحه کنترل غیر متمرکز c:صفحه کنترل هیبرید

با توجه به انواع شبکه های نرم افزار محور فوق الذکر میتوان پارامتر های اصلی بررسی ارزیابی را بصورت زیر معرفی و به بررسی تاثیر هر یک از آنها در کارایی کل سیستم پرداخت.

سطح کنترل متمرکز

اولین بار با پیدایش ابزارهای اولیه پیاده سازی شبکه های مبتنی بر نرم افزار همچون NOX [۱۰] کنترل کننده های متمرکز پدید آمد و پس از آن تعدادی از کنترل کننده های متمرکز دیگر نیز برای SDN پیشنهاد گردید. در ادامه همانطور که در شکل (۷) مشاهده میشود، مزایا و معایب، چالش‌های تحقیقاتی صفحه کنترل متمرکز SDN را بررسی نموده و کنترل‌کننده‌های متمرکز SDN برجسته و پرکاربرد را تحلیل مینماییم.

مزایا و معایب متمرکز بودن صفحه کنترل :

مزایا: بر خلاف کنترل توزیع شده قدیمی، که در آن هر دستگاه دانش محدودی از شبکه را دارا میباشد، یک کنترل کننده متمرکز واحد در SDN دارای اطلاعات کل توپولوژی شبکه، جریان های ترافیک و بار سوئیچ استو همچنین کنترلر SDN متمرکز فیزیکی کل شبکه را نظارت و مدیریت می کند. به همه دستگاه‌های ارسال‌کننده یا درون باند (in-band) یا خارج از باند(out-of-band) متصل باقی می‌ماند و می‌تواند مسیرهای بهینه را برای جریان ترافیک در سراسر شبکه تعریف کند.

چالشها: شبکه‌های ارائه‌دهنده خدمات شامل تعداد محدودی از گره‌ها هستند که در یک منطقه جغرافیایی گسترده توزیع شده‌اند. استفاده از یک کنترل‌کننده SDN متمرکز در چنین شبکه‌ای ممکن است با مشکلات تاخیر در کنترل و پهنای باند بالا مواجه شود. از سوی دیگر، در مراکز داده چند کاربره[19] ، که ماشین‌های مجازی (VM) به سرعت افزایش و کاهش می یابند، ده‌ها هزار عنصر شبکه برای اتصال چنین ماشین‌های مجازی مورد نیاز است.در [۲۴] ویژگی های ترافیک مراکز داده متنوع را که در مقیاس متفاوت هستند مطالعه گردیده و مشاهده شد که حتی برای ۱۰۰ سوئیچ لبه، کنترل کننده ممکن است با ۱۰ میلیون درخواست تنظیم جریان در ثانیه مواجه شود. برای رسیدگی به چنین درخواست‌هایی، پیشنهاد شد که از موازی‌سازی در یک کنترل‌کننده مرکزی استفاده شود یا چندین کنترلر در شبکه راه‌اندازی شود

کنترلر متمرکز

NOX [۲۶] یک سیستم عامل شبکه مبتنی بر رویداد و اولین نسل این نوع سیستم عامل می باشد که می تواند 30K درخواست جریان در ثانیه را مدیریت کند. این کنترل‌کننده در شرکت‌های کوچک، شبکه‌های خانگی یا شبکه‌های دانشگاهی قابل استفاده است و برای محیط‌هایی که درخواست‌های تنظیم جریان بالارا همچون مراکز داده ایجاد می‌کنند مناسب نخواهد یود [۲۷]. شبکه های Nicira جانشینان NOX را توسعه داده است، مانند NOX-MT که یک NOX چند رشته ای است تا عملکرد بهتری را نسبت به حالت تک رشته ای ارائه نماید. از سوی دیگر، POX [۲۸] که بسیاری از ویژگی های خود را از NOX به ارث برده است، محیط توسعه اپلیکیشنهای کاربردی بهتری را برای برنامه نویسان فراهم می کند.

Maestro [۳۰] یک کنترل کننده چند رشته ای مبتنی بر جاوا است که می تواند درخواست های جریان 60k را در ثانیه (rps) اداره نماید، اما هنوز هم از الزامات تحمیل شده توسط یک مرکز داده بزرگ (بیش از ۱۰ میلیون rps) دور است. این نوع کنترلز ها برای یک دامنه کوچک بهینه شده اند که شامل چهار برنامه اصلی یعنی کشف، مسیریابی درون دامنه، احراز هویت و جریان مسیر است. مانند NOX، Maestro نیز زمانی که یک سرآیند OpenFlow ناقص دریافت می کند، دچار خطا شده و در برابر حملات امنیتی بسیار اسیب پذیر است.

Floodlight یکی دیگر از کنترلر های چند نخی [20]محبوب مبتنی بر جاوا در شبکه های سوئیچ بزرگ میباشد[۳۱]. اما جمعی از محققان برجسته در [۳۲] ار تحمل پذیری پایین و چالشهای امنیتی فراوان در آن گزارش داده اند. انها همچنین

[19] Multitenant data centers
[20] multi-threated

گزارش داده اند که این کنترل کننده به طور ذاتی در برابر حملات DoS اسیب پذیر است. برای غلبه بر چنین مسائل امنیتی، نسخه دیگری از Floodlight به نام SE-Floodlight توسط Big Switch Networks منتشر شده است. این نسخه پیشرفته امنیتی هنوز محدودیت نقطه شکست[21] را دارد. با این حال، با توجه به قابلیت های ظاهری و مزایای عملکرد [۳۳]، کنترل کننده Floodlight منبع باز به طور گسترده ای برای ساخت معماری های توزیع شده SDN مانند ONOS [۳۴]، DISCO [۳۵] و غیره استفاده شده است.

Ryu [۳۶] یک کنترلر SDN مبتنی بر مولفه است که در پایتون با استفاده از gevent wrapper در غالب libewent توسعه یافته است. این کنتزلر از رابط های کاربری مختلف باند شمالی از جمله OpenFlow (همه نسخه ها)، Netconf، OF-config و غیره پشتیبانی می کند. همچنین یک محیط توسعه برنامه کاربردی مناسب برای توسعه دهندگان فراهم نموده است و دارای ماژولی به نام Ryu BGPSpeaker است که می تواند برای نوشتن برنامه های BGP جهت تعریف جریان های بین دامنه ای گسترش یابد. از سوی دیگر، MUL [۳۷] نیز یک کنترل SDN چند رشته ای است که به زبان C با استفاده از سرویس های libewent و glib نوشته شده است. در ادامه و در جدول شماره ۳ ویژگیهای عمده و پارامترهای امنیتی کنترلر های برجسته بصورت مقایسه ای بررسی شده است.

سطح کنترل توزیع شده

در چند سال اخیر، صفحه کنترل SDN توزیع شده فیزیکی مورد توجه جامعه تحقیقاتی قرار گرفته است و تعدادی از چارچوب های کنترل SDN توزیع شده پیشنهاد شده است. در این بخش، مزایا و معایب، چالش‌های تحقیقاتی در صفحه کنترل SDN توزیع‌شده را بررسی و کنترل‌کننده‌های مختلف SDN توزیع‌شده را تحلیل مینماییم.

مزایا : صفحه کنترل SDN توزیع شده با معرفی چندین کنترلر در یک SDN بر مقیاس پذیری، قابلیت اطمینان، عملکرد و مشکل شکست نقطه ای صفحه کنترل متمرکز غلبه می کند. صفحه کنترل توزیع شده قوی تر، مقیاس پذیرتر و پاسخگوتر از نوع متمرکز خود است که می تواند به طور موثر به رویدادهای مختلف شبکه مانند خرابی پیوند، درخواست های تنظیم جریان جدید[22]، نفوذ و غیره واکنش نشان دهد. معماری صفحه کنترل توزیع شده راه حل های انعطاف پذیر و مقیاس پذیر را برای مدیریت چنین رویدادهایی ارائه می دهد.

چالشها : به همین ترتیب در شبکه های WAN، قرار دادن کنترل کننده های شبکه در نقاط استراتژیک می تواند پاسخدهی سریع و مشاهده مداوم تغییرات شبکه[23] را تسهیل کند. برای داشتن زمان پاسخ و عملکرد بهتر، کنترل‌کننده‌های SDN توزیع‌شده از مکانیسم‌های اشتراک بار برای توزیع سوئیچ‌های صفحه داده در بین نمونه‌های کنترل‌کننده استفاده می‌کنند. با این حال، متعادل‌سازی بار انعطاف‌پذیر شامل اشتراک‌گذاری مداوم حالت ارتباط سربار بین کنترل‌کننده‌های توزیع‌شده است. علاوه بر این، معماری صفحه کنترل SDN توزیع شده با چالش های متعددی از نظر قابلیت همکاری، سازگاری، قرار دادن کنترلر و غیره مواجه است، و ما تمام این چالش ها را در ادامه بررسی خواهیم نمود.

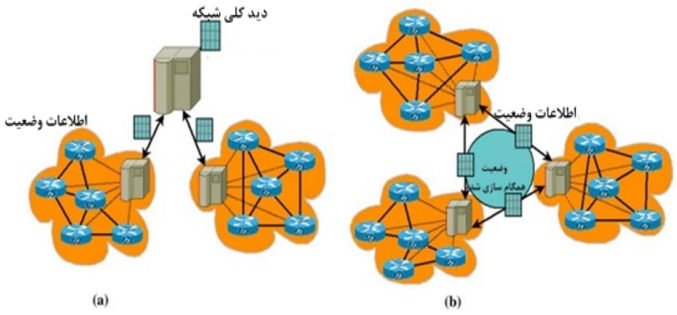
کنترلر توزیع شده

کنترل کننده های توزیع شده فیزیکی را می توان به طور کلی بر اساس روش سازماندهی نمونه های کنترل کننده به دو دسته طبقه بندی کرد. دسته اول شامل صفحه کنترل سلسله مراتبی است که در آن منطق کنترل شبکه به چندین لایه تقسیم می شود همانطور که در شکل۷ (a) نشان داده شده است. دسته دوم یک ساختار مسطح(افقی) است که در آن کنترل شبکه به صورت افقی تقسیم می شود تا مناطق متعدد را همانطور که در شکل ۷ (b) نشان داده شده است کنترل کند. صفحه کنترل سلسله مراتبی که به عنوان مدل عمودی نیز نامیده می شود، مقیاس پذیری و عملکرد بهتری را ارائه نموده و هر لایه از کنترل‌کننده‌ها خدمات خاصی را ارائه مینمایند . به عنوان مثال، در معماری دو لایه همانطور که در شکل ۷(a) نشان داده شده

[21] single point of failure
[22] new flow setup requests
[23] consistent view of network changes

است، لایه پایینی کنترل‌کننده‌ها رویدادهای محلی را مدیریت می‌کنند و خدمات را به سوئیچ‌ها ارائه می‌کنند، در حالی که لایه بالایی نمای کلی و قابلیت همکاری بین لایه‌های پایین‌تر را فراهم می‌کند. کنترل کننده های مخصوص کنترل‌کننده‌های لایه پایین (یا کنترل‌کننده‌های محلی) ارتباط مستقیمی با یکدیگر ندارند، در مقابل هر کنترل‌کننده محلی از خدمات کنترل‌کننده لایه بالایی (یا کنترل‌کننده ریشه) برای اتصال بین دامنه استفاده می‌کند.

در صفحه کنترل SDN مسطح، شبکه به چندین ناحیه تقسیم می شود و هر ناحیه تحت کنترل یک کنترل کننده محلی است. سازماندهی کنترلرها به این شکل، انعطاف پذیری خوب و تأخیر کنترل کمتری را فراهم می کند. از این معماری به عنوان معماری افقی نیز یاد می شود. برای داشتن یک نمای کلی، همه کنترل‌کننده‌ها در یک خوشه مسطح[۲۴] با استفاده از رابط شرق به یکدیگر متصل می‌مانند و اطلاعات وضعیت شبکه را به/از دیگر کنترل‌کننده‌ها همانطور که در شکل ۷ (b) نشان داده شده است به اشتراک می‌گذارند/دریافت می‌کنند. هر رویداد شبکه محلی مانند شکست پیوند یا از کار افتادن هر گره با سایر کنترل‌کننده‌های SDN در ترتیب خوشه‌بندی به اشتراک گذاشته می‌شود تا یک نمای کلی ثابت ارائه نماید. در نتیجه، این مدل به عنوان مدل همتا به همتا یا مدل ماشین حالت تکرار نیز نامگذاری شده است.



شکل (۷) : انواع صفحه کنترل توزیع شده a) صفحه کنترل سلسه مراتبی b) صفحه کنترل مسطح

جدول(۳) : کنترل کننده های متمرکز در SDN

کنترل کننده	زبان برنامه نویسی	چندنخی	رابط	پیمانه ای بودن	رابط شمالی	رابط جنوبی	مجری	بازدهی				بستر	کاربردها
								مقیاس پذیری	قابلیت اطمینان	سازگاری	امنیت		
NOX	C++	دارد	python	ضعیف	Ad-hoc	OF 1.0	Nicira	خیلی خوب	خیلی خوب	خوب	خیلی خوب	لینوکس	سازمانی
POX	Python	ندارد	Python	ضعیف	Ad-hoc	OF 1.0	Nicira	خیلی خوب	خیلی خوب	خوب	خیلی خوب	لینوکس و ویندوز	سازمانی
Mastro	java	دارد	مبتنی بر وب	نرمال	Rest API	OF 1.0	RICE	خیلی خوب	خیلی خوب	خوب	خیلی خوب	لینوکس و ویندوز	تحقیقاتی
FloodLight	java	دارد	مبتنی بر وب	نرمال	Rest API	OF1.0,1.2-5	BIG Switch	خیلی خوب	خیلی خوب	خوب	خیلی ضعیف	لینوکس و ویندوز	سازمانی-تحقیقاتی
Ryu	Python	دارد	CLI	خوب	Rest API	OF1.0,1.2-5	NPPO Tel	ضعیف	خیلی خوب	خوب	خیلی خوب	لینوکس	سازمانی-تحقیقاتی
MUL	C	دارد	CLI	نرمال	Rest API	OF1.0-4	KulClaod	خیلی خوب	خیلی خوب	خوب	خیلی خوب	لینوکس	مراکز داده
Trema	C&Ruby	دارد	CLI	نرمال	Ad-hoc	OF 1.0,1.3	NEC	خیلی خوب	خیلی خوب	خوب	خیلی خوب	لینوکس	تحقیقات
Becon	Java	دارد	مبتنی بر وب	قوی	Rest API	OF 1.0	Stanford	ضعیف	ضعیف	خوب	خیلی خوب	لینوکس و ویندوز	تحقیقات
Iris	Java	دارد	مبتنی بر وب	نرمال	Rest API	OF 1.0,1.3	ETRI	ضعیف	ضعیف	خوب	خیلی خوب	لینوکس و ویندوز	سطح اجرائی
Rosemary	C	دارد	ندارد	قوی	Ad-hoc	OF 1.0,1.3	-	ضعیف	ضعیف	خوب	خوب	لینوکس	سازمانی-تحقیقاتی
ParaFlow	C++	دارد	ندارد	قوی	Ab APIs	OF 1.0,1.3	-	ضعیف	ضعیف	خوب	-	لینوکس	سطح اجرائی

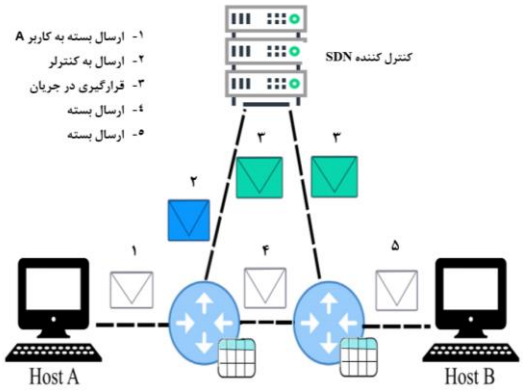
۶. پروتکل Openflow

مفاهیم و کاربردها

OpenFlow پرکاربردترین رابط جنوبی یا پروتکل لایه کنترلی برای SDN است. این پروتکل ارتباط بین برنامه‌های شبکه‌ای که در لایه‌های کنترل و برنامه وجود دارند و تمامی دستگاه‌های موجود در لایه انتقال داده را تسهیل می‌کند. مشخصات اولیه

[24] flat cluster

پیش نویس OpenFlow دائماً در حال تغییر بوده است و اکنون شامل ویژگی های جدیدی است تا بتواند قابلیت رویارویی با چالش های در حال ظهور تحمیل شده توسط الگوی SDN در حال رشد را داشته باشد. برای اجرای وظایف ارسال بسته در SDN، با استفاده از OpenFlow به عنوان رابط جنوب، سوئیچ ها باید از ورودی های جریان ذخیره شده در جداول جریان پشتیبانی کنند. ورودی‌های جریان توسط برنامه‌های کاربردی شبکه و کنترل‌کننده و به منظور دستور دادن به رفتار ارسال بسته صادر می‌شوند که در نهایت با فرآیند تطبیق فیلدهای بسته و سایر ویژگی‌ها مانند اولویت‌ها و شمارنده‌های بسته در برابر برخی محدودیت‌های مشخص‌شده در ورودی های جریان ها حاصل می‌شود. تطابق بین بسته ورودی و ورودی جریان زمانی اتفاق می افتد که تمام فیلدهای ورودی جریان با تمام فیلدهای موجود در سربرگ بسته مطابقت داشته باشند. پس از یک تطابق موفق، یکی از شش دستورالعمل موجود در ورودی جریان ممکن است اجرا شود. پس از آن، عمل خاصی بر روی بسته طبق دستورالعمل اجرا می شود . درست پس از پایان فرآیند تطبیق فیلدها، یک بسته داده ممکن است توسط سوئیچ ارسال یا رها شود. در حالی که بسته کنترلی ممکن است به سوییچ دستور ثبت یا حذف یک ورودی جریان را بدهد یا حتی ممکن است اگر بسته با هیچ یک از ورودی های جریان ذخیره شده در جداول جریان مطابقت نداشته باشد یک رویداد از دست دادن جدول[25] صادر کند . مراحل ارسال بسته در SDN های مبتنی بر OpenFlow به طور خلاصه در شکل (۸) نشان داده شده است.



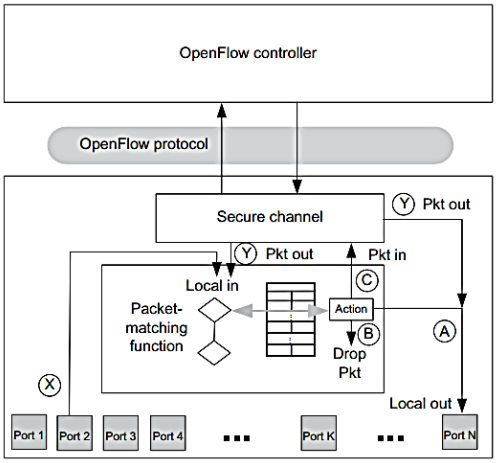
شکل(۸) : مرحله اصلی ارسال بسته از Host A به HostB به کمک پروتکل Openflow

شکل (۹) عملکردهای اساسی یک سوئیچ OpenFlow V.1.0 و رابطه آن با یک کنترلر را نشان می دهد. همانطور که از یک سوئیچ انتظار می رود، می بینیم که عملکرد اصلی این است که بسته ها را از پورتهای ورودی دریافت نموده(مسیر X در پورت ۲ در شکل) و آن را از طریق یک پورت خروجی (پورت N در شکل) ارسال نماید. تغییرات لازم بسته در طول مسیر که از آن میتوان بعنوان یک جنبه منحصر به فرد در سوئیچ OpenFlow نام برد در تابع تطبیق بسته نشان داده شده در شکل (۹) تجسم یافته است. جدول مرکز شکل یک جدول جریان است که در ادامه به طور جداگانه به جزئیات آن پرداخته خواهد شد. فلش پهن، خاکستری و دوتایی در شکل در در زمان وورد بسته جدید به سویچ شروع می شود سپس یک تطابق با یک ورودی خاص در آن جدول را بررسی نموده و بسته منطبق را به بخش عملیات در سمت راست هدایت می کند. این بخش عمل سه گزینه اساسی برای جابجایی این بسته ورودی دارد:

- A: بسته را به خارج از طریق یکی از پورتهای محلی منتقل مینماید(احتمالاً ابتدا فیلدهای سرآیند خاصی اصلاح شود)
- B: بسته را دور میاندازد.
- C: بسته را به کنترلر ارسال مینماید.

[25] Table-miss even

این سه مسیر بسته اساسی در شکل نشان داده شده است. در مورد مسیر C، بسته از طریق کانال امن نشان داده شده در شکل به کنترل کننده ارسال می شود. اگر کنترل کننده یک پیام کنترل یا یک بسته داده برای دادن به سوئیچ داشته باشد، کنترلر از همان کانال امن در جهت معکوس استفاده می کند. هنگامی که کنترلر یک بسته داده برای ارسال از طریق سوئیچ دارد، از پیام OpenFlow PACKET_OUT استفاده می کند. در شکل می بینیم که چنین بسته داده ای که از کنترلر می آید ممکن است دو مسیر متفاوت را از طریق منطق OpenFlow طی کند که هر دو با Y مشخص شده اند.
در سمت راست ترین حالت، کنترل کننده مستقیماً پورت خروجی را مشخص می کند و بسته به آن پورت N ارسال می شود. در مثال در سمت چپ ترین حالت Y، کنترل کننده نشان می دهد که می خواهد تصمیم ارسال را به منطق تطبیق بسته موکول کند. عملیات مختلف در سوئیچ OpenFlow یا بصورت فقط OpenFlow و یا OpenFlow-hybrid است. سوئیچ OpenFlow-Only سوئیچی است که بسته ها را فقط طبق منطق OpenFlow که در بالا توضیح داده شد، ارسال می کند. OpenFlow Hybrid سوئیچی است که می‌تواند بسته‌ها را در حالت ستنی خود به‌عنوان یک سوئیچ اترنت یا روتر IP سوئیچ کند. می توان نمونه هیبریدی را به عنوان یک سوئیچ OpenFlow در کنار یک سوئیچ سنتی کاملا مستقل مشاهده کرد. چنین سوئیچ هیبریدی نیاز به یک مکانیسم طبقه بندی پیش پردازش دارد که بسته ها را به پردازش OpenFlow یا پردازش بسته سنتی هدایت می کند.



شکل(۹): ساختار کلی ارتباطات در SDN

در ادامه خواهیم دید که کنترلر با تعیین پورت مجازی TABLE به عنوان پورت خروجی این امر را اجرا می کند. عملیات مختلف در سوئیچ OpenFlow یا بصورت فقط OpenFlow و یا OpenFlow-hybrid است. سوئیچ OpenFlow-Only سوئیچی است که بسته ها را فقط طبق منطق OpenFlow که در بالا توضیح داده شد، ارسال می کند. OpenFlow Hybrid سوئیچی است که می‌تواند بسته‌ها را در حالت ستنی خود به‌عنوان یک سوئیچ اترنت یا روتر IP سوئیچ کند. می توان نمونه هیبریدی را به عنوان یک سوئیچ OpenFlow در کنار یک سوئیچ سنتی کاملا مستقل مشاهده کرد. چنین سوئیچ هیبریدی نیاز به یک مکانیسم طبقه بندی پیش پردازش دارد که بسته ها را به پردازش OpenFlow یا پردازش بسته سنتی هدایت می کند.

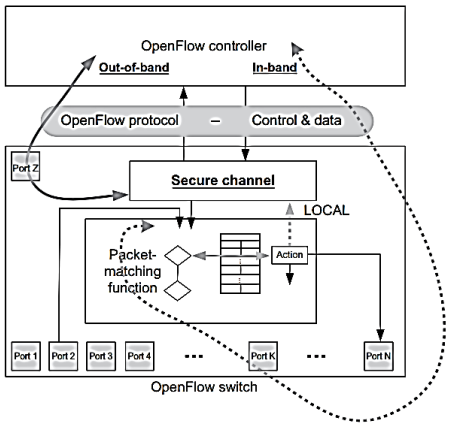
پروتکل Openflow چگونه کار میکند:

همانطور که در شکل (۱۰) نشان داده شده است، پروتکل OpenFlow ارتباط بین یک کنترل کننده OpenFlow و یک سوئیچ OpenFlow را تعریف می کند. این پروتکل چیزی است که به طور منحصر به فرد فناوری OpenFlow را شناسایی می کند. در اصل، پروتکل شامل مجموعه‌ای از پیام‌ها است که از کنترل‌کننده به سوییچ ارسال می‌شوند و مجموعه‌ای از پیام‌ها که در جهت مخالف ارسال می‌شوند. پیام‌ها در مجموع به کنترل‌کننده اجازه می‌دهند تا سوئیچ را طوری برنامه‌ریزی کند که

امکان کنترل دقیق روی تغییر ترافیک کاربر را فراهم کند. بطور کلی یک جریان را به عنوان مجموعه ای از بسته ها تعریف میکنند که از یک نقطه پایانی شبکه (یا مجموعه ای از نقاط پایانی) به نقطه پایانی دیگر (یا مجموعه ای از نقاط پایانی) منتقل می شوند. نقاط پایانی ممکن است به عنوان آدرس IP جفت پورت TCP/UDP، نقاط پایانی VLAN، نقاط پایانی تونل لایه سه و پورت ورودی در میان موارد دیگر تعریف شوند.هنگامی که کنترل کننده یک جریان را تعریف می کند، اطلاعاتی را در اختیار سوئیچ قرار می دهد که برای چگونه رفتار کردن با بسته های ورودی را که مطابق با جریان هستند به آنها نیاز خواهد داشت. با تکامل پروتکل OpenFlow، امکانات برای عملیات پیچیده‌تر شده است، اما ابتدایی‌ترین نسخه‌ها برای عمل روی یک بسته دریافتی با مسیرهای A، B و C در شکل (۱۰) نشان داده شده‌اند. این سه گزینه عبارتند از: ارسال بسته به یک یا چند پورت خروجی، رها کردن بسته، یا ارسال بسته به کنترل کننده برای رسیدگی به استثنا.

اجزای عملکرد OpenFlow

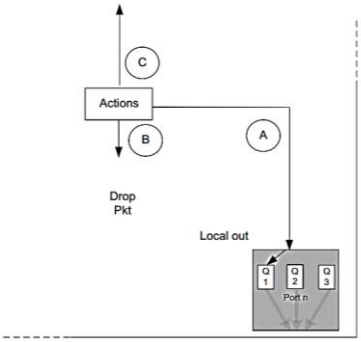
کانال امن ارتباطی : کانال امن مسیری است که برای ارتباط بین کنترلر OpenFlow و دستگاه OpenFlow. به طور کلی، این ارتباط با رمزگذاری نامتقارن TLS-b sed ایمن می شود.اگرچه اتصالات TCP رمزگذاری نشده مجاز هستند، این اتصالات ممکن است درون باند (in bound) یا خارج از باند(out of bound) باشند. شکل (۱۰) این دو نوع کانال امن را نشان می دهد. در مثال خارج از باند، مشاهده می کنیم که اتصال کانال امن از طریق پورت Z وارد سوئیچ می شود که توسط صفحه داده OpenFlow سوئیچ نمی شود. برخی از پشته شبکه قدیمی، پیام‌های OpenFlow را از طریق کانال امن به فرآیند کانال امن در سوئیچ تحویل می‌دهند، جایی که همه پیام‌های OpenFlow تجزیه و تحلیل می‌شوند. بنابراین، کانال امن خارج از باند تنها در مورد سوئیچ OpenFlow-hybrid مرتبط است.



شکل (۱۰) :ساختار کلی کانال امن ارتباطی کنترلر و سویچ های Openflow

در مثال درون باند، پیام های OpenFlow از کنترلر را می بینیم که از طریق پورت K که بخشی از صفحه داده OpenFlow است می رسد. در این حالت این بسته ها توسط منطق تطبیق بسته OpenFlow نشان داده شده در شکل(۱۰) مدیریت می شوند. جداول جریان به گونه‌ای ساخته می‌شوند که این ترافیک OpenFlow به پورت مجازی LOCAL ارسال می‌شود، که منجر به ارسال پیام‌ها به فرآیند کانال امن می‌شود. توجه داشته باشید که وقتی کنترلر و تمام سوئیچ هایی که کنترل می کند در یک محیط کاملاً کنترل شده مانند مرکز داده قرار دارند، ممکن است عاقلانه باشد که از رمزگذاری مبتنی بر TLS برای ایمن سازی کانال استفاده نکنید. زیرا با استفاده از این نوع تبادلات ، سربار عملکردی ایجاد می شود و در صورت عدم نیاز، ترجیحاً از این جریمه عملکردی جلوگیری شود. یکی دیگر از استدلال های مخالف استفاده از رمزگذاری مبتنی بر TLS این است که ممکن است به اشتباه استفاده شود. برای عملی کردن TLS باید گواهینامه های امنیتی را برای هر دستگاه دریافت و پیکربندی کرد، که ممکن است برای افرادی که با این روش ها آشنا نیستند زمان بر و مستعد خطا باشد.

پورت ها و صف های پورت : مشخصات OpenFlow مفهوم پورت OpenFlow را تعریف می کند. یک پورت OpenFlow V.1.0 مربوط به یک پورت فیزیکی است. این مفهوم در نسخه های بعدی OpenFlow گسترش یافته است. برای سال‌های متمادی، سوئیچ‌های پیچیده از چندین صف در هر پورت فیزیکی پشتیبانی می‌کردند. این صف‌ها عموماً توسط الگوریتم‌های زمان‌بندی ارائه می‌شوند که امکان ارائه سطوح مختلف کیفیت خدمات (QoS) را برای انواع مختلف بسته‌ها فراهم می‌کند. OpenFlow این مفهوم را پشتیبانی کرده و اجازه می دهد یک جریان به یک صف از قبل تعریف شده در یک پورت خروجی نگاشت شود. بنابراین، اگر به شکل (۱۰) برگردیم، خروجی یک بسته در پورت N ممکن است شامل تعیین صف در پورت N باشد که بسته باید در کدام صف قرار گیرد. بنابراین، اگر روی گزینه A در شکل (۱۰) بزرگنمایی کنیم، آنچه را که اکنون در شکل (۱۱) می بینیم آشکار می شود. در شکل بزرگنمایی شده ما می‌توانیم ببینیم که جعبه عملیات به‌طور خاص بسته در حال پردازش را در صف ۱ در پورت N قرار داده است.



شکل(۱۱) : وجود صف پورت با زوم گردن در بخش مربوطه از شکل (۹)

جدول جریان: جدول جریان در هسته تعریف سوئیچ OpenFlow قرار دارد. جدول (۴) یک جدول جریان عمومی را نشان می دهد. یک جدول جریان شامل ورودی های جریان است که یکی از آنها در جدول (۵) نشان داده شده است. یک ورودی جریان شامل فیلدهای سرآیند، شمارنده ها و اقدامات مرتبط با آن ورودی است. فیلدهای سرصفحه به عنوان معیار تطبیق برای تعیین اینکه آیا بسته ورودی با این ورودی مطابقت دارد یا خیر استفاده می شود. اگر مطابقت وجود داشته باشد، بسته متعلق به این جریان است. شمارنده ها برای ردیابی آمار مربوط به این جریان استفاده می شوند، مانند تعداد بسته هایی که برای این جریان ارسال شده یا حذف شده اند. فیلدهای اقدامات توضیح می دهند که سوئیچ باید با بسته ای که با این ورودی مطابقت دارد انجام دهد.

جدول (۴): نمونه جدول جریات در Openflow

ورودی جریان ۰		...	ورودی جریان ۱		...	ورودی جریان F		...	ورودی جریان M	
سرآیند	از پورت ۱۲ 192.32.10.1 پورت:1012		سرآیند	از پورت * 209.*.*.* پورت:*		سرآیند	از پورت ۲ 192.32.10.1 پورت:995		سرآیند	از پورت ۲ 192.32.10.1 پورت:995
شمارنده	مقدار		شمارنده	مقدار		شمارنده	مقدار		شمارنده	مقدار
عملیات	مفدار		عملیات	مفدار		عملیات	مفدار		عملیات	مفدار

جدول (۵): یک ورودی ساده جدول جریان

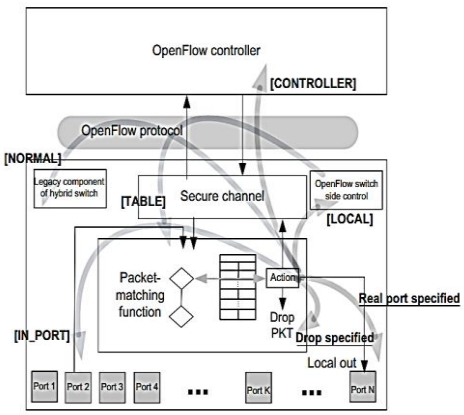
سرآیند	مقدار
شمارنده	مقدار
عملیات	مقدار

تطبیق بسته: هنگامی که بسته ای از یک پورت ورودی (یا در برخی موارد از کنترل کننده) به سوئیچ OpenFlow می رسد، با جدول جریان مطابقت داده می شود تا مشخص شود آیا ورودی جریان منطبقی وجود دارد یا خیر. فیلدهای مطابقت زیر مرتبط با بسته ورودی ممکن است برای تطبیق با ورودی های جریان استفاده شود:

- Switch input port
- VLAN ID
- VLAN priority
- Ethernet source address
- Ethernet destination address
- Ethernet frame type
- IP source address
- IP destination address
- IP protoc
- IP Type of Service (ToS) bits
- TCP/UDP source port
- TCP/UDP destination port

این دوازده فیلد تطبیقی در مجموع به عنوان پایه دوازده عامل تطبیق نامیده می شود. فیلدهای تطبیق ورودی جریان ممکن است با استفاده از یک بیت ماسک به صورت Wildcard درآیند، و هر مقداری که با بیت‌های بدون ماسک در فیلدهای مطابقت بسته ورودی مطابقت داشته باشد، در نظر گرفته خواهد شد. ورودی‌های جریان به ترتیب پردازش می‌شوند، و پس از یافتن یک تطابق، هیچ تلاش دیگری برای تطبیق با آن جدول جریان انجام نمی‌شود. (در نسخه های بعدی OpenFlow خواهیم دید که ممکن است جداول جریان اضافی وجود داشته باشد که تطبیق بسته ممکن است ادامه یابد.) به این دلیل، ممکن است چندین ورودی جریان تطبیق برای یک بسته وجود داشته باشد که در یک جدول جریان وجود داشته باشد. فقط اولین ورودی جریان برای تطبیق معنادار است و باقی به عنوان تطبیق بسته در اولین تطابق در نظر گرفته نمی شوند.

عملیات تطابق و ارسال بسته: اقدامات مورد نیازی که باید توسط یک ورودی جریان پشتیبانی شوند عبارتند از خروجی (ارسال) یا رها کردن بسته منطبق. رایج ترین حالت این است که عملکرد خروجی یک پورت فیزیکی را مشخص می کند که بسته باید بر روی آن ارسال شود. با این حال، پنج پورت مجازی ویژه تعریف شده در نسخه V.1.0 وجود دارد که اهمیت ویژه ای برای عملکرد خروجی دارند. آنها LOCAL، ALL، CONTROLLER، IN_PORT، و TABLE هستند.انتقال بسته های حاصل از این نامگذاری های مختلف درگاه مجازی در شکل (۱۵) نشان داده شده است. در شکل، نمادهای داخل پرانتز در کنار فلش‌های سایه‌دار گسترده، یکی از انواع پورت مجازی مورد بحث در این بخش را نشان می‌دهند.



شکل(۱۴) : ساختار کلی دستورات در Openflow

۷. تهدیدات و آسیب پذیری SDN

SDN مانند هر فناوری جدید مزایا و معایب خاص خود را دارد. به عنوان مثال با توجه به امنیت، فناوری SDN می تواند برای کاهش یا کاهش کامل برخی از خطرات و آسیب پذیری هایی که معمولاً امنیت شبکه های معمولی را مورد تهدید قرار می گیرند، مورد استفاده قرار گیرد. متأسفانه فناوری SDN آسیب‌پذیری‌ها و تهدیدات جدیدی را معرفی می‌کند که در معماری جدید آن ذاتی هستند. در واقع، جداسازی سطوح کنترل و داده، و تمرکز منطقی تمام اطلاعات شبکه، یک نقطه شکست را ایجاد می کند که می تواند برای به خطر انداختن کل شبکه SDN مورد سوء استفاده قرار گیرد. در ابتدا یک نمای کلی از قابل مشاهده ترین سطوح حمله و بردارهای تهدید که در سطوح و رابط های معماری SDN شناسایی شده اند ارائه می شود، در ادامه ، شرح مفصلی از مسائل، اثرات و پیامدهای ناشی از بهره برداری از سطوح حمله و تهدیدات موجود در معماری SDN خواهد آمد و در قسمت پایانی، لیستی از رایج ترین حملات و رفتارهای مخربی که لایه ها را در معماری SDN هدف قرار می دهند، ارائه خواهد گردید.

سطوح حمله و بردارهای تهدید درSDN [۲۹]

همانند شبکه های معمولی، هر نمونه شبکه، پروتکل، دستگاه یا لایه‌ای که در SDN وجود دارند می‌تواند مورد سوء استفاده عمدی یا غیر عمدی قرار گیرد که در برخی موارد برای افشای خطاهای سیستم یا آشکار کردن رفتار انحرافی ضمنی استفاده می‌شود. این استدلال برای اثبات این موضوع کافی است که هر عنصر یا لایه ای که بخشی از معماری SDN را تشکیل می دهد، یک تهدید بالقوه یا سطح حمله است، یعنی هر پیکربندی بد یا استقرار نادرست هر عنصر SDN می تواند به عنوان منبع نوظهور آسیب پذیری های بالقوه و خطرات امنیتی در نظر گرفته شود. از این نقطه به بعد، ما قصد داریم صفحه کنترل را به عنوان نقطه اتصال لایه برنامه و لایه سیستم عامل شبکه در نظر بگیریم، به دنبال این رویکرد، آسیب‌پذیری‌ها و حملاتی که برنامه‌های شبکه یا APIهای شمال را هدف قرار می‌دهند، آسیب‌پذیری یا حملات صفحه کنترل بدون تمایز در نظر گرفته می‌شوند. . در شکل(۱۵) ، هر صفحه/رابط SDN فهرستی با مرتبط ترین سطوح تهدید را گروه بندی می کند که ممکن است توسط کاربران مخرب برای به خطر انداختن شبکه تحت الگوی SDN مورد استفاده قرار گیرد.



شکل (۱۵) : نمای کلی تهدیدات موجود در هر یک از لایه های SDN

مسائل امنیتی: تمام حملات به امنیت شبکه را می توان بر اساس هدف اصلی حمله دسته بندی کرد، به عنوان مثال استراق سمع یک رابط کنترلی را می توان به عنوان حمله ای که هدف اصلی آن دستکاری داده های خصوصی و حساس رد و بدل شده بین وسایل شبکه است و افشای غیرمجاز اطلاعات به معنای گسترده تر برچسب گذاری کرد. فهرست زیر مسائل و تهدیدات کلی در امنیت شبکه را با توضیح سطوح حمله، رفتارهای انحرافی و نقص‌های امنیتی که در متن SDN شناسایی شده‌اند، توضیح می‌دهد.

دسترسی غیرمجاز: از مکانیسم‌های کنترل دسترسی ضعیف یا ناموجود سوء استفاده می‌کنند، حملات brute-force را علیه پایانه‌های اداری و APIهای REST انجام می‌دهند که باعث افشای جلسات ورود (logging sessions) میشوند، یا از پیوندهای آسیب‌پذیری در اجزای شبکه استفاده می‌کنند و سپس اقدام به راه اندازی دستگاه های تفوذی یا اتصال از راه دور برای اتصال به شبکه مینماید.

افشای غیرمجاز اطلاعات : چندین سطح حمله را می توان برای جداسازی اطلاعات حساس شبکه مورد استفاده قرار داد، به عنوان مثال، یک مهاجم می تواند با پخش بسته های Probe برای هدف قرار دادن عناصر شبکه، رفتار ارسال شبکه را استنباط کند. مهاجمی که با موفقیت یک برنامه شبکه آسیب پذیر را به خطر می اندازد، می تواند به پایگاه های داده خط مشی شبکه و سایر ذخیره های داخلی داده های شبکه دسترسی پیدا کند. کانال های ناامن را می توان بوسیله استراق سمع بسته ها کشف کرد. در نهایت، حملات جعل هویت یک دستگاه، مهاجم را قادر می‌سازد اطلاعاتی را دریافت کند که در اصل برای یک عنصر شبکه در معرض خطر قرار گرفته میباشد.

اصلاح غیرمجاز اطلاعات شبکه : مهاجمان می‌توانند از پروتکل‌ها و APIهای آسیب‌پذیر و فقدان مکانیسم‌های تأیید و احراز هویت برای نادیده گرفتن قوانین جریان موجود از طریق برنامه‌های مخربی که قوانین جریان متناقض را صادر می‌کنند، استفاده کنند. علاوه بر این، دسترسی غیرمجاز به فضای ذخیره سازی داخلی به مهاجم این امکان را می دهد که سیاست های شبکه ای متناقض را معرفی کند یا سیاست های موجود را اصلاح کند. از سوی دیگر، تغییرات در توپولوژی شبکه را می توان با اعمال نفوذ تنظیمات اشتباه پروتکل همراه با جعل هویت دستگاه و حملات تزریق بسته های جعلی ایجاد کرد.

تخریب اطلاعات شبکه : برجسته‌ترین سناریوها در این مورد به فلاشینگ قانون جریان تحمیلی در سوئیچ‌ها، برنامه‌های مخرب که بسته‌های کنترلی را که برای یک برنامه دیگر یا یک زنجیره سرویس در نظر گرفته شده است دور می‌اندازند، و حذف خط‌مشی شبکه در نتیجه دسترسی غیرمجاز به ایستگاه‌های اداری یا پایگاه‌های داده داخلی شبکه است.

اختلال در خدمات : سه منبع اصلی اختلال در سرویس وجود دارد، در وهله اول حملات سیل: کنترل سیل بسته ها و جدول قوانین جریان سیل. ثانیا، حمله تزریق بسته نادرست که اغلب باعث قطع اتصال یا قطع شدن دستگاه هدف می شود. در نهایت، حملات توپولوژی که در آن حمله کننده توپولوژی شبکه را تغییر میدهد و ارتباطات شبکه را به میل خود تغییر میدهد.

پیکربندی نادرست : پیکربندی‌های معیوب در پروتکل‌ها، رابط‌ها، APIها و سیستم‌ها به آسیب‌پذیری‌ها و نقص‌های امنیتی جدید تبدیل می‌شوند. سیاست های شبکه و قوانین جریان متناقض؛ مکانیسم های تأیید و احراز هویت نامناسب؛ و دور زدن اقدامات امنیتی قبلاً مستقر شده نیزمیتوانند مشکل آفرین باشند.

مکانیزم های احراز هویت، اعتماد و تأیید پیکربندی ضعیف : کانال‌های متن ساده و مکانیسم‌های احراز هویت نامناسب یا ضعیف راه را برای اکثر حملات و رفتارهای انحرافی هموار می‌کنند: حملاتی چون استراق سمع، تزریق بسته، ساخت بسته، رهگیری ترافیک، مسمومیت اطلاعات شبکه و شناسایی و ربودن هویت.

چالشهای امنیتی مرتبط با کنترل متمرکز در معماری SDN: کنترل متمرکز در SDN نشان دهنده وجود یک نقطه شکست است و SDN را در برابر حملات و اختلالات آسیب پذیر می کند. در واقع، تمرکز مدیریت، کنترل کننده را به یک هدف جذاب برای یک مزاحم تبدیل خواهد نمود. هر شخصی که به کنترل کننده دسترسی داشته باشد می تواند مستقیماً هر

جریان را دستکاری نموده و به این ترتیب کل شبکه را کنترل می نماید. همچنین، اگر کنترل کننده به دلیل یک حمله (مانند حمله DoS) یا به دلیل پیکربندی نادرست در دسترس نباشد، سوئیچ ها مسدود می شوند زیرا آنها فقط می توانند قوانین از پیش تعریف شده را اعمال کنند و نمی توانند بسته های جدیدی را که با هیچ ورودی جریان موجود مطابقت ندارند به درستی مدیریت کنند. با توجه به تمرکز امنیت SDN، راه حل قوی جهت محافظت از کنترل کننده در برابر چنین رویدادهایی هنوز در حال تحقیق است. اما در کنار این تحقیقات راه حل هایی همچون بکار گیری چندین کنترلر پشتیبان در حال انتظار به عنوان آخرین راه جهت بازگردانی یک خرابی در نظر گرفته شده است.

چالشهای امنیتی مرتبط با قابلیت برنامه ریزی در معماری SDN: از آنجایی که شبکه های SDN عمدتاً قابل برنامه ریزی هستند، در برابر حملات هدفمند آسیب پذیر هستند. بدافزاری که معماری‌های شبکه خاصی را هدف قرار می‌دهد، می‌تواند عملکرد دستگاه‌های شبکه را با تغییر تنظیمات آنها به خطر بیاندازد، که با توجه به جدول (۶) پیامدهای چشمگیری بر روی شبکه خواهد داشت.

جدول(۶) :چالشهای امنیتی SDN در سطح تبادل

سطح ارتباطی	حملات	دلایل حمله
باند جنوبی	حملات جعل	احراز هویت ضعیف
	دسترسی مخرب به برنامه های کاربردی	شناسایی اشتباه
باند شمالی	استراق سمع	عدم رمزنگاری
	حملات جعل	احراز هویت ضعیف
	حملات مرد میاتی	احراز هویت ضعیف
	دسترسی تایید نشده	شناسایی اشتباه

چالشهای امنیتی مرتبط با استانداردهای متن باز: SDN از طریق استانداردهای باز مانند OpenFlow پیاده سازی می شود که دارای پیاده سازی متن باز است و از این رو، مهاجمان از مزیت شناسایی آسیب پذیری ها برخوردار هستند.

چالشهای امنیتی مرتبط با ریسک امنیتی جدول جریان: یک جدول جریان را می توان از طریق کنترل کننده اصلی و یک کنترلر پشتیبان مدیریت کرد. کنترلر پشتیبان باید در معرض سطوح امنیتی پایین‌تری باشد، و بنابراین مهم است که ورودی‌های جدول جریان ثابت باقی بمانند و از یک به‌روزرسانی مخرب ناشی از یک کنترل‌کننده در معرض خطر محافظت شوند. در حال حاضر، OpenFlow برخلاف FlowVisor چنین سازگاری را در نظر نمی گیرد.

چالشهای امنیتی مرتبط با فقدان عملکرد های اساسی : عملکردهای امنیتی مهم ذاتاً در معماری SDN مانند فایروال ها یا Network Address Translation (NAT) تعریف نشده اند. در شبکه‌های فعال کنونی، بسیاری از این قابلیت‌ها در قالب دستگاه‌های افزونه (جعبه‌های میانی) تحقق می‌یابند. با این حال، پیاده سازی برخی از توابع آسان نیست و دارای محدودیت هایی مانند بازرسی بسته های عمیق در پروتکل OpenFlow است که توسط این پروتکل پشتیبانی نمیگردد.

چالشهای امنیتی مرتبط با واکنش دینامیک در طراحی: همانطور که قبلا ذکر شد، صفحه داده بسته های ورودی را بر اساس قوانین جریان در جداول جریان خود ارسال می کند. هنگامی که بسته های جدید بدون جریان تعریف شده دریافت می کند، این بسته ها به کنترل کننده ارسال می شود که قوانین حمل و نقل جدیدی را ایجاد می کند تا به صورت پویا و نه فعالانه با آنها برخورد کند. یک مهاجم می تواند از این طراحی واکنش پویا کنترل کننده برای به دست آوردن اطلاعات در مورد وضعیت های شبکه بهره مند شود.

چالشهای امنیتی مرتبط با فقدان ضرورت استفاده ازTLS در SDN : مشخصات OpenFlow فعلی (v1.5.0) پروتکل امنیت لایه انتقال (TLS) را برای ایمن کردن کانال ارتباطی بین سوئیچ‌ها و کنترل‌کننده‌ها پیشنهاد می‌کند. با این حال، استفاده از ، TLS را اختیاری می کند و فرصتی را برای دشمنان ایجاد می کند تا به شبکه های OpenFlow نفوذ

کنند. نشان داده شده است که مزایای امنیتی SDN بر تهدیدهایی که یا خاص SDN هستند یا ارثی هستند، غالب میگردد. آنها امنیت اطلاعات SDN و شبکه‌های معمولی را با توجه به تأثیر روی شبکه از منظر اعتبار، یکپارچگی، محرمانه بودن، در دسترس بودن و سازگاری ارزیابی و مقایسه کردند. علاوه بر این، آنها امنیت اطلاعات یا ویژگی های شبکه ارائه شده توسط SDN و شبکه های معمولی را از منظر مدیریت شبکه، هزینه ها و تشخیص و پیشگیری از حمله ارزیابی کردند. در نتیجه این ارزیابی‌ها ، نویسندگان به این نتیجه رسیدند که SDN گامی رو به جلو برای امنیت شبکه است زیرا مزایا بیش از تهدیدات خواهد بود.

در این بخش به تجزیه و تحلیل امنیتی انواع مختلف مسائل امنیتی و حملاتی که امنیت SDN را تهدید می کنند و برخی اقدامات متقابل مرتبط می پردازیم. در این بخش، ما در مورد حملاتی صحبت می کنیم که به طور فیزیکی بر کنترل کننده ها و سوئیچ ها تأثیر می گذارد، سپس، ما حملاتی را که بر سطوح مختلف SDN همچون Application، Control و Data تأثیر می گذارد، بحث می کنیم. جدول (۵) خلاصه ای از تحقیقات اصلی امنیت SDN، شامل راه حل ها و حملات SDN را بر اساس خط زمانی ارائه می دهد. همچنین نمای کلی حملات فیزیکی و حملات به صفحات SDN در جدول(۸) ارائه شده است.

حملات فیزیکی مبتنی بر نقص امنیتی Universal plug & play (UPnP): به طور خاص، پلاگین و universal plug and play (UPnP) نقش مهمی در اتصال دستگاه‌های ناهمگن برای فعال کردن تبادل اطلاعات بین آنها ایفا می‌کند. UPnP دارای اشکالات ذاتی مرتبط با امنیت است زیرا با استفاده از پروتکل ساده کشف سرویس و پروتکل user data- gram protocol (UDP) کار می کند. UPnP پروتکلی است که در آن به کاربران می توان به طور خودکار آدرسی را بدون درج تنظیمات شبکه اختصاص داد. برای شناسایی خودکار ترافیک غیرقانونی با استفاده از یک سوئیچ مبتنی بر SDN با درج قوانین برای جلوگیری از حملات DDoS در یک محیط UPnP ارایه شده است که پس از دریافت یک هشدار، این هشدار با هشدار های مطابقت شده قبلی مقایسه و سپس تصمیم گیری میگردد.

حملات ربودن کنترلر: کنترلر مستعد حمله Controller Hijacking است که امنیت کلی SDN را مختل می کند و منجر به به خطر افتادن کل شبکه می شود. مهاجمی که کنترل کننده را به دست می گیرد، کنترل کاملی بر سیاست های تعریف شده SDN خواهد داشت و به راحتی می تواند اطلاعات حساسی مانند داده های ارتباطی، رمزهای عبور و غیره را جمع آوری کند. این به مهاجم اجازه می دهد تا داده ها را دستکاری کرده و ترافیک را تغییر مسیر دهد. در عمل، ربودن کنترلر نتیجه برنامه‌های مخربی است که از آسیب‌پذیری‌های API به شمال برای دردست گرفتن کنترل‌کننده شبکه استفاده می‌کنند.

مشکلات مخرب مرتبط با مدیریت: یک مدیر شبکه می تواند کنترلرها را عمداً یا نادرست پیکربندی کند و در نهایت به حمل و نقل، مسیریابی یا در دسترس بودن شبکه آسیب برساند.

حملات مبتنی بر لایه Application در SDN : صفحه Application در SDN در برابر انواع مختلف حملات آسیب پذیر است که عمدتا به دلیل عدم احراز هویت میباشد. از آنجا که ماژول ها و برنامه های مختلف بر روی کنترل کننده نصب می شوند، با یک تابع متفاوت اختصاص داده شده به هر یک، تمام برنامه ها قادر به نصب جریان به سوئیچ ها بدون احراز هویت جریان هستند. مشکل دیگر عدم وجود تایید یا بررسی سازگاری به روز رسانی های نصب شده است که ممکن است منجر به رفتار ناخواسته شود که می تواند بر امنیت شبکه تاثیر بگذارد. هیچ مکانیسم کنترل دسترسی بر روی کنترل کننده برای محدود کردن تعامل بین برنامه ها یا جلوگیری از دسترسی یا تغییر منابع کنترل کننده بکار گرفته نشده است. مسئله دیگر در لایه کاربرد SDN عدم وجود استانداردهای جهانی یا مشخصات باز برای تسهیل API های باز برای برنامه های کاربردی جهت کنترل خدمات و توابع شبکه است که می تواند تهدیدات امنیتی برای منابع، خدمات و توابع شبکه ایجاد کند. از آنجا که SDN یک پروژه باز است، تامین کنندگان مختلف و برنامه های شخص ثالث در محیط های مختلف و در ماژول ها و زبان های مختلف برنامه نویسی توسعه می یابند که منجر به مسائل مربوط به همکاری و برخورد سیاست های امنیتی می شود.

حملات جعل در لایه کنترل SDN: شبکه های OpenFlow در معرض حملات جعل هستند، که مختص SDN ها نیست، با این حال، می تواند تأثیر بیشتری بر آنها داشته باشد. به عنوان مثال، مهاجم می تواند با جعل آدرس کنترل کننده، کل شبکه را کنترل کند. یک حمله جعل به کنترلر می تواند برای چند ثانیه طول بکشد، درست به اندازه زمان مورد نیاز برای برنامه نویسی قوانینی که برای اهداف مخرب اختصاص داده شده اند. در صورت عدم وجود TLS یا تأیید هویت سوئیچ، در جایی که یک سوئیچ OpenFlow در معرض خطرباشد ، ممکن است یک حمله State-Spoofing وضعیت خود را به کنترل کننده شامل اطلاعات آماری، رابط ها و جدول جریان، جعل کند ،،علاوه بر این، یک سوئیچ آسیب‌دیده می‌تواند سوئیچ‌ها یا پیوندهای مجازی را در شبکه ایجاد کند و در نتیجه نمای توپولوژی شبکه را در کنترل‌کننده تغییر دهد، که می‌تواند مسیرهای طی شده برای مسیریابی ترافیک را تغییر دهد، ازدحام ایجاد کند یا پهنای باند را برای خود مهاجم ذخیره نماید.

حمله مرد میانی در لایه کنترل SDN: کانال بین کنترل کننده و سوئیچ ها از طریق یک اتصال TCP که آسیب پذیر است برقرار می شود. همانطور که در مشخصات OpenFlow نشان داده شده است، امنیت لایه حمل و نقل (TLS) با احراز هویت متقابل می تواند به صورت اختیاری برای ایمن سازی ارتباطات استفاده شود. از این رو، این امکان برای کنترل و سوئیچ ها وجود دارد که با استفاده از متن ساده(plain text) ارتباط برقرار کنند. TLS به گواهی‌های تایید شده دو طرفه نیاز دارد که توسط یک کلید خصوصی مطابق با یک کلید عمومی قابل اعتماد متقابل امضا شده باشد. با این حال، TLS به مراحل زیادی برای پیکربندی نیاز دارد. همچنین بسیاری از سوئیچ ها و کنترلرها فاقد پشتیبانی از TLS هستند. به این ترتیب، TLS در بیشتر مواقع قابل استفاده نبوده و به دشمنان اجازه می‌دهد به شبکه‌های OpenFlow نفوذ کنند و قوانین جعلی را درج کنند یا قوانین موجود را اصلاح کنند. بروکس و همکاران با هدف بهره برداری از دو آسیب پذیری خاص SDN شامل کانال ارتباطی غیر ایمن بین سوئیچ های SDN و کنترل کننده و کنترل شبکه با به خطر انداختن کنترلر را مرتفع نمودند. آنها غلبه بر این آسیب پذیری ها از انجام حمله MITM با استفاده از ettercap از طریق حمله مسموم سازی کش روی کنترلروشنود ترافیک و گرفتن اعتبار ورود به سیستم رابط وب Open Daylight (ODL) به ثمر رساندند.

حمله نقض سرویس در لایه کنترل SDN: یک مسئله چالش برانگیز SDN، وجود پتانسیل بیشتر جهت حملات انکار سرویس (DoS) در SDN به دلیل کنترل کننده های متمرکز و محدودیت جداول جریان است. حملات DoS می توانند اطلاعات مسیریابی را هدف قرار دهند و در نتیجه کل عملیات شبکه های SDN را مختل کنند. اساساً، از آنجایی که صفحه داده از صفحه کنترل جدا شده است، صفحه داده به طور معمول از صفحه کنترل می خواهد که قوانین جریان را زمانی که صفحه داده بسته های جدید دریافت می کند، بیابد. یک مهاجم می‌تواند به طور خاص درخواست‌های جریان جعلی را از صفحه داده تولید کند، که دو نتیجه دارد: ۱) می‌تواند رسیدگی به تمام درخواست‌ها را برای صفحه کنترل متمرکز دشوار کند (مصرف منابع صفحه کنترل) و ۲) درخواست‌های جریان ساخته شده می‌تواند قوانین جریان غیرقابل استفاده زیادی را ایجاد می کند که باید توسط صفحه داده ذخیره شوند (مصرف منابع صفحه داده).

حملات پیمایش در لایه داده SDN: یک دشمن می تواند از راه دور شبکه های SDN را با ارسال Probe به آدرس های IP تصادفی در شبکه اسکن کند. هنگامی که یک هدف پاسخ می دهد، می توان آن را شناسایی یا مورد حمله قرار داد. اگر کسی پاسخ ندهد، آدرس‌های IP مورد بررسی بلااستفاده در نظر گرفته می‌شوند.

حمله افشای اطلاعات در لایه داده SDN: در این حمله مهاجم اطلاعاتی در مورد قوانین جریان فعال بدست می آورد. سپس با تنظیم زمان بندی TCP دو تلاش برای اتصال به دست می آید. اگر تلاش دوم اتصال به طور قابل توجهی سریعتر از اولین باشد، مهاجم ممکن است به این نتیجه برسد که یک قانون جریان جدید به تازگی نصب شده است و قبل از تلاش برای اتصال وجود نداشته است. برعکس، اگر واریانس قابل توجهی وجود نداشته باشد، یک قانون جریان قبلا وجود داشته است. از این رو، مهاجم از تجمع جریان برای کشف محتوای جداول جریان با مشاهده تفاوت در زمان پاسخ کنترلر استفاده می کند. با

تزریق قوانین جریان جعلی به سوییچ ها از طریق برنامه های مخرب روی کنترلرها، هکرها می توانند فایروال را دور بزنند و به سیستم شبکه حمله کنند که به آن تونل سازی جریان پویا[۲۶] می گویند.

حمله دستکاری داده ها در لایه داده SDN: یک نوع مهم از حملات دستکاری در SDN قوانین جریان کلاهبرداری است که به دلیل فقدان عدم تأیید و بررسی سازگاری است. یک مثال عینی از حمله دستکاری تونل سازی جریان پویا است که در آن یک مهاجم ممکن است سعی کند چندین قانون را تنظیم کند، جایی که هیچ جریانی هیچ یک از قوانین دیوار آتش را نقض نمی کند، اما در واقع می توانند قوانین دیوار آتش را به روشی مشترک نقض کنند. کنترل‌کننده OpenFlow می‌تواند قوانین مسیریابی جریان بهینه را از کلاینت‌های راه دور به منابع محاسباتی تقریباً تولید شده ایجاد کند.

حمله TCP در لایه داده SDN: دستگاه های تبادل داده از طریق TCP به کنترل از راه دور متصل می شوند. در نتیجه، یک مهاجم می تواند حملات شناخته شده در سطح TCP را برای نفوذ به شبکه راه اندازی کند. صرف نظر از استفاده از SSL بر روی TCP، بسیاری از حملات در سطح TCP وجود دارند که امنیت SDN را تهدید می کنند. این حملات می تواند به شکل حمله ICMP، حمله بازنشانی، حمله SYN، حمله پیش بینی توالی و حمله DoS باشد. با این حال، مشخصات OpenFlow نشان‌دهنده کاربرد پروتکل دیتاگرام کاربر (UDP) با امنیت لایه انتقال داده‌گرام (DTLS) است، اما هیچ ملاحظات کاملی در مورد نحوه پیاده‌سازی و استفاده از آن وجود ندارد.

حمله ذخیره سازی مسموم جداول جریان و وضعیت کنترلر: این نوع حمله به اصلاح غیرمجاز قوانین در جداول جریان اشاره دارد. مهاجمان می توانند قوانین جریان تقلبی را اضافه کنند که ممکن است باعث سوء رفتار شبکه شود. در این حمله از تزریق جعلی LLDP استفاده می شود که در آن یک مهاجم بسته های جعلی LLDP را در یک شبکه OpenFlow تولید می کند تا پیوندهای داخلی جعلی بین دو سوئیچ را ایجاد نماید. با مشاهده ترافیک سوئیچ های OpenFlow، مهاجم می تواند بسته واقعی LLDP را دریافت کند .

حمله فقدان احراز هویت: این حمله به دلیل عدم تأیید اعتبار در لایه داده رخ می دهد. بطور ویژه، عدم وجود تأیید هویت لایه داده (DPID) باعث ناامنی و بی ثباتی شبکه می شود. واکنش در برابر تکرارهای DPID به نحوه پیاده سازی کنترلر وابسته است که در آن برخی بسته ها را به همه سوئیچ هایی که دارای DPID یکسان هستند ارسال می کنند در حالی که برخی دیگر یک اتصال موجود را با دیگری با همان DPID جایگزین می کنند. مطالعه‌ای در مورد آسیب‌پذیری‌ها درکنترلرهای ONOS، Floodlight و ODL از طریق توسعه یک ردیابی توپولوژی شبکه که خود را به عنوان متعادل‌کننده بار با اعمال نفوذ در عدم احراز هویت بین کنترل‌کننده و برنامه‌های کاربردی مخفی می‌کند، انجام شد. یک برنامه مخرب ، مولفه شنونده Floodlight PacketIn را تغییر می دهد تا خود را اولین نفری کند که پیام های PacketIn را دریافت می کند نشان دهد و پس از حذف بخش Payload پیام را به برنامه علاقه مند بعدی ارسال می کند که پس از ایجاد اولین نمونه استثنا فاقد بخش Payload ، کنترل کننده Floodlight خود را از سوئیچ جدا می کند.

حمله اشباع در لایه داده SDN:: در این حمله ابتدا یک ماژول نگهداری بسته های از دست رفته در سوئیچ OpenFlow اضافه کردند که می تواند بسته هایی را که در جدول جریان مطابقت ندارند موقتاً کش کند. سپس، آنها مکانیزم جداسازی سرآیند و محتویات بسته‌ها را در صف کش در زمانیکه سوئیچ تشخیص میدهد که حجم صف کش بیش از آستانه اندازه کش است، اعمال کردند. علاوه بر این، سوئیچ می‌تواند سرآیند بسته‌ها را طبقه‌بندی کند و آن را در یک پیام هشدار برای پردازش بیشتر به کنترل‌کننده SDN ارسال کند.

۸. جمع بندی و محور های تحقیقاتی آینده حوزه SDN

در این مقاله به شرح کاملی از شبکه های نرم افزار محور پرداخته شد و همچنین پروتکل های برجسته بکار گیری شده در آن از جمله Openflow مورد بررسی قرار گرفت. معماری شبکه های نرم افزار محور تشریح گردید و ساختار عملکردی آن در

[26] Dynamic Flow Tunneling

Openflow بررسی گردید. ذکر این نکته ضروریست که شبکه های نرم افزار محور در حال حاضر در بخش عمومی و صنعت بعنوان یک تکنولوژی پذیرفته شده شناخته میشود واین نشان میدهد که با گذر زمان توانسته بر چالشهای پیش روی خود غلبه نماید. اما باید به این نکته توجه گردد که پروتکل ها و ابزارهای متفاوت پیاده سازی آن در گذر زمان در حال تکامل و بروزرسانی می باشد تا بتوانند هر چه بهتر و بیشتر بر چالشهای آینده در حوزه مالی(تجهیزات پشتیبانی کننده) و امنیتی فائق آیند. لازم به ذکر است که درتحقیقات جدید به استفاده از این تکنولوژی در حوزه هایی همچون اینترنت اشیا و محاسبات لبه و محاسبات مه توجه بسیاری زیادی شده است. شبکه‌های سنتی با چالش‌های مقیاس‌پذیری، تحویل بلادرنگ داده، قابلیت برنامه‌ریزی تحرک برای پشتیبانی از این اشیاء هوشمند که در مجموع به عنوان اینترنت اشیا شناخته می‌شوند، مواجه هستند .برای حل این مسائل، ادغام دو فناوری شبکه نوظهور، یعنی شبکه‌های نرم‌افزار محور و محاسبات مه، به عنوان یک مدل جدید که از معماری اینترنت اشیا برای مدیریت و تأخیر کم پشتیبانی می‌کند، شتاب بیشتری به دست آورده‌اند. به‌روزرسانی و توسعه پروتکل OpenFlow و معرفی پروتکل‌های جدید برای بهبود تعامل و امنیت در SDN و همچنین ایجاد پروتکل‌هایی که به‌طور خاص برای تأمین امنیت در محیط‌های SDN طراحی شده‌اند. همانطور که در ملاحظه میگردد با بهبود بخشیدن متریک های Openflow میزان از دست روی بسته ها را کاهش و کیفیت سرویس افزایش داده شده است. خودکارسازی سیاست‌های امنیتی به کمک پیاده‌سازی ابزارهای خودکار برای مدیریت و به‌روزرسانی سیاست‌های امنیتی در SDN و ارکستراسیون شبکه با استفاده از ابزارهای ارکستراسیون برای هماهنگی و مدیریت منابع شبکه به‌طور یکپارچه انجام خواهد شد. تحقیقات جدید در زمینه شناسایی و تحلیل آسیب‌پذیری‌های خاص SDN و ارائه راهکارهای بهبود و همچنین ارائه مدل‌های امنیتی جدید که به طور خاص برای محیط‌های SDN طراحی شده‌اند. در جدول (۵) سیر فعالیت های صورت گرفته و تهدیدات بررسی شده در حوزه امنیت شبکه های نرم افزار محور به تفکیک سال و به ترتیب مشاهده میگردد[۴۲]. با توجه به گسترش روز افزون شبکه های نرم افزار محور و همچنین رشد سایر تکنولوژی های موازی در کنار آن، امکان ادغام با سایر فناوری ها و توسعه هر چه بیشتر جهت رفع عیوب این شبکه ها وجود خواهد داشت. خصوصا از ظرفیت بسیار پویای این شبکه ها در تامین نیازهای تجهیزاتی شبکه های کشور نیز می توان بهره مند شد.

جدول(۷) : موضوعات تحقیقاتی حوزه امنیت SDN در گذر زمان

سال	۲۰۰۹	۲۰۱۰	۲۰۱۲	۲۰۱۳	۲۰۱۴	۲۰۱۶	۲۰۱۷
نوع /حوزه تهدید	Flow Visor	Flow Checker	FortNox	POCO	Flow	HoneyMix	DELTA
			VeriFlow	NSV	Payless	BGPSEX	DaaS
			LiveSec	Fresco	Rosemary	SHEILD	SODM
				Avant-Guard	DBA	UNISAFE	Distributed-SOM
					OrchSec	CPP	SLICOTS
					FlowGuard	DDos Detection	WedgeTail
					Firewell	OpenSec	Perm-Guard
					SPINX	NFG	
سال	۲۰۱۸	۲۰۱۹	۲۰۲۰	۲۰۲۱	۲۰۲۲	۲۰۲۳	۲۰۲۴
نوع /حوزه تهدید	Controller Security	Attack Mitigation	IoT Networks	AI/ML-Based	Quantum-Resistant	Critical Infrastructure	6G Networks
	(MitM)	Attacks on SDN Data Plane	Control Plane Attacks	Blockchain	5G and Beyond	Cloud Environments	Self-Healing
	(DDoS)	5G Networks	Controller Resilience	Autonomous Vehicle Networks	Zero Trust		
	(IDPS)[27]		Data Routing in Cloud Networks	Edge Computing			

[27] SDN-Based Intrusion Detection and Prevention Systems

جدول (۸) : جمع بندی انواع تهدیدات امنیتی حوزه SDN

اهداف	نوع تهدیدات	منشاء	ویژه SDN
حمله فیزیکی	حمله DDos در محیط UpnP	وجود ترافیک نا خواسته در زمانیکه ابزارهای نا همگون برای سرویسهایی همچون IOT به یکدیگر متصل میشوند تا تبادل اطلاعات کنند	میباشد
صفحه کنترل	از دست رفتن کنترل کننده	برنامه های مخرب به آسیب پذیری های رابط شمالی نفوذ مکنند.	میباشد
صفحه کاربرد	تهدیدات ناشی از برنامه های کاربردی	فقدان احراز هویت و شناسایی	میباشد
صفحه کنترل	حمله Spoofing	چک نکردن سازگاری و تایید در بروز رسانی های نصب شده و به خطر افتادن سویچ به دلیل عدم احراز هویت و عدم بکارگیری پروتکل TLS	نمیباشد
صفحه کنترل	حمله مرد میانی بین کنترلر و سویچ ها	عدم امن سازی کانال ارتباطی به کمک پروتکل TLS	نمیباشد
صفحه داد	شبکه های SDN مبتنی بر اثر انگشت	تفاوت زمان پردازش بسته ها بین شبکه SDN وسنتی	میباشد
صفحه کنترل	حمله منع سرویس در زمان پر شدن جدول جریان	کنترل کننده متمرکز و محدودیت جدول جریان	میباشد
صفحه داده	افشای اطلاعات	تفاوت زمانی پردازش بستهها که اطلاعات مربوط به محتویات جدول جریان را افشاء میکند	میباشد
صفحه داده	حمله Tempering به کمک قوانین جریان قلابی	عدم بررسی تایید هویت و سازگاری	نمیباشد

۹. فهرست **مراجع**:

[1] Jain Al S. b4: experience with a globally-deployed software defined wan. Acm Sigcomm Comput Commun Rev. 2013;43:3
[2] Foundation ON. Open netwoking foundation; 2017. Available from:http://www.Opennetworking.org
[3] Wetherall DJ, Guttag JV, Tennenhouse DL. Ants: a toolkit for building and dynamically deploying network protocols. IEEE Open Archit Network Program. 1998;1998:117–129.
[4] Bhattacharjee S, Calvert KL, Zegura WE. An architecture for active networking. In: Tantawy A. editor. High performance networking VII. IFIP — The International Federation for Information Processing; HPN; Boston, MA: Springer; 1997. p. 265–279.
[5] l AG. A clean slate 4d approach to network control and management. Acm SigcommComput Commun Rev. 2005;35:41–54.
[6] l MC. Sane: a protection architecture for enterprise networks. In: 15th Usenix security symposium; Vancouver, BC, Canada; 2006. p. 50.
[7] l MC. Ethane: taking control of the enterprise. In: ACM SIGCOMMcomputer communication review; January 2007; New York, NY: ACM. 2007;37(1):1–12.
[8] l MC. Ethane: taking control of the enterprise. In: ACM SIGCOMMcomputer communication review; January 2007; New York, NY: ACM. 2007;37(1):1–12
[9] Al NM. Openflow: enabling innovation in campus networks. Acm Sigcomm Comput Commun Rev. 2008;38:69–74.
[10] Al N. Nox: towards an operating system for networks. Acm Sigcomm Comput Commun Rev. 2008;38:105–110.
[11] Foundation ON. Open netwoking foundation; 2017. Available from: https://www. opennetworking.org/.
[12] undation ON. software-defined networking: the new norm for networks. ONF whitepaper. 2012;2:1–6.
[13] Benson, T., Akella, A., Maltz, D.A.: Network Traffic Characteristics of Data Centers in the Wild. In: Proceedings of the tenth ACM SIGCOMM Conference on Internet Measurement, New York, USA: ACM, pp. 267–280. (2010).
[14] Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., Shenker, S.: NOX: Towardsan Operating System for Networks", Computer Communication Review, (2008).
[15] Benson, T., Akella, A., Maltz, D.A.: Network Traffic Characteristics of Data Centers in the Wild. In: Proceedings of the tenth ACM SIGCOMM Conference on Internet Measurement, New York, USA: ACM, pp. 267–280. (2010).
[16] POX. (online) https ://www.noxre po.org/pox/about -pox/.

[17] Cai, Z., Cox, A.L., Ng, T.S: Maestro: A System for Scalable Open Flow Control", (2011).
[18] Floodlight Project. (online) https ://www.proje ctflo odlig ht.org/
[19] Dhawan, M., Poddar, R., Mahajan, K., Mann, V.: Sphinx: Detecting Security Attacks in Software Defined Networks. In: The proceedings of Network and Distributed System Security (NDSS) Sym- posium. The Internet Society, ISBN 1–891562–38-X, (2015).
[20] Zhu, L., Karim, M.M., Sharif, K., Li, F., Du, X., Guizani, M.: SDN Controllers: Benchmarking an Performance Evaluation. arXiv:1902.04491v1. [cs. NI] (2019).
[21] Phemius, K., Bouet, M., Leguay, J.: DISCO: Distributed Multi-Domain SDN Controllers", CoRR, vol. abs/1308.6138, (2013).
[22] Ryu SDN Framework. (online) https ://ryu-sdn.org/
[23] MUL SDN Contoller. (online) https ://www.openm ul.org
[24] Ilyas, Q., Khondoker, R.: "Security analysis of FloodLight, ZeroSDN, beacon and POX SDN con trollers" L. Notes Netw. Syst. 30, 85–98 (2018).
[25] Benson, T., Akella, A., Maltz, D.A.: Network Traffic Characteristics of Data Centers in the Wild. In: Proceedings of the tenth ACM SIGCOMM Conference on Internet Measurement, New York, USA: ACM, pp. 267–280. (2010).
[26] Muhammad Shoaib Farooq , Shamyla Riaz and Atif Alv, A.: Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review , Electronics 2023, 12, 3077. https://doi.org/10.3390/electronics12143077
[27] Botelho, F., Bessani, A., Ramos, F.M., Ferreira, P.: On the Design of Practical Fault-Tolerant SDN Controllers. In: Third European Workshop on Software Defined Networks, pp. 73–78, Sept (2014).
[28] Arash Shaghaghi,Mohamed Ali Kaafar,Rajkumar Buyya ,Sanjay Jha," Software-Defined Network (SDN) Data Plane Security: Issues,Solutions and Future Directions", Cluster Computing Journal in the second half of 2020.
[29] S. Ahmad, A. Hussain Mir, "Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers", Journal of Network and Systems Management,2021.
[30] Lara, A., Kolasani, A., Ramamurthy, B., 2014b. Network innovation using openflow: a survey. IEEE Commun. Surv. Tutor. 16 (1), 493–512.
[31] Abubakar, A., Pranggono, B., 2017. Machine learning based intrusion detection system for software defined networks. In: 2017 Seventh International Conference on Emerging Security Technologies. EST, pp. 138–143, https://doi.org/10.1109/EST.2017.8090413
[32] Al-Shabibi A. Flowvisor. Open Networking Lab; 2013. Retrieved from: https://github.com/OPENNET
[33] Hong Al S. Poisoning network visibility in software-defined networks: new attacks and countermeasures. NDSS Symposium 2015; San Diego, CA; 2015.
[34] Kloti R, Kotronis V, Smith P Openflow: A security analysis. 21st IEEE International Conference On Network Protocols (ICNP); Goettingen, Germany; 2013. p. 1–6.
[35] Antikainen M, Aura T, Särelä M Spook in your network: attacking an sdn with a compromised openflow switch. In: Nordic Conference on Secure IT Systems; Tromso, Norway; 2014. p. 229–244.
[36] Benton K, Camp LJ, Small C Openflow vulnerability assessment. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking; Hong Kong, China; 2013. p. 151–152.
[37] rooks M, Yang B A man-in-the-middle attack against opendaylight sdn controller. In: Proceedings of the 4th Annual ACM Conference on Research in Information Technology; Chicago, IL; 2015. p. 45–49.
[38] Scott-Hayward S, O'Callaghan G, Sezer S. Sdn security: A survey. IEEE SDN Future Networks Serv (SDNFNS). 2013;4:1–7.
[39] Al SS Avant-guard: scalable and vigilant switch flow management in software-defined networks. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security; Berlin, Germany; 2013. p. 413–424.
[40] Al SN. Enabling secure mobility with openflow. 2013 IEEE SDN Future Networks Serv (SDN4NFS). 2013;4:1–5.
[41] Reddy VK, Sreenivasulu D. Software-defined networking with ddos attacks in cloud computing. Int J Innovative Technol. 2016 Dec;04:3779–3783.
[42] Jinwoo Kim, M. Seo, S. Lee, and J. Namg, "Enhancing security in SDN: Systematizing attacks and defenses from a penetration perspective", Computer Networks 241, 1389-1286, 2024.

بررسی نقش اساسی نوع و پارامترهای کد مورد استفاده توسط سامانه‌ی رمزنگاری مک‌الیس در امنیت و کارایی این سامانه

سیده راضیه حسینی[۱]، نسرین سلطانخواه حقیقی[۲]، مهناز نوروزی[۳]

۱- گروه علوم ریاضی، دانشکده علوم ریاضی، دانشگاه الزهرا (س)

۲- گروه علوم ریاضی، دانشکده علوم ریاضی، دانشگاه الزهرا (س)

۳- گروه علوم کامپیوتر، دانشکده علوم ریاضی، دانشگاه الزهرا (س)

چکیده

سامانه‌های رمزنگاری متشکل از الگوریتم‌هایی هستند که می‌توانند برای حفاظت از اطلاعات و یا دیگرکاربردهای امنیتی مورد استفاده قرارگیرند. هر سامانه رمزنگاری مبتنی بر یک یا چند حوزه از ریاضیات مانند نظریه اعداد، خم‌های بیضوی و . . . طراحی می‌شود. دسته‌ای از سامانه های رمزنگاری نیز مبتنی بر نظریه کدگذاری بوده و از کدهای تصحیح کننده خطا استفاده می‌کنند که به آنها سامانه‌های کدمبنا می‌گویند. از آنجائیکه این سامانه‌ها می‌توانند در برابر حملات کوانتومی مقاومت کرده و با وجود عملیاتی شدن کامپیوترهای کوانتومی همچنان امنیت را برآورده نمایند، توجه جامعه رمزنگاری را به خود جلب کرده‌اند. در این تحقیق یک بررسی بر عملکرد یک سامانه‌ی رمزنگاری کدمبنا به نام مک‌الیس خواهیم داشت و مواردی چند از روش‌های نفوذ و حملات وارد بر آن را به طورکلی و به خصوص از دیدگاه حملات با رویکرد جبری که اساساً به ساختار جبری سامانه وارد می‌شوند مورد بررسی قرار می‌دهیم. در آخر ضمن ارائه یک مثال از این سامانه و دو رویکرد حمله علیه آن، یک جمع‌بندی در مورد الزامات کدهای مورد استفاده در این سامانه و اهمیت ساختار جبری آنها خواهیم داشت.

واژه‌های کلیدی: سامانه رمزنگاری مک‌الیس، رمزنگاری پساکوانتومی، حملات کدگشایی، حملات بحرانی، حملات غیربحرانی.

۱. مقدمه

کامپیوترهای کوانتومی دارای قدرت پردازشی بسیاربالا می‌باشند و عملکرد آنها اساساً با کامپیوترهای کلاسیک متفاوت است و با به کارگیری الگوریتم هایی مانند Shor[4] و Grover[5] می‌توانند مسئله تجزیه اعداد صحیح بزرگ و لگاریتم گسسته را که سختی آنها مبنای امنیت بسیاری از سامانه‌های رمزنگاری است، در زمان چندجمله‌ای حل کنند[۱]. رمزنگاری

1 Raziyehosseyni.68@gmail.com
2 soltan@alzahra.ac.ir
3 M.noroozi@alzahra.ac.ir
4 Peter Williston Shor
5 Lov Kumar Grover

پساکوانتومی رویکردی برای مقابله با تهدید کامپیوترهای کوانتومی است؛ که شامل طراحی و توسعه‌ی الگوریتم‌هایی در بسترکامپیوترهای کلاسیک است که با فرض در دسترس بودن کامپیوترهای کوانتومی و حملاتی که توسط آنها صورت می‌گیرد، همچنان اَمن باشند[۲]. در بررسی‌های صورت گرفته توسط سازمان‌های استانداردسازی مانند NIST[6]، ISO[7] و . . . در جهت توسعه رمزنگاری پساکوانتومی، رمزنگاری کدمبنا به ویژه طرح رمزنگاری مک‌الیس با مقاومت کوانتومی بالا معرفی شده است[۳]. از این رو بررسی و تجزیه تحلیل این سامانه‌ی رمزنگاری جهت ارائه‌ی هرگونه ایده برای توسعه‌ی امنیت و کارایی آن در قالب تحلیل نفوذ سامانه، بهبود پارامترهای کد مورد استفاده، و یا تغییر کد و دیگر رویکردها حائز اهمیت می‌باشد. این بررسی به گردآوری بخشی از پژوهش‌های صورت گرفته در مورد سامانه‌ی رمزنگاری مک الیس می‌پردازد و پس از ارائه خلاصه‌ای از مفاهیم جبری مورد استفاده، به شرح کلی عملکرد الگوریتم‌های سامانه‌ی رمزنگاری مک‌الیس پرداخته و فرضیه‌های اساسی تامین کننده‌ی امنیت در این سامانه، و انواع حملات ممکن علیه آن را بررسی می‌کند. در آخر با ارائه یک مثال از این سامانه و دو مورد از حملات وارد بر ساختار جبری آن خواهیم دید که کد مورد استفاده در این سامانه چه نقشی در عملکرد و امنیت آن خواهد داشت و الزامات کدهای مورد استفاده در این سامانه شامل چه مواردی خواهد بود.

۲. پیش‌نیازها

یک کد خطی C به طول n، بعد k و حداقل فاصله‌ی d را به صورت سه‌تایی $[n,k,d]$ نمایش می‌دهیم. همچنین پارامتر $t=\left\lfloor\frac{d-1}{2}\right\rfloor$ نیز قدرت تصحیح خطای کد C می‌باشد. کد خطی C را می‌توان با ماتریس مولد آن معرفی کرد که یک آرایه از اندازه‌ی $k\times n$ است که سطرهای آن اعضای یک پایه برای C هستند. همچنین حالت ساختار یافته یا به اصطلاح استاندارد ماتریس مولد یک کد خطی نیز به صورت $G=\left(I_k\middle|A_{k\times(n-k)}\right)$ نمایش داده می‌شود. یک ماتریس بررسی توازن برای کد C آرایه‌ای از اندازه‌ی $((n-k)\times n)$ است که سطرهای آن فضای پوچی کد C هستند. ماتریس بررسی توازن یک کد خطی با استفاده از فرم استاندارد ماتریس مولد آن به صورت $H=\left(-A^T\middle|I_{(n-k)}\right)$ نمایش داده می‌شود. همچنین دو مسئله مهم در نظریه کدگذاری به شرح زیر هستند.

مسئله‌ی کدگشایی[8]: فرض کنید $\mathbb{F}_q$ یک میدان متناهی و $k\le n$ اعداد صحیح و مثبت باشند. و فرض کنید یک ماتریس مولد $G\in\mathbb{F}_q^{k\times n}$ و یک بردار داده شده $c\in\mathbb{F}_q^n$ و $t\in\mathbb{N}$، ورودی های مسئله هستند. بردار $m\in\mathbb{F}_q^k$ و بردار $e\in\mathbb{F}_q^n$ را طوری بیابید که تساوی $c=mG+e$ برقرار باشد.

مسئله ی کدگشایی خطانما یا سیندرم[9]: فرض کنید $\mathbb{F}_q$ یک میدان متناهی و $k\le n$ اعداد صحیح و مثبت باشند؛ و فرض کنید یک ماتریس بررسی توازن $H\in\mathbb{F}_q^{(k-n)\times n}$ و یک سیندروم داده شده $s\in\mathbb{F}_q^{n-k}$ و $t\in\mathbb{N}$، ورودی‌های مسئله هستند. بردار $e\in\mathbb{F}_q^n$ را به شرط $wt_H(e)\le \mathrm{t}$، طوری بیابید که تساوی $eH^T=s$ برقرار باشد.

ثابت شده است که این دو مسئله با یک‌دیگر معادل هستند و در کلاس سختی NP-Complete قرار دارند[۴].

۳. سامانه رمزنگاری کدمبنا مک‌الیس:

این سامانه در سال ۱۹۷۸ توسط مک‌الیس، ریاضیدان و مهندس آمریکایی طراحی و معرفی شده است[۵]. اگرچه به طور کلی مک‌الیس یک سامانه‌ی رمزنگاری کلیدعمومی است، ولی ایده ضمینه‌ساز طراحی آن، سختی کدگشایی یک کد

[6] National Institute of Standards and Technology
[7] International Organization for Standardization
[8] Decoding Problem (DP)
[9] Syndrome Decoding Problem (SDP)

خطی تصادفی می‌باشد، نه مسائل سخت در حوزه‌ی نظریه اعداد. طرح اولیه‌ی سامانه‌ی مک‌الیس با به‌کارگیری کد گوپا[10] که دارای یک الگوریتم کدگشایی کارامد است عمل می‌کند. در شکل۱، سه الگوریتم تولید کلید، رمزگذاری و رمزگشایی سامانه‌ی رمزنگاری مک‌الیس به طور کلی بررسی شده است.

- در الگوریتم تصادفی[11] تولید کلید سامانه رمزنگاری مک‌الیس، یک کد خطی $[n,k]$ روی میدان F_q انتخاب می‌شود که توسط یک الگوریتم کدگشایی کارامد D_C، قابلیت تصحیح t خطا را نیز دارد. کاربر به جای ارسال ماتریس مولد کد C (در جدول زیر با G نمایش داده شده است.) به عنوان کلیدعمومی، آن را با ماتریس‌های جایگشتی P و درهم‌ساز S مخفی کرده و سپس ماتریس $A = SGP$ و عدد t را منتشر می‌کند. ضمناً ماتریس A هیچ اطلاعاتی را در مورد ساختار کد C فاش نمی‌کند.
- الگوریتم رمزگذاری تصادفی[12] به صورت کدگذاری پیام m با استفاده از ماتریس A و اعمال یک بردار خطای تصادفی به وزن همینگ t بر آن انجام می‌شود.
- انجام الگوریتم رمزگشایی نیز فقط برای کاربر قانونی مقدور است که کلید خصوصی را در اختیار دارد و با استفاده از آن خطا را تصحیح کرده و پیام m را بازیابی می‌کند.

پارامترها: $S_t^n = \{x \in F_2^n , wt(x) = t\}$; k, n, t و $wt(.)$ = وزن همینگ

$G \in F_2^{k\times n}$:

$S \in F_2^{k\times k}$: یک ماتریس غیر یکه

$P \in F_2^{n\times n}$: یک ماتریس جایگشتی

$A = SGP \in F_2^{k\times n}$: ماتریس مولد کد عمومی

$t \in \mathbb{N}, t \le \left\lfloor \frac{d-1}{2} \right\rfloor$: قدرت تصحیح خطا در کد C

کلید خصوصی: (S, P, G, D_C)، کلید عمومی: (A, t)

$\xrightarrow{(A,t)}$

رمزگذاری

بردار پیام: $m \in F_2^k$

بردار خطا: $e \in S_t^n$

بردار متن رمز شده: $y = mA + e$

$\xleftarrow{y=mA+e}$

رمزگشایی

$m' = yP^{-1} = mSGPP^{-1} + eP^{-1} = mS(G) + eP^{-1}$

$(Dec)_G(m') \to mS$

$mSS^{-1} \to m$

شکل ۱- الگوریتم‌های سامانه‌ی رمزنگاری کدمبنا مک‌الیس

[10] Goppa Code
[11] Probabilistic Algorithm
[12] Probabilistic Encryption

در تحلیل امنیت یک سامانه‌ی رمزنگاری کلید عمومی از هر نوع، ابتدا باید توجه داشت که امنیت آن سامانه‌ی رمزنگاری مبتنی بر چه فرضیه‌ها و چه مسائل سختی است که حل آنها امنیت سامانه را برهم خواهد زد. به طور کلی امنیت سامانه مک‌الیس به دو فرضیه محاسباتی متکی است[۶] :

۱) تشخیص کد عمومی (کلید عمومی) از یک کد تصادفی سخت است.

۲) کدگشایی یک کد تصادفی در مدل خطای ثابت سخت است که سختی این مسأله در [۴] ثابت شده است.

۴. برخی حملات و راه‌های نفوذ در سامانه رمزنگاری مک‌الیس[۷]:

سامانه‌ی رمزنگاری کدمبنای مک‌الیس، مانند دیگر سامانه‌های رمزنگاری کلید عمومی مورد حمله و نفوذ قرار می‌گیرد. حمله‌های وارد بر این سامانه شامل انواع مختلف و طیف گسترده‌ای هستند؛ با این حال می‌توان به طور کلی حملات نام‌برده در شکل۲ را برای آنها در نظر گرفت.

انواع حملات					
ساختاری	کانال جانبی	جبری	کوانتومی	کدگشایی	
				غیربحرانی	بحرانی

شکل۲- رویکردهای مختلف حملات وارد بر سامانه‌ی رمزنگاری مک‌الیس

i) حملات ساختاری[۱۳]

در حملات ساختاری هدف یافتن کلید خصوصی با استفاده از کلید عمومی است. حمله کننده سعی دارد تا به کلید خصوصی دسترسی پیدا کند و با استفاده از ساختار کد تصادفی یا همان کلید عمومی، کلید خصوصی را بازیابی کند. موارد زیر دو مورد از حملات ساختاری به شمار می‌روند.

۱. حمله‌ی جست و جوی فراگیر[۱۴]: حمله کننده سعی دارد تا در میان تمام ماتریس‌های درهم‌ساز $S \in F_q^{k\times k}$، تمام ماتریس‌های مولد $G \in F_q^{k\times n}$ و تمام ماتریس‌های جایگشتی $P \in F_q^{n\times n}$، جست‌وجو کرده و هر بار با ساختن $A = SGP$ و تطبیق آن با کلید عمومی ماتریس مولد کد به کار رفته در سامانه را پیدا کند. البته که قطعا این روش به صرفه نیست و بسیار بسیار وقت‌گیر و پرهزینه می‌باشد.

۲. استفاده از ضعف‌های ساختاری یا ساختار منظم کد به کاربرده‌شده در سامانه، که تشخیص کلید خصوصی را از کلید عمومی امکان‌پذیر سازد. مانند ضعف در ساختار برخی کدهای به کار برده شده در سامانه برای مثال ضعف در ساختار کدهای GRS[۱۵] وReed muller که منجر به بازیابی کلید خصوصی از کلید عمومی است. درنتیجه می‌توان ساختار و نوع کد مورد استفاده در سامانه‌ی مک‌الیس را در نفوذ پذیری و شکست آن بسیار مؤثر دانست. تاکنون کدهای خطی متعددی برای به‌کارگیری در سامانه‌ی مک‌الیس

[13] **Structural attacks**
[14] **Brute force attack**
[15] **Generalized Reed Solmon**

استفاده شده‌اند با این حال بسیاری از آنان در برابر حملات شکسته شده‌اند. علاوه بر ساختار کد، پارامترهای آن نیز در میزان آسیب‌پذیری سامانه بسیار مؤثر هستند.

ii) حملات کانال جانبی[16]

در حملات کانال جانبی هدف یافتن اطلاعاتی درباره کلید خصوصی و یا پیام در پیاده‌سازی‌های سخت افزاری و نرم افزاری است، با فرض در اختیار بودن ابزار رمز (حمله های متن رمزشده انتخابی). این حملات می‌توانند از در دسترس‌ترین سخت افزارها مانند اجزای فیزیکی تا انرژی مصرفی در پیاده‌سازی‌های نرم افزاری را شامل شوند. مانند حملاتی که زمان یا توان مصرفی استفاده شده برای انجام یک الگوریتم یا قسمتی از آن در سامانه‌ی رمزنگاری را اندازه‌گیری یا تحلیل و تفسیر می‌کنند.

iii) حملات جبری[17]

دسته‌ی دیگری از روش‌های بازیابی کلید علاوه بر حملات ساختاری بر اساس تجزیه و تحلیل‌ها و معادلات جبری می‌باشند در این حملات، هدف استفاده از مفاهیم جبری برای تشخیص ساختار کد اصلی یا به عبارتی تشخیص ماتریس مولد کد به کار برده شده است. در واقع مسئله‌ی بازیابی کلید خصوصی را می‌توان به عنوان یک دستگاه معادلات چندجمله‌ای بازنویسی کرد که حل دستگاه منجر به بازیابی کلید خصوصی می‌شود. حملات جبری می‌توانند سامانه‌ی کدمبنا با کلید خصوصی‌های فشرده (کوتاه) را شکست دهند و علاوه بر آن در کدهایی با نرخ نزدیک به یک می‌توانند ماتریس مولد کد خصوصی را از کد عمومی تصادفی تشخیص دهند.

iv) حملات کوانتومی

حملات کوانتومی در واقع اجرای الگوریتم‌هایی در کامپیوترهای کوانتومی هستند. مانند الگوریتم شور[۱] که به یک کامپیوتر کوانتومی این امکان را می‌دهد تا در زمان کارامد مسائل سخت لگاریتم گسسته و تجزیه اعداد صحیح بزرگ را حل نماید.

v) حملات کدگشایی[18]

در این حملات هدف تصحیح خطا و بازیابی پیام اصلی است. می‌توان آن‌ها را به دو بخش جزئی‌تر با عنوان‌های حملات بحرانی و حملات غیربحرانی نیز تقسیم‌بندی کرد.

حملات غیربحرانی:
یک حمله‌ی غیر بحرانی سعی دارد تا کلید خصوصی یا پیام را به صورت ترکیبی و بدون بکارگیری ساختارهای جبری بازیابی کند. همچنین با افزایش پارامترها امنیت مورد نظر نسبت به این حملات حاصل می‌شود.

[16] **Side channel attacks**
[17] **Algebraic attacks**
[18] **Decoding attacks**

- حمله‌ی کدگشایی مجموعه اطلاعات[۱۹]: الگوریتم‌های (ISD) مؤثرترین حملات علیه سامانه‌های رمزنگاری مبتنی برکد هستند. آنها تلاش می‌کنند تا مسئله‌ی کدگشایی عمومی را حل کنند. یعنی اگر بردار m یک متن اصلی باشد و بردار $c = mG + e$ متن رمزشده باشد که در آن e بردار خطا به وزن t و G نیز ماتریس مولد کد مورد استفاده در سامانه رمزنگاری است. آن‌گاه الگوریتم‌های ISD تلاش می‌کنند تا c را به عنوان ورودی گرفته و متقابلاً m (یا به طور معادل e) را بازیابی کنند[۸].
- الگوریتم تولد تعمیم یافته[۲۰]: این الگوریتم سعی دارد تا مسئله‌ی کدگشایی سیندرم را حل کند. یعنی برای ماتریس زوج آزمایی H داده شده و بردار سندرم s و عدد صحیح t، تلاش می‌کند تا بردار e با وزن همینگ $w_h(e) = t$ را به نحوی پیدا کند که تساوی $He^T = s^T$ برقرار باشد[۸]. به عبارت دیگر در یک کد دودویی این الگوریتم سعی دارد تا مجموعه‌ای از ستون‌های ماتریس H را پیدا کند که مجموع وزنی آنها برابر با بردار سیندرم داده شده باشد.

حملات بحرانی:

این حملات نیازمند اطلاعات اضافی از جمله قسمتی از پیام رمزشده و یا ارتباط دو متن رمزشده هستند. این حملات زمانی که حمله کننده قابلیت‌های اضافه‌تر دارد ممکن هستند؛ و درواقع نمی‌توان گفت به تنهایی برای بازیابی پیام یا کلید خصوصی کافی می‌باشند. اما در کاهش پیچیدگی حملات بازیابی پیام یا کلید مؤثر هستند. منظور از اطلاعات اضافه‌ای که یک مهاجم می‌تواند داشته باشد در اختیار داشتن اوراکل تصادفی[۲۱] و یا در اختیار داشتن بخشی از یک متن ساده، دانستن ارتباط دو متن ساده و . . . است. همچنین با افزایش دادن پارامترهای کد نمی‌توان از آنها جلوگیری کرد. حمله‌ی پخش[۲۲]، حمله با متن اصلی جزئی معلوم[۲۳]، حمله‌ی پیام مرتبط[۲۴] ، حمله با ارسال مجدد پیام[۲۵]، حمله با متن اصلی منتخب[۲۶]، حمله با متن رمز منتخب[۲۷]، حمله‌ی واکنشی[۲۸] از انواع حملات غیربحرانی هستند.

۵. یک نمونه از سامانه‌ی رمزنگاری مک‌الیس با به‌کارگیری کد همینگ و دو رویکرد حمله علیه آن[۵]:

در بخش فوق به معرفی راه‌های نفوذ و حمله به سامانه‌ی رمزنگاری کدمبنا مک‌الیس پرداختیم. حال در این بخش یک مثال ساده از عملکرد آن را با استفاده از یک کد دودویی همینگ [7,4,3] بررسی می‌کنیم و سپس دو حمله با رویکرد جبری را توضیح خواهیم داد. ارائه‌ی این مثال گواه بر آن است که در عمل به‌کارگیری یک کد با ساختار جبری ساده به هیچ عنوان آمن نخواهد بود و سامانه‌ی مک‌الیس با استفاده از چنین کدهایی در عمل غیرقابل استفاده است. همچنین از تعاریف کوتاهی که برای انواع حملات ممکن علیه این سامانه تعریف شد، نتیجه می‌شود که ساختار و پارامترهای کد مورد استفاده

[19] **Information Set Decoding (ISD) Attack**
[20] **Generalized Birthday Algorithm (GBA)**
[21] **Random Oracle**
[22] **Broadcast attack**
[23] **Known partial plaintext attack**
[24] **Related-message:**
[25] **Message-resend attack**
[26] **Chosen plaintext (CPA)**
[27] **Chosen-ciphertext attack (CCA)**
[28] **Reaction attack**

در این سامانه نقش اساسی را در امنیت و عملکرد آن خواهند داشت. لذا همواره تلاش برای بهبود پارامترها و نوع خاص کد مورد استفاده در این سامانه از اهمیت بسیاری برخوردار است.

۱.۵ سامانه‌ی رمزنگاری مک‌الیس با استفاده از کد همینگ [7,4,3]:

فرض کنید C یک کد دودویی [7,4,3] همینگ است، که به طور کارامد قابلیت تصحیح ۱ خطارا دارد. ماتریس مولد آن را به صورت زیر درنظر می‌گیریم

$$G = \begin{pmatrix} 1&0&0&0&1&1&0 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \end{pmatrix}$$

همچنین ماتریس‌های $S \in M^{4\times4}$ و $P \in M^{7\times7}$ با درایه‌هایی از $\mathbb{Z}_2$ را به صورت زیر انتخاب می‌کنیم.

$$S = \begin{pmatrix} 0&1&1&1 \\ 1&0&1&1 \\ 1&0&1&0 \\ 0&0&1&1 \end{pmatrix} \qquad P = \begin{pmatrix} 0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}$$

حال با ضرب ماتریس مولد کد همینگ در ماتریس‌های جایگشت و درهم‌ساز انتخاب شده یک ماتریس مولد (G') تولید خواهد شد که در مورد کد به‌کار برده شده اطلاعات کارامدی را ارائه نمی‌دهد و به عنوان ماتریس مولد یک کد تصادفی درنظر گرفته می‌شود. در این صورت $(G', 1)$ به عنوان کلید عمومی منتشر می‌شوند.

$$G' = SGP = \begin{pmatrix} 1&0&0&1&0&1&1 \\ 1&1&1&0&0&1&0 \\ 0&1&0&0&1&1&1 \\ 1&0&0&1&1&0&0 \end{pmatrix}$$

فرستنده می‌خواهد پیام $m = (1\ 0\ 1\ 1) \in \mathbb{F}_2^4$ را با استفاده از کلید عمومی گیرنده رمزنگاری کند، این فرایند معادل با کدگذاری بردار m و اضافه کردن یک بردار خطای تصادفی e است و به صورت زیر اجرا می‌شود.

$$c = mG' + e \quad e = (1\ 0\ 0\ 0\ 0\ 0\ 0) \in \mathbb{F}_2^7 \quad mG' = (0\ 1\ 0\ 1\ 0\ 1\ 0)$$
$$c = (1\ 1\ 0\ 1\ 0\ 1\ 0)$$

حال متن رمزگذاری‌شده c به گیرنده ارسال می‌شود و گیرنده نیز محاسبات زیر را برای بازیابی پیام m انجام می‌دهد.

$$cP^{-1} = cP^T = mSG + eP^{-1} = (1\ 1\ 1\ 1\ 0\ 0\ 0)$$

سپس با استفاده از الگوریتم تصحیح خطایی که برای کد همینگ [7,4,3] در اختیار دارد خطای صورت گرفته را تصحیح کرده و بردار mS را به عنوان خروجی می‌دهد. با ضرب بردار $mS = (1\ 1\ 1\ 0)$ در ماتریس S^{-1} که به صورت زیر است، پیام m بازیابی می‌شود.

$$S^{-1} = \begin{pmatrix} 0\,1\,0\,1 \\ 1\,0\,0\,1 \\ 0\,1\,1\,1 \\ 0\,1\,1\,0 \end{pmatrix} \qquad mSS^{-1} = (1\ 0\ 1\ 1)$$

مثال فوق سامانه رمزنگاری مک‌الیسی است که با استفاده از یک کد دودویی همینگ $[7,4,3]$ کار می‌کند تاکنون انواع بسیاری از کدهای تصحیح کننده‌ی خطا با پارامترهای بهینه در این سامانه به کار برده شده‌اند.

۲.۵ بررسی دو حمله با رویکرد جبری برای احراز ساختار نامناسب کد به‌کار برده شده:

برای این بررسی، مثال فوق را در نظر می‌گیریم. با توجه به اینکه حمله‌کننده کلید عمومی (G', t) و متن رمزشده‌ی c را در اختیار دارد می‌تواند دو رویکرد در تصمیم خود داشته باشد.

۱. بازیابی مستقیم پیام m.

۲. بازیابی کلید خصوصی یا به اصطلاح همان ساختار کد اصلی.

حمله‌ی نوع اول به صورت زیر عمل می کند.

ماتریس مولد عمومی را با عملیات سطری مقدماتی به حالت ساختار یافته‌ی آن که در بخش دو توضیح داده شد تبدیل می کند. سپس با استفاده از $\bar{G}$ ماتریس بررسی توازن به راحتی قابل محاسبه است.

$$G' = (A \mid B), \qquad A^{-1}G' = \bar{G} = (I_4 \mid M_{4\times 3}) = \begin{pmatrix} 1\,0\,0\,0 & 1\,1\,0 \\ 0\,1\,0\,0 & 1\,1\,1 \\ 0\,0\,1\,0 & 0\,1\,1 \\ 0\,0\,0\,1 & 1\,0\,1 \end{pmatrix}$$

$$\bar{G} \to \bar{H} = (-M^T \mid I_3) = \begin{pmatrix} 1\,1\,0\,1 & 1\,0\,0 \\ 1\,1\,1\,0 & 0\,1\,0 \\ 0\,1\,1\,1 & 0\,0\,1 \end{pmatrix}$$

حمله کننده می‌تواند خطانمای بردار c را با استفاده از $\bar{H}$ محاسبه کند، که بردار حاصل همان خطانمای بردار e می‌باشد

$$s = c\bar{H}^T = (1\ \ 1\ \ 0) = e\bar{H}^T$$

البته در کد همینگ $[7,4,3]$ با توجه به اینکه $t = 1$، خطانما برابر با ستون jاُم ماتریس بررسی توازن خواهد بود، که دراین‌صورت در بردار خطا داریم $e_j = 1$ در نتیجه بردار خطا و پیام اصلی به راحتی قابل بازیابی خواهند بود.

$$e = (1\ 0\ 0\ 0\ 0\ 0\ 0)$$
$$mG' = c - e = (0\ 1\ 0\ 1\ 0\ 1\ 0)$$
$$\bar{m} = mA$$
$$mG' = mAA^{-1}G' = \bar{m}\bar{G}, \qquad \bar{G} = (I_4 \mid M_{4\times 3})$$
$$\bar{m}\bar{G} = (\bar{m} \mid \bar{m}M)$$

سپس با ضرب $\bar{m}$ در ماتریس A^{-1} پیام اصلی بازیابی می شود.

حمله‌ی نوع دوم به صورت زیر عمل می کند.

۱. حمله‌کننده یک زیرمجموعه از اندیس‌ها مانند $I \subset \{1, \dots n\}$ از اندازه‌ی k را انتخاب می‌کند، که یک مجموعه‌ی اطلاعات می‌باشد. همچنین ماتریس G'_I را با استفاده از ستون‌های ماتریس G' که اندیس آنها در I است، تشکیل می دهد.

۲. سپس با محاسبه‌ی $(G'_I)^{-1}G'$ یک ماتریس از اندازه ی $k \times n$ به دست می‌آورد که ستون‌های اندیس‌گذاری شده با اعضای مجموعه‌ی I در آن یک ماتریس همانی تشکیل می‌دهند.

۳. ماتریس جایگشت P' را به گونه‌ای انتخاب می‌کند که ماتریس همانی موجود در ستون‌های اندیس‌گذاری شده با اعضای I را به k ستون اول ماتریس A انتقال دهد.

این روش در نهایت منجر به بازیابی ماتریس مولد کد اصلی یعنی G و به دست آوردن الگوریتم کدگشایی برای آن خواهد شد. همچنین با داشتن G' و G بازیابی ماتریس‌های P و S نیز ممکن خواهد بود.

۶. الزامات کد به‌کار برده شده در سامانه‌ی رمزنگاری کدمبنا مک‌الیس

سامانه‌ی مک‌الیس اولیه که در سال ۱۹۷۸ معرفی و منتشر شده است، با به‌کارگیری کد باینری گوپا با پارامترهای $[1024,524]$ عمل می‌کند. اگرچه بزرگی اندازه‌ی ماتریس مولد این کد، فضای ذخیره‌سازی زیادی را اشغال می‌کند، اما به‌کارگیری این کد نسبت به دیگر کدهای پیشنهاد شده تا به حال از امنیت بهتری برخوردار بوده است[۶] . طبق نتایج به‌دست آمده از به‌کارگیری انواع دیگر کدهای تصحیح کننده‌ی خطا در این سامانه رمزنگاری می‌توان برخی الزامات را برای کدهای به کار برده شده در نظر گرفت.

۱. کد مورد نظر باید دارای الگوریتم کدگشایی کارامد باشد تا کاربر قانونی بتواند فرایند تصحیح خطارا به طور کارامد انجام دهد.

۲. کد مورد نظر باید قابلیت تصحیح خطای بالایی داشته باشد که این مستلزم بزرگ بودن پارامتر حداقل فاصله در کد است؛ چرا که اگر قابلیت تصحیح خطای کد مورد استفاده در سامانه مک‌الیس کوچک باشد با یک جست و جوی ساده می‌توان بردار خطای اِعمال شده در رمزگذاری را به دست آورد و پیام را بازیابی کرد.

۳. نتایج موجود نشان می‌دهند که ساختار جبری و مجموعه پارامترهای کد مورد استفاده در سامانه‌ی مک الیس می‌تواند در مقاومت آن در برابر برخی حملات مؤثر باشد از جمله اینکه ادعا شده است در حال حاضر تنها برای برخی مجموعه پارامترهای خاص کدهای گوپا حملات جبری موفق وجود دارد [۹ و ۱۰] و در واقع برای تعداد زیادی از مجموعه پارامترهای کدهای گوپا هنوز هیچ خاصیت جبری شناخته نشده است که بتواند آنها را از یک کد تصادفی قابل تشخیص سازد[۶] .

۴. همچنین از دیگر الزامات کد مورد استفاده در این سامانه بزرگ بودن مجموعه‌ی کدهای هم‌عرض با آن است، به این معنی که تعداد زیادی کد با پارامترهای مشابه آن وجود داشته باشند چراکه پارامترهای کد عمومی نباید ساختار کد خصوصی را آشکار کنند.

۷. نتایج پیاده‌سازی

سامانه‌ی رمزنگاری مک‌الیس تاکنون در بسترهای سخت‌افزاری و نرم‌افزاری متفاوتی پیاده‌سازی شده است[۱۱]، که در میزان آسیب‌پذیری این سامانه نسبت به حملات کانال جانبی تفاوت ایجاد می‌کنند. تغییر در زمان اجرای الگوریتم‌ها، و یا در توان مصرفی سخت افزارها ممکن است به عنوان نشت اطلاعات، منجر به بهبود عملکرد حملات کانال جانبی شود[۱۲] . برای مثال اخیراً یک حمله‌ی کانال جانبی موفق بر یک سامانه کپسوله سازی کلید مک‌الیس کلاسیک با موفقیت اعمال شده است[۱۳]. از آنجایی که هدف ما در این تحقیق، بررسی عملکرد کد مورد استفاده در سامانه‌ی مک‌الیس است. لذا با فرض پیاده‌سازی سامانه‌ی مک‌الیس در یک بستر سخت افزاری و نرم افزاری مشخص، تنها به بررسی نتایج به‌کارگیری کدهایی با ساختار جبری متفاوت در این سامانه می‌پردازیم.

در پژوهش‌های صورت‌گرفته از زمان انتشار سامانه‌ی مک‌الیس اولیه، همواره پیشنهادهای بسیاری برای استفاده از دسته‌بندی خاص و یا پارامترهای خاصی از یک نوع کد تصحیح کننده‌ی خطا ارائه می‌شود. و درپی آن پیشنهادهای بسیاری نیز در قالب رویکردهای حمله و نفوذ به این سامانه ارائه می‌شود. و جامعه‌ی رمزنگاری همواره در تلاش است تا ضمن حفظ و بهبود سطوح امنیت این سامانه، کارایی آن را نیز در عمل بهبود بخشد. با وجود اینکه کدهای گوپا عملکرد خوبی از نظر سطح امنیت از خود نشان داده‌اند اما مشکل بسیار جدی آنها اندازه‌ی بزرگ کلید عمومی است. برای مثال در مقایسه با سامانه رمزنگاری کلید عمومی RSA[29] [۱۴]، در جدول زیر نتایج سامانه مک‌الیس با به‌کارگیری چند کدگوپا با پارامترهای مختلف ارائه شده است[۱۵] .

جدول ۱- مقایسه کلید عمومی سامانه رمزنگاری RSA و مک‌الیس با به‌کارگیری چند کد گوپا

سطح امنیت(bits)	[n,k]	T	اندازه‌ی کلید عمومی (bits)	اندازه‌ی کلید عمومی در RSA(bits)
80	[1632, 1269]	33	469647	512
126	[2960, 2288]	56	1537536	3072
256	[6624,5129]	115	7667855	15360

از این‌رو پیشنهادهای بسیاری برای استفاده از کدهای جایگزین در این سامانه‌ی رمزنگاری تاکنون ارائه شده است. برای مثال استفاده از کدهای گوپای غیردودویی[۱۶]. استفاده از کدهای هندسه جبری[۱۷]. کدهای LDPC[30] و MDPC[31] [۱۸و۱۹] . کدهای ریدمولر[32][۲۰] و کانولوشنال[33][۲۱] که البته بیشتر آنها در مخفی نگه داشتن ساختار کلید خصوصی ناموفق بوده‌اند. همچنین اخیراً در سال ۲۰۲۳ در [۲۲] یک سامانه‌ی رمزنگاری مک‌الیس با استفاده از کدهای خوددوگان با حداقل فاصله‌ی زیاد معرفی شده است که توانسته است ضمن برقراری سطح امنیت مطلوب اندازه کلید عمومی را ۳۸٪ کاهش دهد. البته در این مقاله مشخص شده است که در الگوریتم کدگشایی این کد یک ضعف وجود دارد

[29] Rivest-Shamir-Adelman
[30] Low-Density Parity Check Codes
[31] Mediom-Density Parity Check Codes
[32] Reed-Muller
[33] Convolutional

که ملزم به بررسی‌های بیشتر می‌باشد. همچنین یک سامانه‌ی مک‌الیس با به‌کارگیری کدی که از دو کد خطی دلخواه ساخته می شود ادعا می‌کند به‌کارگیری چنین کدی ضمن برقراری سطح امنیت مطلوب منجر به کاهش ۲۵٪ اندازه کلید عمومی خواهد شد[۲۳] . به منظور کاهش اندازه‌ی کلید سامانه‌ی مک الیس کدهای شبه‌دوری و دوری بیشترین پیشنهادها را به خود اختصاص می‌دهند اما به دلیل اینکه عموماً ساختار کلید خصوصی را فاش می‌کنند همواره حملات موفقی علیه آنها صورت می‌گیرد[۲۴].

۸. نتیجه گیری

در آخر و به عنوان سخن پایانی در این تحقیق ضمن بررسی مثال ارائه شده از سامانه مک‌الیس با به‌کارگیری کد همینگ و نقش ساختار کد مورد استفاده در حملات صورت‌گرفته بر این سامانه و مواردی که در نتایج پیاده سازی‌ها به آن اشاره کردیم نتیجه می‌شود که انتخاب دسته بندی و پارامترهای خاصی از کدهای تصحیح کننده‌ی خطا که در الزامات مورد نیاز سامانه صدق می‌کنند می‌تواند تأثیر بسیار جدی و اساسی بر امنیت و عملکرد سامانه‌ی رمزنگاری مک‌الیس داشته باشد. همچنین روشن است که مطالعات در حوزه‌ی کدهای تصحیح کننده‌ی خطا و توسعه‌ی آنها زمینه ساز توسعه‌ی سامانه‌ی رمزنگاری مک‌الیس و دیگر سامانه‌های کدمبنا خواهد بود. این موضوع انگیزه‌ای برای تحقیق در زمینه‌های مختلف از جمله مطالعه و طراحی الگوریتم‌های کدگشایی کارامد برای کدهایی با پارامتر و ساختار مطلوب، می‌باشد. برای مثال در سال ۲۰۲۱ در [۲۵] وجود الگوریتم کدگشایی نسبتاً خوب برای دسته‌ی خاصی از کدهای خوددوگان اثبات شده و دو سال بعد، این کدها با داشتن الگوریتم کدگشایی در سامانه‌ی مک‌الیس به‌کار برده شده‌اند[۲۲]. همچنین از دیگر ابعاد تحقیقاتی در این زمینه می‌توان به طراحی و توسعه الگوریتم‌هایی برای تشخیص هم‌ارزی میان دسته خاصی از کدهای تصحیح کننده‌ی خطا پرداخت. برای مثال بررسی هم ارزی میان کدهای دوری، که منجر به ساخت کدهای جدید می‌شود و در نهایت به‌کارگیری آنها می‌تواند در کاهش اندازه‌ی کلید در سامانه‌ی مک‌الیس مؤثر واقع شود[۲۶] .

مراجع

[1] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303-332.

[2] Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. *Cryptography*, *7*(3), 40.

[3] Balamurugan, C. Singh, K. Ganesan, G. & Rajarajan, M. (2021). Post-quantum and code-based cryptography—some prospective research directions. *Cryptography*, *5*(4), 38.

[4] E. Berlekamp and R. McEliece and H. Van Tilborg. (1978). "On the inherent intractability of certain coding problems", *IEEE Transactions on Information Theory*, 24(3):384– 386.

[5] McEliece, R. J. (1978). A public key cryptosystem based on algebraic, *coding theory*, DSN progress report 42–44, pp. 114–116.

[6] Weger, V. Gassner, N. and Rosenthal, J. (2022).A survey on code-based cryptography, *arXiv preprint arXiv:2201.07119*.

[7] Wang, J. Liu, L. Lyu, S. Wang, Z. Zheng, M. Lin, F. ... & Ling, C. (2022). Quantum-safe cryptography: crossroads of coding theory and cryptography. *Science China Information Sciences*, *65*(1), 111301.

[8] D. Engelbert and R. Overbeck and A. Schmidt, (2007). A summary of McEliece-type cryptosystems and their security, *Journal of Mathematical Cryptology*, *1*(2), 151-199.

[9] Couvreur, A., Otmani, A., & Tillich, J. P. (2016). Polynomial time attack on wild McEliece over quadratic extensions. *IEEE Transactions on Information Theory*, *63*(1), 404-427.

[10] Faugere, J. C., Gauthier-Umana, V., Otmani, A., Perret, L., & Tillich, J. P. (2013). A distinguisher for high-rate McEliece cryptosystems. *IEEE Transactions on Information Theory*, *59*(10), 6830-6844.

[11] López-García, M. & Cantó-Navarro, E. (2020). Hardware-software implementation of a McEliece cryptosystem for post-quantum cryptography. In *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 2* (pp. 814-825). Springer International Publishing.

[12] Chen, P. J. Chou, T. Deshpande, S. Lahr, N. Niederhagen, R. Szefer, J. & Wang, W. (2022). Complete and improved FPGA implementation of classic McEliece. *Cryptology ePrint Archive*.

[13] Drăgoi, V. F. Colombier, B. Vallet, N. Cayrel, P. L., & Grosso, V. (2025). Full Key-Recovery Cubic-Time Template Attack on Classic McEliece Decapsulation. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2025*(1), 367-391.

[14] Rivest, R. L. Shamir, A. and Adleman, L. (1983). A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, vol. 26, no. 1, pp. 96–99, Jan.

[15] Bucerzan, D., Dragoi, V., & Kalachi, H. T. (2017). Evolution of the McEliece public key encryption scheme. In *Innovative Security Solutions for Information Technology and Communications: 10th International Conference, SecITC 2017, Bucharest, Romania, June 8–9, 2017, Revised Selected Papers 10* (pp. 129-149). Springer International Publishing.

[16] Bernstein, D. J., Lange, T., & Peters, C. (2010, August). Wild mceliece. In *International Workshop on Selected Areas in Cryptography* (pp. 143-158). Berlin, Heidelberg: Springer Berlin Heidelberg.

[17] Janwa, H., & Moreno, O. (1996). McEliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes and Cryptography*, *8*(3), 293-307.

[18] Baldi, M., Bodrato, M., & Chiaraluce, F. (2008). A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In *Security and Cryptography for Networks: 6th International Conference, SCN 2008, Amalfi, Italy, September 10-12, 2008. Proceedings 6* (pp. 246-262). Springer Berlin Heidelberg.

[19] Monico, C., Rosenthal, J., & Shokrollahi, A. (2000, June). Using low density parity check codes in the McEliece cryptosystem. In *2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060)* (p. 215). IEEE.

[20] Sidelnikov, V. M. (1994). A public-key cryptosystem based on binary Reed-Muller codes.

[21] Löndahl, C., & Johansson, T. (2012). A new version of McEliece PKC based on convolutional codes. In *Information and Communications Security: 14th International Conference, ICICS 2012, Hong Kong, China, October 29-31, 2012. Proceedings 14* (pp. 461-470). Springer Berlin Heidelberg.

[22] Mariot, L., Picek, S., & Yorgova, R. (2023). On McEliece-type cryptosystems using self-dual codes with large minimum weight. *IEEE access*, *11*, 43511-43519.

[23] Bindal, E., & Singh, A. K. (2024). Secure and Compact: A New Variant of McEliece Cryptosystem. *IEEE Access*.

[24] Ayoub Otmani, Jean-Pierre Tillich, and L´eonard Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. Mathematics in Computer Science, 3(2):129– 140, 2010.

[25] Yorgova, R. (2021). On decoding of a specific type of self-dual codes. *arXiv preprint arXiv:2106.11146*.

[26] Aydin, N. & VandenBerg, R. O. (2023). A new algorithm for equivalence of cyclic codes and its applications. *Applicable Algebra in Engineering, Communication and Computing*, *34*(4), 649-661.

مدل CTran: رویکردی نوین برای تشخیص دستورات صوتی در خانه‌های هوشمند

ساره مستخدمین حسینی [1]، علیرضا نعیمی صدیق [2و*]

1- دانشجوی کارشناسی ارشد علوم کامپیوتر – دانشگاه سمنان

2- عضو هیات علمی گروه علوم کامپیوتر- دانشگاه سمنان

چکیده

در حوزه خانه‌های هوشمند، کنترل دستگاه‌ها و لوازم خانگی از طریق دستورات صوتی به یکی از موضوعات کاربردی و جذاب تبدیل شده است. این فناوری با تشخیص الگوهای گفتاری، به کاربران امکان می‌دهد تا به‌طور دقیق و مؤثر، لوازم منزل را کنترل کنند. الگوریتم‌های پیشرفته یادگیری ماشین، یادگیری عمیق و پردازش زبان طبیعی نقش اساسی در افزایش دقت و کارایی این سیستم‌ها ایفا می‌کنند. در این پژوهش، مدل **CTran** به‌عنوان یک روش نوین در پردازش دستورات صوتی معرفی شده و بر روی مجموعه داده Fluent Speech Commands ارزیابی شده است.

مدل **CTran** با بهره‌گیری از معماری‌های ترکیبی و قدرتمند یادگیری عمیق، توانایی بالایی در استخراج ویژگی‌های معنایی و الگوهای گفتاری از داده‌های صوتی دارد. این مدل از مکانیزم‌های توجه و ترکیب معماری‌های ترانسفورمر با رویکردهای توالی‌به‌توالی استفاده می‌کند که منجر به بهبود چشمگیر در تشخیص گفتار و تفسیر دقیق دستورات کاربران شده است. در این تحقیق، عملکرد مدل **Ctran** با دیگر مدل‌های پیشرفته مقایسه شده و معیارهای ارزیابی شامل دقت تشخیص، سرعت پردازش و توانایی تعمیم به داده‌های جدید بوده است.

نتایج نشان می‌دهد که مدل **CTran** با استفاده از معماری‌های مدرن و طراحی بهینه‌شده، در بسیاری از شاخص‌ها عملکرد قابل‌توجهی دارد. یافته‌های این پژوهش می‌تواند به توسعه سامانه‌های مؤثرتر در حوزه خانه‌های هوشمند و تعامل انسان و ماشین کمک کند و گامی مؤثر در جهت ارتقای فناوری‌های مبتنی بر پردازش گفتار باشد.

کلمات کلیدی: خانه‌های هوشمند، دستورات صوتی، یادگیری عمیق، مدلCTran ، پردازش گفتار.

1. مقدمه

سیستم‌های هوشمند امروزی به‌طور فزاینده‌ای توانایی تشخیص الگوهای گفتاری کاربران را دارند. این قابلیت به آن‌ها اجازه می‌دهد تا دستورات مرتبط با کنترل لوازم منزل را به‌صورت دقیق و کارآمد اجرا کنند. این سیستم‌ها از الگوریتم‌های پیشرفته‌ای برای شناسایی و پردازش صداهای انسانی استفاده می‌کنند.

و با تحلیل الگوهای گفتاری، می‌توانند دستورات مختلف را شناسایی کرده وپس از شناسایی دستورات، سیستم‌های هوشمند می‌توانند به‌طور خودکار لوازم منزل را کنترل کنند. این کنترل می‌تواند شامل روشن و خاموش کردن لامپ‌ها، تنظیم دما، یا مدیریت دستگاه‌های دیگر باشد. به منظور شناسایی و تشخیص دقیق عملیات مورد اشاره در دستورات صوتی، ضروری است که نیت‌ها و اهداف نهفته در این فراخوانی‌ها به دقت دریافت و تحلیل گردند. در این راستا، فهم عمیق از مقاصد بیان‌شده و معناهای ضمنی آنها می‌تواند به ما در فرایند تفسیر و واکنش مؤثر کمک کند. به عبارتی دیگر، هر دستور صوتی حامل پیامی است که برای دریافت صحیح آن، نیازمند توجه به جنبه‌های گوناگون هدف و منظور گوینده است. این امر این امکان را می‌دهد تا با دقت بیشتری به نیازها و خواسته‌های مطرح شده پاسخ داده و ارتباطی مؤثرتر و معنادارتر برقرار کنید. تشخیص هدف و تخصیص اطلاعات به بخش ها وظایف حیاتی در درک زبان گفتاری و طبیعی برای سیستم‌های گفتگوی هدف‌محور هستند. [1]

مدل‌های درک زبان گفتاری*، هدفشان درک معنای گفتار است. آن‌ها معمولاً نیازی به تبدیل گفتار به متن کامل ندارند و به طور مستقیم از داده‌های صوتی، اطلاعات مورد نیاز (مانند intent و slots) را استخراج می‌کنند. سیستم‌های SLU برای تبدیل گفتار به عمل یا پرسش مورد نظر استفاده می‌شوند، مانند تبدیل یک جمله به دستور برای لامپ. معمولاً این سیستم‌ها شامل دو ماژول تشخیص خودکار گفتار† و درک زبان طبیعی‡ هستند. مدل‌های End-to-End SLU به طور مستقیم از گفتار به هدف می‌روند، بدون اینکه متن میانی تولید کنند. این مدل‌ها با استفاده از یادگیری عمیق برای یادگیری نمایش‌های سلسله‌مراتبی از سیگنال‌های گفتاری استفاده می‌کنند[2].

اخیراً، معماری E2E SLU که از مدل های SLU هستند، توجه زیادی به خود جلب کرده‌اند که در آن مدل‌های صوتی و متنی به‌طور مشترک بهینه‌سازی می‌شوند. برای هدایت یادگیری معناشناسی از سیگنال‌های صوتی، از تلفات چندمنظوره استفاده شده است. محدودیت برخی از این روش‌ها این است که برای برچسب‌گذاری توالی مناسب نیستند.

به‌منظور رفع این محدودیت، معماری های E2E توسعه داده‌شده‌اند که بدون نیاز به رمزگشایی خودکار عمل می‌کنند و کارآمدتر هستند[3]. یکی از معماری‌های مهم در زمینهSLU ، معماری CTran [8]است که به‌طور خاص برای درک معنای گفتار و تشخیص اهداف و اطلاعات مرتبط اسلات طراحی شده است.

CTran به‌جای استفاده از روش‌های سنتی که نیازمند تبدیل گفتار به متن از طریق ASR هستند، از یک رویکرد End-to-End بهره می‌برد. در این معماری، مدل به‌طور مستقیم از داده‌های صوتی، اطلاعات معنایی مورد نیاز را استخراج می‌کند. این معماری از ماژول هایی همانند CNN استفاده می کند که به کاهش پیچیدگی کمک می کند و همچنین از ترانسفورمر رمزگذار§ برای رمزگذاری** ویژگی‌ها بهره می‌برد. این بخش قادر است با استفاده از مکانیسم Self-Attention، بخش‌های مهم داده‌های ورودی را شناسایی کند و اطلاعات معنایی مربوط به هدف†† و شکاف‌های معنایی‡‡ را استخراج نماید.

---

* Spoken language understanding(SLU)
† Automatic Speech Recognition(ASR)
‡ Natural Language Understanding(NLU)
§ Transformer Encoder
** encoding
†† intent
‡‡ slot

این معماری به دلیل طراحی مستقل از متن و استفاده بهینه از اطلاعات صوتی، به عنوان یکی از معماری‌های پیشرفته در SLUشناخته می‌شود. در این مقاله، به پیاده‌سازی معماری CTran بر روی دیتاست FSC پرداخته شده است. هدف اصلی این پژوهش، ارزیابی عملکرد این معماری در مقایسه با یک معماری (E2E) است که قبلاً بر روی همین دیتاست پیاده‌سازی شده است .

در این مقاله، نتایج پیاده‌سازی و مقایسه این دو معماری با تمرکز بر معیارهایی مانند دقت، سرعت پردازش، و توانایی تشخیص هدف و اسلات‌ها مورد بررسی قرار می‌گیرد. در بخشهای بعدی این مقاله، ابتدا روشهای موجود برای تشخیص هدف و تخصیص اطلاعات به بخش ها مورد بررسی قرار میگیرد. سپس، به آماده سازی داده ها و روش های مورد استفاده در طراحی مدل پرداخته خواهد شد. در بخش سوم،روش های مختلف قبل از اعمال معماریCTranبررسی خواهند شد وبهترین روش انتخاب میشود. دربخش چهارم نتایج به دست آمده از اجرای مدل ارائه میشود و در بخش پنجم، این نتایج مورد بحث قرار میگیرند. نهایتادر بخش ششم، به نتیجه گیری پرداخته میشود.

2. مروری بر روش های موجود

مشکل شناسایی هدف در زبان‌های با منابع محدود برای زبان هایی با داده های آموزشی محدود، تمرکز چندین کار تحقیقاتی اخیر بوده است. در این بخش، برخی از مرتبط ترین آنها را مورد بحث قرار می دهیم و کارهای اخیر، از جمله مجموعه داده ها، معیارها، و مدل هایی که هدفشان رفع این چالش است.[1]

روش‌های مبتنی برASR که در این رویکرد، ابتدا گفتار کاربر به متن تبدیل می‌شود و سپس از مدل‌های پردازش زبان طبیعی* برای استخراج هدف و اسلات‌ها استفاده می‌شود. اگرچه این روش‌ها به دلیل تفکیک مراحل، قابل درک و تفسیر هستند، اما وابستگی آن‌ها به دقت مدل ASR، عملکرد کلی سیستم را تحت تأثیر قرار می‌دهد.[4]

از دیگر روش ها در رویکردهای End-to-End، مدل مستقیماً از داده‌های صوتی برای استخراج اطلاعات معنایی استفاده می‌کند و نیازی به مرحله تبدیل گفتار به متن وجود ندارد. این روش‌ها، با حذف واسطه‌ها، توانایی کاهش خطاهای انباشته‌شده و بهبود دقت کلی سیستم را دارند[5]. همچنین، استفاده از معماری‌هایی مانند RNN، CNN، وترانسفورمر در این روش‌ها مرسوم است. ما در این کار، معماری های بدون نیاز بهASRبرای طبقه بندی قصد پیشنهاد میکنیم که به طور مستقیم از ویژگیهای صوتی استفاده میکند و با استفاده از سه اسالت (عمل، شی و مکان) قصد را پیش بینی میکند.[11]

معماری‌های جدید مانند CTran که در این مقاله به آن می پردازیم با بهره‌گیری از ترانسفورمر رمزگذار و رویکردهای مبتنی بر Self-Attention، توانسته‌اند عملکرد بهتری در استخراج اطلاعات معنایی از گفتار داشته باشند. این معماری‌ها مستقیماً بر روی داده‌های صوتی اعمال می‌شوند و با ترکیب لایه‌های استخراج ویژگی و رمزگذاری معنایی، همزمان هدف و اسلات‌ها را پیش‌بینی می‌کنند[6].

برای ارزیابی مدل‌هایSLU ، معیارهایی مانند دقت در پیش‌بینی، سرعت پردازش، و توانایی عملکرد در داده‌های کم‌منبع حائز اهمیت هستند. شاخص دقت† میزان عملکرد مدل را در استخراج هدف و شکاف‌های معنایی نشان می‌دهد.

دقت بالا به معنای توانایی بهتر مدل در درک معنای گفتار است[5],[4]. سرعت اجرای مدل، به‌ویژه در سیستم‌های بلادرنگ، اهمیت زیادی دارد. مدل‌هایی که زمان پردازش کمتری دارند، برای کاربردهای تعاملی مناسب‌تر هستند[6] .

* Natural language processing

† accuracy

توانایی مدل در کار با زبان‌ها یا داده‌های کم‌منبع نشان‌دهنده انعطاف‌پذیری آن است. مدل‌هایی که در شرایط داده محدود همچنان عملکرد خوبی ارائه می‌دهند، برای زبان‌های نادر و سیستم‌های چندزبانه مناسب‌تر هستند [1].
پیچیدگی پیاده‌سازی، نیازمندی‌های محاسباتی، و قابلیت اجرا بر روی سخت‌افزارهای مختلف از معیارهای مهم برای انتخاب مدل مناسب است. معماری‌های ساده‌تر معمولاً هزینه‌های کمتری برای آموزش و استقرار دارند[7]. در این مقاله، به بررسی و مقایسه معماری CTran با معماری E2E در پردازش دیتاست FSC پرداخته می‌شود تا کارایی و نقاط قوت این روش‌ها بهتر ارزیابی شوند.

3- روش شناسی

3-1-آماده سازی داده ها

مجموعه داده‌های ما شامل فایل‌های صوتی 16 کیلوهرتز با برچسب‌های عمل، شیء و مکان است. برای هر هدف، چندین عبارت مختلف جمع‌آوری شده و داده‌ها به صورت تصادفی به تقسیم‌های آموزش، اعتبارسنجی و تست تقسیم می‌شوند. این مجموعه داده‌ها شامل تعداد زیادی عبارت و ضبط‌های متعدد است. مجموعه داده ها در مجموع 31 هدف منحصر به فرد دارد. مجموعه داده ها می تواند به عنوان یک کار طبقه بندی چند برچسب استفاده شود.

برای مجموعه اصلی آزمایشات ، از مجموعه داده دستورات گفتار روان استفاده می کنیم [2]. دستورات گفتار روان مجموعه داده ای از 30.430 صوتی انگلیسی با 77 بلندگو است که هر کدام با اسلات های "عمل" ، "موضوع" و "مکان" برچسب گذاری شده اند. 248 جمله متمایز وجود دارد که هر کدام توسط چندین سخنران در هر دو مجموعه آموزش و مجموعه اعتباربخشی/تست صحبت می شود.طبق جدول 1 میزان داده های مربوط به بخش های آموزش و تست و اعتبارسنجی نشان داده شده است.

Split	# of speakers	# of utterances	# hours
Train	77	23,132	14.7
Valid	10	3,118	1.9
Test	10	3,793	2.4
Total	97	30,043	19.0

جدول 1. دیتاست fluent speech commands

ما همچنین از مجموعه داده Snips SLU [8] استفاده می کنیم ، این مجموعه داده کوچکتر و چالش برانگیزتر از دستورات گفتاری روان است: شامل اعداد است و فقط 1660 صوتی دارد که هر کدام با یک جمله متفاوت مطابقت دارد ، بنابراین مدل به طور کامل بر روی جملاتی که قبلا نشنیده است آزمایش می شود و باید برای دستیابی به دقت بالا به آنها تعمیم دهد. به عنوان مثال ، جمله "آیا می توانید چراغ ها را روشن کنید ؟ "دارای برچسب {عمل : روشن - شی: چراغ – مکان: ندارد} [9].

3-2-روش پیشنهادی

مدل CTRAN:

مدل* CTRAN یک مدل نوآورانه برای درک زبان طبیعی است که ترکیبی از شبکه‌های کانولوشنی (CNN) و ترنسفورمرها را برای تحلیل داده‌های متنی به کار می‌برد. این مدل به طور خاص برای بهبود عملکرد در کارهایی مانند شناسایی هدف و تخصیص اطلاعات به بخش ها در وظایف پردازش زبان طبیعی طراحی شده است. در این مدل، ابتدا از شبکه‌های کانولوشنی برای استخراج ویژگی‌های سطح پایین از داده‌های متنی استفاده می‌شود. شبکه‌های CNN قادرند تا اطلاعات محلی در متون را به خوبی استخراج کرده و ویژگی‌های مفیدی از ساختار کلمات و جملات ارائه دهند. پس از استخراج ویژگی‌ها توسط CNN، مدل CTRAN از بخش ترنسفورمر برای مدل‌سازی وابستگی‌های بلندمدت بین کلمات و توالی‌های داده استفاده می‌کند. ترنسفورمر با استفاده از مکانیسم توجه†، به مدل این امکان را می‌دهد که به بخش‌های مختلف ورودی توجه کرده و وابستگی‌های پیچیده‌تری را در داده‌ها شبیه‌سازی کند.

ترکیب CNN و ترنسفورمر باعث می‌شود که مدل بتواند هم از ویژگی‌های محلی (که توسط CNN استخراج می‌شود) و هم از وابستگی‌های بلندمدت (که توسط ترنسفورمر یاد گرفته می‌شود) استفاده کند.[8]

در ابتدای کار مجموعه‌ای از توابع پیش‌پردازش برای آماده‌سازی داده‌های متنی جهت استفاده در مدل‌های پردازش زبان طبیعی مبتنی بر BERT در نظر میگیریم. این توابع شامل مواردی مانند تبدیل توکن‌ها و کلاس‌های قصد ، حذف علائم نگارشی، تمیزسازی متن، و ایجاد ماسک برای تشخیص توکن‌های اصلی و فرعی است. همچنین، اعداد موجود در متن به تگ خاص تبدیل می‌شوند و داده‌ها به شکل تنسور آماده می‌گردند.

این مراحل به بهبود کیفیت داده‌های ورودی و سازگاری آن‌ها با مدل‌های یادگیری عمیق کمک می‌کنند و برای آماده‌سازی داده‌ها جهت آموزش یا ارزیابی مدل‌های پردازش زبان طبیعی طراحی شده است و از کتابخانه‌های پیشرفته‌ای مانند Hugging Face ترانسفورمراستفاده می‌کند. در ادامه با استفاده از کتابخانه Hugging Face، واحدساز‡ bert-base-uncased برای توکن‌سازی داده‌ها بارگذاری می‌شود. ستون‌های مربوط به مقاصد (مانند عمل، شی، و مکان) به آیدی تبدیل می‌شوند تا مدل بتواند آن‌ها را پردازش کند.

این فرآیند برای هر دو دیتاست آموزش و تست اجرا می‌شود تا داده‌ها برای مدل آماده شوند. دیکشنری‌هایی برای نگاشت بین توکن‌ها، برچسب‌ها و نیات به ایندکس‌های عددی و بالعکس ایجاد می‌کنیم و این دیکشنری‌ها برای تبدیل داده‌های متنی به قالب عددی و بالعکس در طول آموزش و پیش‌بینی مدل استفاده می‌شوند.

چارچوب مدل:

یک کلاس به نام Encoder تعریف می‌کنیم که به‌عنوان بخشی از یک مدل یادگیری عمیق عمل می‌کند. این Encoder از لایه‌های کانولوشن 1-بعدی (Convolution1D) برای پردازش ویژگی‌های تعبیه‌شده§ استفاده می‌کند و خروجی‌هایی را برای مراحل بعدی مدل تولید می‌کند و شامل اندازه‌های مختلف کرنل‌ها (2، 3، و 5) است که تعداد آن‌ها برابر 3 است. این رمزگذار چهار لایه کانولوشن یک‌بعدی با اندازه‌های کرنل مختلف (1، 2، 3، 5) دارد و هر لایه کانولوشن از پدینگ** استفاده می‌کند که طول ورودی و خروجی را یکسان نگه می‌دارد. از ReLU به‌عنوان تابع فعال‌سازی بهره

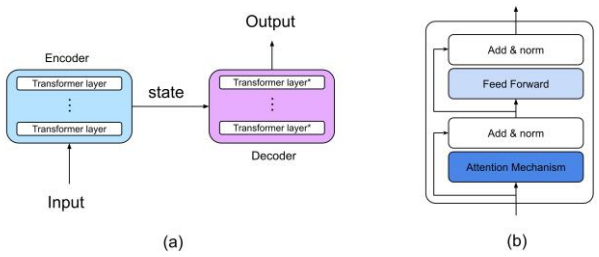
* CNN-Transformer-based Network
† Attention Mechanism
‡ Tokenizer
§ embeddings
** padding

می‌برد. از ویژگی های کلیدی آن این است که چهار لایه کانولوشن به‌طور همزمان ویژگی‌های متنی را با اندازه‌های مختلف کرنل پردازش می‌کنند و اطلاعات زمینه‌ای* محلی را استخراج می‌کنند.

کلاس BertLayer یک ماژول PyTorch است که برای استفاده از مدل پیش‌آموزش‌یافته BERT طراحی شده است. این کلاس از کتابخانه Transformers برای بارگذاری و استفاده از مدل BERT بهره می‌برد. کلاس Middle یک ماژول میانجی است که وظیفه پردازش داده‌های ورودی با استفاده از یک ترنسفورمر انکودر† را بر عهده دارد. این کلاس شامل یک موقعیت‌یاب‡ و چند لایه انکودر ترنسفورمر است و برای پردازش توالی‌ها به کار می‌رود.

این ماژول برای مدل‌هایی که با داده‌های ترتیبی مانند متن یا صوت کار می‌کنند مناسب است. به‌طور خاص، در مدل‌های ترجمه ماشینی، تحلیل توالی‌های متنی و پردازش زبان طبیعی به کار می‌رود. کلاس Decoder یک دیکودر مبتنی بر ترنسفورمر است که برای تولید پیش‌بینی‌های توکن‌های ورودی (مثل برچسب‌های اسلات یا نیات) در یک مدل پردازش زبان طبیعی طراحی شده است. این کلاس از چندین لایه مختلف و تکنیک‌های خاص مانند ماسک‌ها، self-attention و ترنسفورمرها برای پردازش و پیش‌بینی استفاده می‌کند. از ReLU به عنوان تابع فعال‌سازی و از Dropout برای جلوگیری از بیش‌برازش استفاده می‌شود.

Self-Attention برای پردازش و توجه به تمامی توکن‌ها در ورودی انجام می‌شود. این دیکودر از یک ترنسفورمر با 2 لایه و self-attention برای پردازش توکن‌ها و پیش‌بینی برچسب‌های اسلات و نیات استفاده می‌کند. تکنیک‌های دیگری مانند Dropout ولایه LayerNorm، برای بهبود عملکرد مدل و جلوگیری از بیش‌برازش در طول آموزش به‌کار رفته‌اند.



شکل 1. تصویر معماری ترانسفورمر

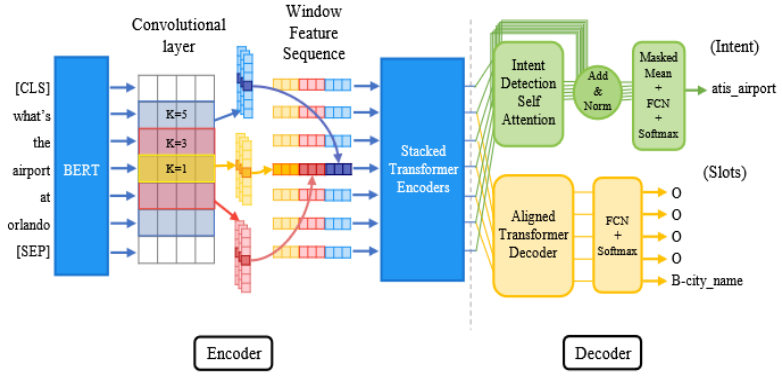
شکل1: شامل دو بخش است:

1 . بخش(a) : این قسمت یک مدل ترنسفورمر را نشان می‌دهد که شامل یک رمزگذار§ و یک رمزگشا** است. ورودی به مدل از طریق رمزگذار پردازش می‌شود، که به صورت لایه‌ای از ترنسفورمرها نمایش داده شده است. سپس وضعیت (state) به رمزگشا انتقال داده می‌شود تا خروجی مدل تولید گردد.

2. بخش(b) : این بخش جزئیات بیشتری از معماری ترنسفورمر را نشان می‌دهد، به‌ویژه مراحلی که در هر لایه ترنسفورمر انجام می‌شود. شامل دو جزء اصلی است: الف) مکانیزم توجه†† : که به مدل کمک می‌کند تا بر بخش‌های مختلف ورودی

* contextual
† Transformer Encoder
‡ Transformer Encoder
§ Encoder
** Decoder
†† Attention Mechanism

تمرکز کند. ب) پردازش پیشرو*: که پردازش اضافی را در لایه انجام می‌دهد. این ساختار معمولاً در مدل‌های ترانسفورمر برای پردازش دنباله‌ای از داده‌ها مانند متن و گفتار استفاده می‌شود.



شکل 2. معماری CT-ran [8]

شکل 2: نمای کلی دقیقی از معماری رمزگذار-رمزگشا پیشنهادی ما را نشان می دهد. همانطور که در شکل نشان داده شده است، توکن‌ها به BERT وارد می‌شوند که یک جاسازی متنی† تولید می‌کند که ما آن را در شبکه خود پردازش می‌کنیم. سپس، عملیات کانولوشن با اندازه‌های مختلف هسته‌ها‡ بر روی کلمات جاسازی شده انجام می‌شود. به طور معمول از عملیات‌هایی مانند ماکس پولینگ§ پس از کانولوشن‌ها استفاده می شود[8].

رمزگذارهای ترنسفورمر**: این رمزگذارها از ویژگی‌های پنجره‌ای استفاده کرده و به تولید نمایه‌های پیچیده‌تر از ورودی کمک می‌کنند. در بخش دیکودر، مدل هدف جمله را شناسایی کرده و خروجی آن در قالب هدف‌های مختلف مانند atis_airport (در داده های ATIS) ارائه می‌شود. رمزگشای ترنسفورمر هماهنگ†† این رمزگشا با استفاده از ویژگی‌های تولید شده توسط رمزگذار، به استخراج هدف و تخصیص اطلاعات همانند عمل و مکان و شی (در داده های FSC) می‌پردازد. مکانیزم‌های افزودن و نرمال‌سازی‡‡ در اینجا برای بهبود عملکرد مدل، از نرمال‌سازی و افزودن ویژگی‌های مختلف استفاده می‌شود. در این معماری، از یادگیری مشترک§§ برای انجام همزمان وظایف شناسایی هدف و تخصیص اطلاعات به بخش ها بهره‌برداری می‌شود.

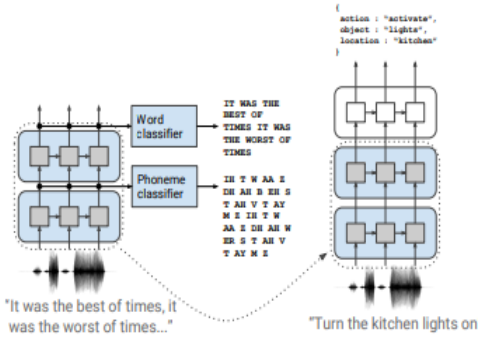
3-3-روش End-to-End

شامل ماژول‌های پیش‌آموزش برای واج‌ها و کلمات است که سپس به صورت انتها به انتها برای SLU آموزش داده می‌شود. ما از پیش‌آموزش با اهداف کلمات به دلیل اینکه این همان چیزی است که ماژول درک زبان طبیعی*** معمولاً انتظار دارد،

* Feed Forward
† contextualized embedding
‡ kernel sizes
§ max-pooling
** Stacked Transformer Encoders
†† Aligned Transformer Decoder
‡‡ Add & Norm
§§ joint learning
*** Natural Language Undrestanding

استفاده کرده‌ایم. مدل‌ها به تدریج لایه‌ها را باز می‌کنند تا عملکرد بهتری داشته باشند و نیاز به ذخیره‌سازی و محاسبات کمتری دارند.[2]

3 ماژول خواهیم داشت که یکی ماژول phoneme، دیگری ماژول هدف [10]و ماژول Unfreezing است.



شکل 3. معماری مدل E2E [2]

شکل 3: لایه های پایینی مدل با استفاده از اهداف ASR (کلمات و واج ها) از قبل آموزش داده شده اند. طبقه بندی کننده های کلمه و فونم کنار گذاشته می شوند و ویژگی های بخش از پیش آموزش دیده مدل (آبی) به عنوان ورودی به ماژول بعدی (سفید) استفاده می شود که با استفاده از اهداف SLU آموزش داده می شود. مدل یک شبکه عصبی عمیق است که از یک مجموعه ماژول‌ها تشکیل شده است، جایی که ماژول‌های اول برای پیش‌بینی آواها و کلمات پیش‌آموزش داده شده‌اند. طبقه‌بندهای کلمات و آواها حذف می‌شوند و سپس کل مدل به‌صورت انتها به انتها برای وظیفه نظارت شده SLU آموزش داده می‌شود[2].

SincLayer فیلتری را بر اساس تابع sinc برای انجام فیلتر فرکانس اجرا می کند که در درجه اول برای پیش پردازش داده های گفتاری استفاده می شود.

Downsample داده‌های ورودی را در امتداد یک محور مشخص با استفاده از میانگین‌گیری، حداکثر ادغام، یا بدون نمونه‌برداری پایین‌آوری می‌کند.

PretrainedModel مدلی متشکل از لایه های کانولوشن (شاملSincNet) و به دنبال آن لایه های تکراری (RNN ها، به طور خاصGRU) برای وظایف تشخیص واج و کلمه است. finalPool یک لایه ترکیبی که حداکثر مقدار را در امتداد یک محور خاص انتخاب می کند.

RNNSelect خروجی یک لایه RNN خاص را انتخاب می کند و کلاس بعدی مدل اولیه که شامل یک مدل واج و تشخیص کلمه از پیش آموزش دیده است و یک لایه طبقه بندی قصد اضافه می کند. از RNN ها برای تشخیص هدف استفاده می کند و دارای قابلیت هایی برای انجماد/بازکردن لایه ها برای انتقال یادگیری است. توابع انجماد/بازکردن انجماد* که این توابع، انجماد/بازکردن انجماد لایه ها را در مدل از پیش آموزش دیده در حین تنظیم دقیق مدیریت می کنند. این مدل برای درک گفتار سرتاسر(SLU) ، ترکیبی از وظایف تشخیص گفتار و طبقه‌بندی هدف طراحی شده است.

* Unfreeze

3-4-مقایسه روش های انجام شده

در مقایسه مدل CTRAN و مدل End-to-End از لحاظ ساختاری، تفاوت‌های قابل توجهی در نحوه پردازش داده‌ها، معماری و استفاده از ماژول‌ها مشاهده می‌شود:

معماری مدلCTRAN :

این مدل ترکیبی از شبکه‌های کانولوشنی (CNN) و ترنسفورمرها است. در ابتدا، CNNها برای استخراج ویژگی‌های سطح پایین از داده‌های متنی استفاده می‌شوند و سپس ترنسفورمرها برای مدل‌سازی وابستگی‌های بلندمدت و پردازش اطلاعات پیچیده‌تر از داده‌ها به کار می‌روند. این ترکیب باعث می‌شود که مدل بتواند از ویژگی‌های محلی و وابستگی‌های بلندمدت به طور همزمان استفاده کند. مدل برای شناسایی نیت‌ها و پر کردن اسلات‌ها در وظایف پردازش زبان طبیعی طراحی شده است. این مدل قادر است ویژگی‌های محلی و وابستگی‌های بلندمدت را به طور همزمان پردازش کند. در این پژوهش دقت مدل برابر با 98.5 درصد بر روی داده آزمایشی به دست آمد اما از لحاظ سرعت پردازش زمان بیشتری به طول انجامید.

End-to-End: این مدل از یک روش پیش‌آموزش انتها به انتها برای پردازش داده‌ها استفاده می‌کند. در این معماری، هدف بهینه‌سازی کل مدل به صورت همزمان برای تمام مراحل، از تشخیص واج‌ها تا شناسایی نیت‌ها است. مدل به تدریج لایه‌ها را باز می‌کند تا عملکرد بهتری داشته باشد و نیازی به ذخیره‌سازی و محاسبات کمتری دارد. همچنین قابلیت‌هایی برای انجماد و بازکردن لایه‌ها در حین تنظیم دقیق مدل دارد، که به انتقال یادگیری و بهبود عملکرد کمک می‌کند. این مدل برای درک گفتار سرتاسر (SLU) طراحی شده است که شامل وظایف تشخیص گفتار و طبقه‌بندی نیت‌ها است. هدف این مدل پردازش گفتار به‌طور انتها به انتها و بهبود عملکرد آن از طریق پیش‌آموزش و انجماد/بازکردن لایه‌ها است.در این پژوهش دقت مدل 97 درصد به دست آمده است و با توجه به محاسبات کمتری که دارد سرعت پردازش بالاتری نسبت به مدل CTran دارد.

در مجموع، مدل CTRAN بر ترکیب شبکه‌های CNN و ترنسفورمر برای تحلیل ویژگی‌های محلی و وابستگی‌های بلندمدت تاکید دارد، در حالی که مدل End-to-End بر پردازش داده‌های گفتاری از طریق پیش‌آموزش و استفاده از RNNها و تکنیک‌های انجماد/بازکردن لایه‌ها متمرکز است. پس بنابراین مدل End-to-End با توجه به محاسبات کمتر و سرعت بالاتر اجرا عملکرد بهتری نسبت به مدل CTran خواهد داشت اما از لحاظ دقت مدل Ctranعملکرد بهتری دارد.

ردیف	مدل ها	دقت داده
1	CTran	98.5
2	End-to-End	97

جدول 2: دقت مدل در داده های آزمایشی

4-نتایج و نمودارها

در این پژوهش مدل پس از 20 دوره آموزش به دقت 98 درصد بر روی داده های آموزشی و 98.5 بر روی داده آزمایشی رسید. همچنین این مدل بر روی دیتاست Atis , snips نیز پیاده سازی شده است [8] که نتایج آن به شرح زیر است.

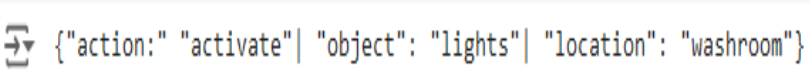
Dataset / Model	ATIS	SNIPS
Aligned LSTM with attention	98.30	98.10

در مقایسه عملکرد مدل Ctran در تشخیص بخش ها بر روی این سه نوع دیتاست F1-score به شرح زیر خواهد بود:

ردیف	دیتاست	F1-score
1	Fluent speech commands	0.97
2	Snips	0.98.17
3	ATIS	0.98

جدول 3: دقت مدل در داده های آزمایشی

نتیجه تشخیص اهداف با توجه به هر دو مدل ذکر شده به شرح زیر خواهد بود:



شکل4. نمونه ای خروجی مدل به منظور تشخیص نیت و اهداف

در شکل 4 خروجی دستور صوتی وارد شده به مدل به صورت بخش هایی از اهداف مشخص می شود . برای دیتاست FSC بخش ها به صورت عمل و شی و مکان هستند .

5-بحث

در این پژوهش، به پیاده‌سازی مدل CTRAN بر روی دیتاست (FSC) پرداخته شده است. مدلCTRAN ، که ترکیبی از شبکه‌های کانولوشنی (CNN) و ترنسفورمرها است، با هدف بهبود عملکرد در شناسایی نیت‌ها و پر کردن اسلات‌ها طراحی شده است. این مدل به طور خاص برای تحلیل ویژگی‌های محلی و وابستگی‌های بلندمدت در داده‌های متنی به کار می‌رود. با استفاده ازترنسفورمرها، وابستگی‌های پیچیده و بلندمدت بین کلمات و توالی‌ها مدل‌سازی می‌شود که این ترکیب، موجب دقت بالاتر در شناسایی نیت‌ها و پر کردن اسلات‌ها می‌شود. نتایج به دست آمده از آزمایش‌های انجام شده بر روی دیتاست FSC نشان می‌دهند که مدل CTRAN توانسته است دقت بالایی در پیش‌بینی نیت‌ها و پر کردن اسلات‌ها با دقت 98.5 درصد بدست آورد.

6- نتیجه گیری

مدل CTRAN با ترکیب معماری‌های CNN و ترنسفورمر توانسته است دقت بالاتری در تشخیص هدف و تخصیص اطلاعات به بخش ها نسبت به مدل End-to-End (E2E) ارائه دهد. این به دلیل توانایی آن در استخراج ویژگی‌های محلی و مدل‌سازی وابستگی‌های بلندمدت است. با این حال، پیچیدگی محاسباتی بیشتر مدل CTRAN منجر به زمان پردازش طولانی‌تر می‌شود، در حالی که مدل E2E با سرعت بیشتر، دقتی نزدیک به CTRAN دارد. در نهایت، مدل CTRAN به دلیل دقت بالا و قابلیت تحلیل پیچیده، گزینه‌ای مناسب برای کاربردهایی است که حساسیت زمانی در آن‌ها اهمیت کمتری دارد.

مراجع

[1] Kwon, S. Y., et al. (2023). "Zero-Shot Slot and Intent Detection in Low-Resource Languages." *arXiv preprint arXiv:2304.13292*. Retrieved from https://arxiv.org/abs/2304.13292

[2] Lugosch, L., Ravanelli, M., Ignoto, P., Tomar, V. S., & Bengio, Y. (2019). Speech Model Pre-training for End-to-End Spoken Language Understanding. *Interspeech*, September 2019. Available at arXiv:1904.03670

[3] Radfar, M., et al. (2023). End-to-End Spoken Language Understanding Using Joint CTC Loss and Self-Supervised, Pretrained Acoustic Encoders. *ICASSP 2023: IEEE International Conference on Acoustics, Speech and Signal Processing*, 4–10 June 2023, Rhodes Island, Greece. Available at arXiv:2305.02937

[4] Graves, A., Fernández, S., Gómez, F., & Schmidhuber, J. (2006). "Connectionist temporal classification: Labeling unsegmented sequence data with recurrent neural networks." *Proceedings of the International Conference on Machine Learning (ICML 2006)*, 369-376

[5] Qian, K., Morais, E., Kuo, H. J., Thomas, S., Tuske, Z., & Kingsbury, B. (2020). *End-to-End Spoken Language Understanding Using Transformer Networks and Self-Supervised Pretrained Features*. arXiv. https://doi.org/10.48550/arxiv.2011.08238:contentReference[oaicite:0]{index=0}:contentReference[oaicite:1]

[6] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). *Attention is All You Need*. In *Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS 2017)*, 6000–6010. https://doi.org/10.5555/3295222.3295349.

[7] Hinton, G., Deng, L., Yu, D., Dahl, G. E., Mohamed, A.-r., Jaitly, N., Senior, A., Vanhoucke, V., Sainath, T. N., & Kingsbury, B. (2012). *Deep neural networks for acoustic modeling in speech recognition*. In *Proceedings of the IEEE* 100(5), 1-30. https://doi.org/10.1109/JPROC.2012.2183986.

[8] Zhang, H., Wang, S., Zhang, Q., & Liu, Y. (2021). CTRAN: CNN-Transformer-based Network for Natural Language Understanding. *arXiv preprint arXiv:2104.06892*.

[9] Lugosch, L., Meyer, B., Nowrouzezahrai, D., & Ravanelli, M. (2020). Using Speech Synthesis to Train End-to-End Spoken Language Understanding Models. *ICASSP 2020*Misc, A., 2003. Miscellaneous Title. On the WWW, May. URL http://www.abc.edu.

[10] D. Serdyuk, Y. Wang, C. Fuegen, A. Kumar, B. Liu, and Y. Bengio, “Towards end-to-end spoken language understanding,” ICASSP, 2018.

[11] [21]Elisavet Palogiannidi, Ioannis Gkinis, George Mastrapas, Petr Mizera, Themos Stafylakis”:END-TO-END ARCHITECTURES FOR ASR-FREE SPOKEN LANGUAGE UNDERSTANDING,” arXiv:1910.10599v3 [eess.AS] 1 May 2020

یک رویکرد جدید در حل مسایل بهینه‌سازی غیرخطی فازی با استفاده از ضرایب لاگرانژ

نرجس امیری [*۱]، سید هادی ناصری[۲]،داوود درویشی[۳]

۱-گروه ریاضی کاربردی، دانشگاه مازندران؛ narges.amirii.97@gmail.com

۲- گروه ریاضی کاربردی، دانشگاه مازندران؛ nhadi57@gmail.com

۳- گروه ریاضی کاربردی، دانشگاه ساری؛ *d_darvishi@pnu.ac.ir*

چکیده

مساله بهینه سازی یک تابع هدف که در محدودیت های آن معادلات و نامعادلات وجود دارد توسط برنامه ریزی غیرخطی مورد بررسی قرار می گیرد. در این مقاله، یک مدل فازی جدید برای رسیدگی به ابهام ارائه شده در مسائل برنامه ریزی غیرخطی پیشنهاد شده است. مدل پیشنهادی شرح داده شده است. فرمول ریاضی و روش محاسباتی دقیق آن با استفاده از توابع عضویت فازی ذوزنقه ای نشان داده شده است. در اینجا روش محاسباتی با استفاده از شرایط لازم و کافی روش ضرایب لاگرانژی از نظر فازی، نقش مهمی در کسب نتیجه بهینه دارد. در نهایت، ارزیابی عملکرد بیان می کند که سطح کارایی مدل پیشنهادی تأثیر بالایی دارد.

کلمات کلیدی: مساله برنامه ریزی غیرخطی فازی، بهینه سازی غیرخطی، روش ضریب لاگرانژی از نظر فازی، توابع عضویت ذوزنقه ای، شاخص رتبه بندی.

۱. مقدمه

برنامه ریزی غیرخطی فازی به دلیل ماهیت نامطمئن و نادقیق بودن آن مشکل ساز یا به دلیل ترتیب دقیق آن در مواجهه با مسائل با ارزش است. در این مورد، یک تابع هدف باید در حین کار در محدودیت های خاص بهبود یابد. تئوری تصمیم گیری فازی و فازی و تصمیم درست مورد استفاده در مسائل تصمیم گیری را برای دستیابی به نتیجه بهینه معرفی کرد[1]. در موقعیت های خاص زندگی واقعی، تصمیمات مبهم هستند و تلاش های اولیه برای انتخاب ها برای فرموله کردن یک مدل یا موارد مناسب برای تجزیه و تحلیل مورد نیاز است. به طور مشابه، فازی را در مدل های خود از چنین موقعیت هایی قرار می دهیم تا رویکردهایی را برای مقابله با داده های فازی پیشنهاد کنیم[2]. یک جواب بهینه در برنامه ریزی خطی هم محدودیتها و هم تابع هدف را برآورده می کند. به طور مشابه، این مسئله یک تابع هدف دارد با متغیرهای تصمیم فازی در قیود، از جمله ضرایب به شکل فازی ارائه شده است[3,4] . یک مدل مناسب توسعه داده شده است، و انتخاب

[*] **Corresponding author: Narjes Amiri**
Email: narges.amirii.97@gmail.com

مناسب ترین الگوریتم های بهینه سازی برای دستیابی به جواب های مقرون به صرفه برای مساله حمل و نقل گسسته غیرخطی در برنامه ریزی اعداد صحیح مختلط برای هر دو خطی و غیرخطی ضروری است[5]. مطالعه ای برای یک مسئله تخصیص چندهدفه با انتقالی که از توزیع وایبول با استفاده از رویکرد تصادفی با عدم قطعیت پیروی می کند، پیشنهاد شده است. علاوه بر این، این مطالعه با نشان دادن الگوریتم های بهینه سازی مختلف با تحلیل حساسیت، کارایی نتایج محاسباتی را بهبود می بخشد[6]. مساله زمان بندی به عنوان یک مساله بهینه سازی تصادفی،به ویژه در برنامه ریزی غیرخطی تعبیر شده است، و سپس در یک مساله بهینه سازی چندهدفه مدل سازی شده است که زمان بندی مناسبی را با مدل های مختلف ارائه می دهد[7]. مشکلات عملیات ترجیحی دوسطحی و همچنین روشی برای تخمین پارامترهای قابلیت اطمینان با استفاده از بهینه سازی غیرخطی با رویکرد کان-تاکر پیشنهاد شده اند[8]. رویکردی برای بهینه سازی چندهدفه، عمدتاً زنجیره های تامین غیرخطی تحت عدم قطعیت، برای به دست آوردن کمترین هزینه حمل و نقل و در عین حال کنترل سایر عوامل زوال توصیه شده است. همچنین برای بهبود برخی از الگوریتم های بهینه سازی و مدیریت داده استفاده می شود[9]. نتایج با یک رویکرد پیشنهادی برای طراحی مقاطع کانال با کمترین هزینه در روش نیوتن مقایسه می شوند، که در شرایط کاروش-کان-تاکر برای مسائل بهینه سازی غیرخطیمحدود به نامحدود با الگوریتم های استاندارد اعمال می شود[10]. روش لاگرانژی مبتنی بر فازی را می توان به عنوان مکانیزم اطلاعات دیجیتال برای پشتیبانی از ماشین های بردار برای تفسیر داده های زیست پزشکی به آسانی توصیف کرد[11] . مطالعه روش ها و تکنیک های مختلفی را برای مقابله با مسائل خطی مانند برنامه ریزی درجه دوم، حمل و نقل جامد و همچنین بسیاری از کاربردهای صنعتی در شرایط عدم قطعیت توصیه کرده اند. این بهترین رویکرد برای پرداختن به این نوع مسایل برنامه ریزی غیرخطی به شیوه ای مقرون به صرفه آغاز می کند[12].

اگر تابع هدف یا محدودیت ها غیرخطی باشند، آن را به عنوان یک مساله برنامه ریزی غیرخطی در نظر می گیریم. در این مدل، برای مقابله با چنین مساله بهینه سازی غیرخطی، با شرایط لازم و کافی روش ضرب کننده های لاگرانژی با فازی شروع می کنیم تا جواب بهینه را به دست آوریم. با این حال، این با استفاده از توابع عضویت فازی ذوزنقه ای و محاسبات ریاضی آنها انجام می شود .یک مدل فازی به شکل مساله برنامه ریزی غیرخطی عمومی ارائه شده است، که به مدیریت ابهام کمک می کند و همچنین جواب بهینه به دست آمده را در توصیف توابع عضویت توجیه می کند[13,14]. علاوه بر این، روش محاسباتی پیشنهادی به دو روش مجزا انجام شد: مساله اول با توابع عضویت فازی در نظر گرفته شده است، و مساله دوم با یک شاخص رتبه بندی قوی ارائه شده است. بر این اساس، تابع عضویت به عنوان یک عدد فازی ذوزنقه ای در نظر گرفته شده است که خطی است و ترجیحاً هر نوع اعداد فازی بسته به مناسب بودن مدل را به طور موثر اداره می کند.

۲. سیستم های فازی

دراین بخش، برخی از مفاهیم اولیه و پیشینه های اساسی در ریاضیات فازی [4,13] و همچنین چند تعاریف که بیشتر مورد نیاز هستند پرداخته می شود:

تعریف ۱[14]. در نظر بگیرید $T=[t_1,t_2,t_3,t_4]$ یک عدد فازی ذوزنقه ای با تابع عضویت زیر باشد:

$$\mu_T(x)=\begin{cases}\dfrac{x-t_1}{t_2-t_1}, & t_1\le x\le t_2\\ 1, & t_2\le x\le t_3\\ \dfrac{x-t_4}{t_3-t_4}, & t_3\le x\le t_4\end{cases}$$

تعریف ۲[13].(α برش) یک مجموعه فازی T را در X و هر عدد حقیقی α را در $[0,1]$ در نظر بگیرید، سپس α-برش T را با علامت گذاری T^{α} نشان می دهیم، مجموعه آن $T^{\alpha}=\{x\in X:\mu_T(x)\geq\alpha\}$ را در نظر میگیریم. برای مثال، فرض کنید T یک مجموعه فازی باشد که تابع عضویت آن به صورت بالا آورده شده است. α-برش از T پیدا کنید که در آن $\alpha\in[0,1]$ ، فرض کنید توابع مرجع T را به سمت چپ و راست تنظیم کنیم.

$$\alpha=\frac{x^{(1)}-t_1}{t_2-t_1} \quad = \quad \alpha \quad \frac{x^{(2)}-t_4}{t_3-t_4}$$

و

x به α بیان می کند، که در آن $x^{(1)}=(t_2-t_1)\alpha+t_1$ و $x^{(2)}=t_4+(t_3-t_4)\alpha$ که α-برش از T را خواهیم داشت:

$$T^{\alpha}=\left[x^{(1)},x^{(2)}\right]=\left[(t_2-t_1)\alpha+t_1,t_4+(t_3-t_4)\alpha\right]$$

تعریف۳[13] .(شاخص رتبه بندی قوی).شاخص رتبه بندی قوی، ویژگی های جبران، سازگاری و افزودنی را برآورده می کند و نتایجی را ایجاد می کند که توسط ادراک انسان کنترل می شوند. اگر T یک عدد فازی باشد، شاخص رتبه بندی قوی به صورت زیر اندازه گیری می شود:

$$R(T)=\int_0^1(0.5)*\left[T_\alpha^L,T_\alpha^u\right]d\alpha$$

که در آن $\left[T_\alpha^L,T_\alpha^u\right]=\left[x^{(1)},x^{(2)}\right]=\left[(t_2-t_1)\alpha+t_1,t_4+(t_3-t_4)\alpha\right]$ که یک α-برش از T است. در اینجا شاخص رتبه بندی قوی $R(T)$ اهمیت عددی T را نشان می دهد.

۳. مدل بهینه سازی برای برنامه ریزی غیرخطی فازی

تاکید پژوهش بر مسائل بهینه سازی فازی در حوزه برنامه ریزی غیرخطی عمدتا محدود است. با این حال، توجه کمی به برنامه ریزی غیرخطی، مانند برنامه ریزی درجه دوم، برنامه ریزی قابل تفکیک و روش های جستجو و بسیاری موارد دیگر متمرکز شده است. با این حال، جدای از آن، چندین شکل از برمه ریزی غیرخطی فازی وجود دارد که به طور گسترده در مسایل مختلف مهم، عمدتاً در سیستم های صنعتی پیچیده، مورد توجه قرار می گیرد. تاکید تحقیقات بر روی مسایل بهینه سازی فازی در زمینه برنامه ریزی غیرخطی به طور کلی محدود است. علاوه بر این، علاقه کمی به برنامه ریزی غیرخطی برای پرداختن به مبهم بودن مسایل وجود دارد. علاوه بر این، در بسیاری از مسایل واقعی، بسیاری از انواع برنامه ریزی های غیرخطی فازی، عمدتا در سیستم های تولیدی پیچیده، رخ می دهند. این را نمی توان با مدل های سنتی نشان داد.

درهمین حال، مطالعات علمی در مورد تکنیک های مدل سازی و رویکردهای تقویتی برای برنامه ریزی غیرخطی در موقعیت های فازی نه تنها از چارچوب بهینه سازی فازی، بلکه در کاربرد چالش ها نیز حائز اهمیت است. در نتیجه، مدل بهینه سازی غیرخطی فازی در دو مرحله پیشنهاد شده است: فرمولاسیون مدل و روش محاسباتی.

۳. ۱. فرمول بندی برنامه ریزی غیرخطی فازی

مسایل برنامه ریزی غیرخطی به خوبی تعریف شده است به عنوان مساله یافتن یک بردار فازی $\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]$ که در آن $\left(x_j^{(k)}\right), j=1,2,3,...,n$ و برای هر k=1,2,3,4، یک توابع عضویت فازی ذوزنقه ای، که تابع هدف Z را بهینه می کند،که یک تابع باارزش واقعی است توسط متغیرهای n تعریف می شود[14].

$$\left[Z^{(k)}\right]=f\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right) \quad (1)$$

تحت محدودیت ها، $g^i\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)\ \{\geq,\leq,=\}\left(b_i^{(k)}\right)$,k=1,2,3,4;i=1,2,3,....m

که در آن g^i ها m تا تابع مقدار واقعی و n تا متغیر فازی همچنین b_iها m تا ثابت هستند و $\left(x_j^{(k)}\right)\geq 0, m<n$.

علاوه بر این، همانطور که قبلا ذکر شد، می توان آن را مجدداً بیان کرد:

$$Maximize\ \left[Z^{(k)}\right]=f\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)$$

تحت محدودیت های

$$g^i\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)=\left(b_i^{(k)}\right),\text{k=1,2,3,4;i=1,2,3,....m} \quad (2)$$

$$\left(x_j^{(k)}\right)\geq 0,\ \text{i=1,2,...,m, j=1,2,...,n, } m<n,\ \text{k=1,2,3,4} \quad (3)$$

بردار فازی که شرایط (۲) و (۳) را برآورده می کند یک جواب امکان پذیر برای برنامه ریزی غیرخطی فازی است.

۲.۳ . رویه محاسباتی

این بخش روش محاسباتی مدل را شرح می دهد که از شرایط لازم و کافی لاگرانژی برای یافتن جواب بهینه برای یک مساله برنامه ریزی غیرخطی فازی شده استفاده می کند.

در نظر بگیرید h^iها توابع مقدار واقعی که از n متغیر فازی تشکیل شده است:

$$h^i\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)=g^i\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)-\left(b_i^{(k)}\right),\text{k=1,2,3,4;i=1,2,3,....m}$$

درنتیجه، می توان آن را مجدداً به عنوان

$$Maximize\ \left[Z^{(k)}\right]=f\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)$$

$$h^i\left(\left[\left(x_1^{(k)}\right),\left(x_2^{(k)}\right),...,\left(x_n^{(k)}\right)\right]\right)=0,\ \text{k=1,2,3,4,}\ \text{i=1,2,3,....m}$$

$$\left(x_j^{(k)}\right) \geq 0,\ \ i=1,2,...,m,\ \ \ j=1,2,...,n,\ \ i=1,2,...,m\ \ \ k=1,2,3,4$$

تابع لاگرانژی را که برای ارزیابی نقاط ثابت با استفاده از روش ضریب لاگرانژی تعریف شده است، نشان دهیم:

$$\left[L(X,\lambda)\right] = f\left(x_j\right) - \sum_{i=1}^{m} \lambda_i \left[h^i\left(x_j\right)\right]$$

که در آن $i=1,2,...,m$ و $j = 1,2,\ldots,n$ و m تا ضریب لاگرانژ که با λ_i ها نمایش می دهیم.

روش ضریب لاگرانژ لزوماً به شرایط زیر نیاز دارد :

$$\frac{\partial L}{\partial x_j} \equiv \frac{\partial f}{\partial x_j} - \sum_{i=1}^{m} \lambda_i \frac{\partial h^{(i)}}{\partial x_j} = 0$$

$$\frac{\partial L}{\partial \lambda_i} \equiv -\left[h^i\left(x_j\right)\right] = 0$$

شرایط کافی برای روش ضریب لاگرانژ را می توان به صورت بیان کرد:

$$H^B = \begin{vmatrix} 0 & \mathrm{M} \\ M^T & \mathrm{N} \end{vmatrix}_{(m+n)\times(m+n)}$$

که در آن m و n به ترتیب تعداد محدودیت ها و تعداد متغیرها را نشان می دهد، ماتریس بالا به عنوان ماتریس هسیان شناخته می شود.

$$M = \begin{vmatrix} \frac{\partial h^{(i)}}{\partial x_j} & \frac{\partial h^{(i)}}{\partial x_{j+1}} & \cdots & \frac{\partial h^{(i)}}{\partial x_{j+n}} \\ \frac{\partial h^{(i+1)}}{\partial x_j} & \frac{\partial h^{(i+1)}}{\partial x_{j+1}} & \cdots & \frac{\partial h^{(i+1)}}{\partial x_{j+n}} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial h^{(i+m)}}{\partial x_j} & \frac{\partial h^{(i+m)}}{\partial x_{j+1}} & \cdots & \frac{\partial h^{(i+m)}}{\partial x_{j+n}} \end{vmatrix}$$

$$N = \begin{vmatrix} \frac{\partial^2 L}{\partial x_j^2} & \frac{\partial^2 L}{\partial x_j \partial x_{j+1}} & \cdots & \frac{\partial^2 L}{\partial x_j \partial x_{j+n}} \\ \frac{\partial^2 L}{\partial x_{j+1} \partial x_j} & \frac{\partial^2 L}{\partial x_{j+1}^2} & \cdots & \frac{\partial^2 L}{\partial x_{j+1} \partial x_{j+n}} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial^2 L}{\partial x_{j+n} \partial x_j} & \frac{\partial^2 L}{\partial x_{j+n} \partial x_{j+1}} & \cdots & \frac{\partial^2 L}{\partial x_{j+n}^2} \end{vmatrix}$$

به صورت فازی، شرایط کافی برای روش ضریب لاگرانژ به شرح زیر است:

$$N = f\left(x_j^{(k)}\right) - \sum_{i=1}^{m} \lambda_i^{(k)} \left[h^i\left(x_j\right)^{(k)}\right] = 0$$

$$M=\left[h^{i}\left(x_{j}\right)^{(k)}\right]=0$$

که در آن i =1,2,...,m و j = 1,2,…,n و m تا ضریب لاگرانژ که با λ_i ها نمایش می دهیم.

درمرحله بعد، تابع عضویت فازی شرایط فوق را تعیین می کنیم. در نظر بگیرید:

$$E=\left(f_j^{(k)}\right), F=\left(\lambda_i^{(k)}\right), D=\left(h_j^{i(k)}\right), k=1,2,3,4$$

$$\mu_E(x)=\begin{cases}\dfrac{x-f_j^{(1)}}{f_j^{(2)}-f_j^{(1)}} & f_j^{(1)}\le x\le f_j^{(2)}\\ 1 & f_j^{(2)}\le x\le f_j^{(3)}\\ \dfrac{x-f_j^{(4)}}{f_j^{(3)}-f_j^{(4)}} & f_j^{(3)}\le x\le f_j^{(4)}\\ 0 \quad \text{در غیر این صورت} & \end{cases}$$

$$\mu_F(x)=\begin{cases}\dfrac{x-\lambda_j^{(1)}}{\lambda_j^{(2)}-\lambda_j^{(1)}} & \lambda_j^{(1)}\le x\le \lambda_j^{(2)}\\ 1 & \lambda_j^{(2)}\le x\le \lambda_j^{(3)}\\ \dfrac{x-\lambda_j^{(4)}}{\lambda_j^{(3)}-\lambda_j^{(4)}} & \lambda_j^{(3)}\le x\le \lambda_j^{(4)}\\ 0 \quad \text{در غیر این صورت} & \end{cases}$$

$$\mu_D(x)=\begin{cases}\dfrac{x-h_j^{(1)}}{h_j^{(2)}-h_j^{(1)}} & \mathrm{h}_j^{(1)}\le x\le h_j^{(2)}\\ 1 & \mathrm{h}_j^{(2)}\le x\le h_j^{(3)}\\ \dfrac{x-h_j^{(4)}}{h_j^{(3)}-h_j^{(4)}} & \mathrm{h}_j^{(3)}\le x\le h_j^{(4)}\\ 0 \quad \text{در غیر این صورت} & \end{cases}$$

برای تخمین زدن تابع عضویت فازی $F*D$ ها، با محاسبه α که سطح اطمینان برای D و F هست شروع کنید و سپس به محاسبه تابع عضویت فازی $F*D$ ادامه دهید. در معادلات اول و دوم به جای x برای تابع عضویت F، $a_1^{(\alpha)}$ و $a_2^{(\alpha)}$ جایگزین کنید.

$$\alpha=\frac{x_1^{(\alpha)}-\lambda_i^{(1)}}{\lambda_i^{(2)}-\lambda_i^{(1)}}\Rightarrow x_1^{(\alpha)}=\left(\lambda_i^{(2)}-\lambda_i^{(1)}\right)\alpha+\lambda_i^{(1)}$$

$$\alpha=\frac{x_2^{(\alpha)}-\lambda_i^{(4)}}{\lambda_i^{(3)}-\lambda_i^{(4)}}\Rightarrow x_2^{(\alpha)}=\left(\lambda_i^{(3)}-\lambda_i^{(4)}\right)\alpha+\lambda_i^{(4)}$$

بنابراین، F_α به عنوان فاصله اطمینان F نشان داده می شود،

$$F_\alpha = \left[\left(\lambda_i^{(2)} - \lambda_i^{(1)}\right)\alpha + \lambda_i^{(1)}, \left(\lambda_i^{(3)} - \lambda_i^{(4)}\right)\alpha + \lambda_i^{(4)}\right]$$

به طور مشابه، فاصله اطمینان C به صورت زیر است:

$$D_\alpha = \left[\left(h_j^{i(2)} - h_j^{i(1)}\right)\alpha + h_j^{i(1)}, \left(h_j^{i(3)} - h_j^{i(4)}\right)\alpha + h_j^{i(4)}\right]$$

پس از جایگذاری و ساده سازی تابع عضویت $F_\alpha * D_\alpha$ به شرح زیر است:

$$\mu\lambda_i h_j(x) = \begin{cases} \dfrac{-\left(\lambda_i^{(1)}h_j^{i(2)} + \lambda_i^{(2)}h_j^{i(1)} - 2\lambda_i^{(1)}h_j^{i(1)}\right) \pm \left(\left(\lambda_i^{(1)}h_j^{i(2)} + \lambda_i^{(2)}h_j^{i(1)} - 2\lambda_i^{(1)}h_j^{i(1)}\right)^2 - 4\lambda_i^{(2)}h_j^{i(2)}\lambda_i^{(1)}h_j^{i(1)} + 4\lambda_i^{(2)}h_j^{i(1)}\lambda_i^{(1)}h_j^{i(1)} + 4\lambda_i^{(1)}h_j^{i(2)}\lambda_i^{(1)}h_j^{i(1)} - 4\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(1)}h_j^{i(1)}\right)^{\frac{1}{2}}}{2\left(\lambda_i^{(2)}h_j^{i(2)} - \lambda_i^{(2)}h_j^{i(1)} - \lambda_i^{(1)}h_j^{i(2)} + \lambda_i^{(1)}h_j^{i(1)}\right)} \\ \dfrac{-\left(\lambda_i^{(3)}h_j^{i(4)} + \lambda_i^{(4)}h_j^{i(3)} - 2\lambda_i^{(4)}h_j^{i(4)}\right) \pm \left(\left(\lambda_i^{(3)}h_j^{i(4)} + \lambda_i^{(4)}h_j^{i(3)} - 2\lambda_i^{(4)}h_j^{i(4)}\right)^2 - 4\lambda_i^{(3)}h_j^{i(3)}\lambda_i^{(4)}h_j^{i(4)} + 4\lambda_i^{(3)}h_j^{i(4)}\lambda_i^{(4)}h_j^{i(4)} + 4\lambda_i^{(4)}h_j^{i(3)}\lambda_i^{(4)}h_j^{i(4)} - 4\lambda_i^{(4)}h_j^{i(4)}\lambda_i^{(4)}h_j^{i(4)}\right)^{\frac{1}{2}}}{2\left(\lambda_i^{(3)}h_j^{i(3)} - \lambda_i^{(3)}h_j^{i(4)} - \lambda_i^{(4)}h_j^{i(3)} + \lambda_i^{(4)}h_j^{i(4)}\right)} \\ 0 \qquad \text{درغ یرایِ ن صور ت} \end{cases}$$

به صورت فازی، شرایط لازم برای روش ضریب لاگرانژ به شرح زیر است:

$$f\left(x_j^{(k)}\right) - \sum_{i=1}^{m} \lambda_i^{(k)} \left[h^i\left(x_j^{(k)}\right)'\right] = 0$$

که در آن i =1,2,...,m و j = 1,2,…,n و m تا ضریب لاگرانژ که با λ_i ها نمایش می دهیم.

درمرحله بعد، تابع عضویت فازی را تعیین می کنیم. در نظر بگیرید:

$$E = \left(f_j^{(k)}\right), F = \left(\lambda_i^{(k)}\right), D = \left(h_j^{i(k)}\right), k = 1,2,3,4$$

اکنون فاصله اطمینان را برای هر درجه α برای تابع عضویتE محاسبه کنید. با جایگزین کردن مقادیر α در هر دو معادله تابع عضویت E داریم:

$$\alpha = \frac{x_1^{(\alpha)} - f'^{(1)}}{f'^{(2)} - f'^{(1)}} \Rightarrow a_1^{(\alpha)} = \left(f'^{(2)} - f'^{(1)}\right)\alpha + f'^{(1)}$$

$$\alpha = \frac{x_2^{(\alpha)} - f'^{(4)}}{f'^{(3)} - f'^{(4)}} \Rightarrow a_2^{(\alpha)} = \left(f'^{(3)} - f'^{(4)}\right)\alpha + f'^{(4)}$$

$$\{E\}_\alpha = \left[\left\{\left(f'^{(2)} - f'^{(1)}\right)\alpha + f'^{(1)}\right\}, \left\{\left(f'^{(3)} - f'^{(4)}\right)\right\}\alpha + f'^{(4)}\right]$$

تابع عضویت $F*D$ قبلا $\mu_{F*D}(x)$ محاسبه شده است.حال، فاصله اطمینان α را برای تابع عضویت فازی $F*D$ با جایگذاری f_1^{α} و f_2^{α} در هر دو معادله تابع عضویت $F*D$محاسبه می کنیم. در نهایت بعد از جایگذاری و ساده سازی خواهیم داشت:

$$\{E_\alpha\} - \left\{\left(F(*)D\right)_\alpha\right\} = \left\{e_1^{(\alpha)} - f_2^{(\alpha)}, e_2^{(\alpha)} - f_1^{(\alpha)}\right\} = \left\{\begin{matrix} -2E_1\alpha^2 - \left\{2F_1 - (f'^{(2)} - f'^{(1)})\alpha\right\} + f'^{(1)} - D_1, \\ -2E_2\alpha^2 - \left\{2F_2 - (f'^{(3)} - f'^{(4)})\alpha\right\} + f'^{(4)} - D_2 \end{matrix}\right\}$$

با جایگذاری کردن $\alpha = 0$ و $\alpha = 1$ تابع عضویت $\{E_\alpha(-)F_\alpha(*)D_\alpha\}$ به شرح زیر است:

$$\mu_{E(-)F(*)D}(x)=\begin{cases}\dfrac{-\left(2F_1-(f'^{(2)}-f'^{(1)})\right)\pm\left(\left\{2F_1-(f'^{(2)}-f'^{(1)})\right\}^2-8E_1\left(f'^{(1)}-D_1\right)\right)^{\frac{1}{2}}}{4E_1} & f'^{(1)}-\lambda_i^{(1)}h_i'^{(1)}\le x\le f'^{(2)}-\lambda_i^{(2)}h_i'^{(2)}\\ 1 & f'^{(2)}-\lambda_i^{(2)}h_i'^{(2)}\le x\le f'^{(3)}-\lambda_i^{(3)}h_i'^{(3)}\\ \dfrac{-\left(2F_2-(f'^{(3)}-f'^{(4)})\right)\pm\left(\left\{2F_2-(f'^{(3)}-f'^{(4)})\right\}^2-8E_2\left(f'^{(2)}-D_2\right)\right)^{\frac{1}{2}}}{4E_2} & f'^{(3)}-\lambda_i^{(3)}h_i'^{(3)}\le x\le f'^{(4)}-\lambda_i^{(4)}h_i'^{(4)}\\ 0 & \text{در غیر این صورت}\end{cases}$$

که در آن

$$E_1=\lambda_i^{(2)}h_i'^{(2)}\lambda_i^{(3)}h_j^{i(3)}-\lambda_i^{(2)}h_i'^{(2)}\lambda_i^{(3)}h_j^{i(4)}-\lambda_i^{(2)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(3)}+\lambda_i^{(2)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(4)}-\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(3)}+$$
$$\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(4)}+\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(3)}-\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(3)}h_j^{i(3)}+\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(3)}h_j^{i(4)}+$$
$$\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(3)}-\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(4)}+\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(3)}-\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(3)}+\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}$$
$$F_1=\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(3)}-\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}+\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(3)}-\lambda_i^{(2)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(4)}+$$
$$\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(3)}+\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}+\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(3)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(4)}+$$
$$\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(3)}-\lambda_i^{(1)}h_i'^{(2)}\lambda_i^{(4)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(3)}h_j^{i(4)}+\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}-\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(3)}+\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}$$
$$D_1=\lambda_i^{(1)}h_i'^{(1)}\lambda_i^{(4)}h_j^{i(4)}$$
$$F_2=\lambda_i^{(2)}h_j^{i(1)}\lambda_i^{(3)}h_i'^{(4)}-\lambda_i^{(2)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}+\lambda_i^{(2)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(3)}+\lambda_i^{(2)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}-\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(3)}h_i'^{(4)}+$$
$$\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}-\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(3)}+\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}+\lambda_i^{(1)}h_j^{i(2)}\lambda_i^{(3)}h_i'^{(4)}-\lambda_i^{(1)}h_j^{i(2)}\lambda_i^{(4)}h_i'^{(4)}+$$
$$\lambda_i^{(1)}h_j^{i(2)}\lambda_i^{(4)}h_i'^{(3)}-\lambda_i^{(1)}h_j^{i(2)}\lambda_i^{(4)}h_i'^{(4)}-\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(3)}h_i'^{(4)}+\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}-\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(3)}+\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}$$
$$D_2=\lambda_i^{(1)}h_j^{i(1)}\lambda_i^{(4)}h_i'^{(4)}$$

۴. نتیجه‌گیری

تلاش شده است تا مدلی ایجاد شود که مساله برنامه ریزی غیرخطی را در یک محیط فازی حل کند. مدل فازی مساله با استفاده از شرایط لازم و کافی ضریب های لاگرانژی از نظر فازی مورد بررسی قرار گرفته است. که در آن یکی از تابع عضویت ها استفاده می کند و دیگری رویکرد رتبه بندی قوی تابع عضویت نقش مهمی در ایجاد یک مدل در زمینه فازی ایفا می کنند. بیشتر تکنیک های تحقیق در ایجاد تنها تابع عضویت ها برای اهداف یا محدودیت های فازی مورد بحث قرار گرفته اند. با این حال، این رویکرد پیچیدگی متقابل اهداف و همچنین محدودیت ها را با استفاده از توابع عضویت حل کرد. این مدل یک رویکرد کارآمد برای مقابله با مسایل برنامه ریزی غیرخطی ارائه می دهد. بنابراین، جواب بهینه از طریق فازی بودن در نتیجه و بحث مشخص شده است. علاوه بر این، جواب با روش عضویت فازی ذوزنقه ای مورد بررسی قرار میگیرد. علاوه بر این، تجزیه و تحلیل مقایسه می تواند یک تلاش جدید طراحی شده برای حل برنامه ریزی غیرخطی فازی باشد. این مدل بر پرداختن به عدم قطعیت ها و تجربیات ذهنی تصمیم گیرندگان تمرکز دارد و می تواند به حل مسائل تصمیم گیری کمک کند. در آینده مدل پیشنهاد می کندکه این مدل در انواع دیگر مسایل برمانه ریزی غیرخطی یا مدل های بهینه سازی غیرخطی مناسب در مدل های آینده، ترجیحاً مدل های بهینه سازی، تحت موقعیت های فازی متعدد استفاده شود.

۵. مراجع

[1] Zimmermann, H.-J. Fuzzy Sets, Decision Making, and Expert Systems; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012; Volume 10.
[2] Vasant, P.; Nagarajan, R.; Yaacob, S. Fuzzy linear programming: A modern tool for decision making. In Computational Intelligence for Modelling and Prediction; Springer: Berlin/Heidelberg, Germany, 2005; pp. 383–401.
[3] Kheirfam, B.; Hasani, F. Sensitivity analysis for fuzzy linear programming problems with fuzzy variables. Adv. Model. Optim. 2010, 12, 257–272.
[4] Palanivel, K. Contributions to the Study on Some Optimization Techniques in Fuzzy Membership Functions; Bharathidasan University: Trichy, Tamil Nadu, India, 2013.
[5] Klanšek, U. A Comparison between Milp and Minlp Approaches to Optimal Solution of Nonlinear Discrete Transportation Problem. Transport 2014, 30, 135–144.
[6] Das, A.; Lee, G.M. A Multi-Objective Stochastic Solid Transportation Problem with the Supply, Demand, and Conveyance Capacity Following the Weibull Distribution. Mathematics 2021, 9, 1757.
[7] Ahmadini, A.A.H.; Varshney, R.; Ali, I. On multivariate-multiobjective stratified sampling design under probabilistic environment: A fuzzy programming technique. J. King Saud. Univ.-Sci. 2021, 33, 101448.
[8] Khan, M.F.; Modibbo, U.M.; Ahmad, N.; Ali, I. Nonlinear optimization in bi-level selective maintenance allocation problem. J. King Saud. Univ.-Sci. 2022, 34, 101933.
[9] Ali, S.S.; Barman, H.; Kaur, R.; Tomaskova, H.; Roy, S.K. Multi-Product Multi Echelon Measurements of Perishable Supply Chain: Fuzzy Non-Linear Programming Approach. Mathematics 2021, 9, 2093.
[10] El-Sobky, B.; Abo-Elnaga, Y.; Mousa, A.A.A.; El-Shorbagy, M.A. Trust-Region Based Penalty Barrier Algorithm for Constrained Nonlinear Programming Problems: An Application of Design of Minimum Cost Canal Sections. Mathematics 2021, 9, 1551.
[11] Gupta, D.; Borah, P.; Sharma, U.M.; Prasad, M. Data-driven mechanism based on fuzzy Lagrangian twin parametric-margin support vector machine for biomedical data analysis. Neural Comput. Appl. 2021, 1–11.
[12] Gani, A.N.; Saleem, R.A. Solving Fuzzy Sequential Quadratic Programming Algorithm for Fuzzy Non-Linear Programming. J. Phys. Sci. 2018, 23, 89–96.
[13] Palanivel, K. Fuzzy commercial traveler problem of trapezoidal membership functions within the sort of α optimum solution using ranking technique. Afr. Mat. 2016, 27, 263–277.
[14] Saranya, R.; Palanivel, K. Fuzzy nonlinear programming problem for inequality constraints with alpha optimal solution in terms of trapezoidal membership functions. Int. J. Pure Appl. Math. 2018, 119, 53–63.

حل عددی معادلات انتگرال خطی ترکیبی ولترا- فردهلم براساس توابع پایه ای اصلاح شده

آتنا غیاثی*[1]، دکتر بهمن غضنفری[2]

1- دانشجوی دکتری ریاضی کاربردی دانشگاه لرستان

2- دانشیار ریاضی کاربردی دانشگاه لرستان

چکیده

تکنیک به کار گرفته شده در این مقاله برای حل عددی معادله انتگرال خطی ترکیبی ولترا- فردهلم بر اساس توابع بلاک پالس اصلاح شده در بازه $[0, T)$ است. بیان می کند که نرخ همگرایی و دقت روش ارائه شده بهتر از روش مبتنی بر توابع بلاک پالس است. که همراه با مثال عددی در پایان تایید می شود.

کلمات کلیدی: معادله انتگرال خطی ترکیبی ولترا- فردهلم از نوع دوم، ماتریس عملیاتی انتگرال، معادلات اصلاح شده بلاک پالس MBPFs

1.مقدمه

معادلات انتگرال در زمینه های مختلف علوم و کاربردهای متعددی در نظریه تقریب، دینامیک سیالات، الکترودینامیک، پزشکی و غیره یافت می شود. اخیراً چندین کار به وجود جواب نوع ترکیبی معادلات انتگرال ولترا- فردهلم اختصاص یافته است [1, 2, 3]. حل تحلیلی این نوع معادله انتگرال در [1, 4, 5] به دست می آید، در حالی که روش های عددی جایگاه مهمی در حل آنها دارند. معادله انتگرال خطی ترکیبی ولترا- فردهلم از نوع دوم $(LMV - FIESK)$ که به شکل زیر

$$X(t) = f(t) + \int_0^t \int_a^b k(x,s)X(s)dsdx \quad (1)$$

در این مقاله در نظر گرفته شده است، جایی که f تابع معلوم و k هسته مشخصی می باشند، در حالی که $X(t)$ تابع مجهول معادله است .

در [6]، ابراهیم و همکاران. از روش تکراری جدید برای حل معادلات انتگرال ترکیبی ولترا- فردهلم استفاده کره اند.وانگ این مشکل را در [7] با استفاده از روش هم محلی تیلور رفع کرد. شاهوث در [8]] معادلات انتگرال ولترا-فردهلم از نوع دوم را با استفاده از روش چندجمله ای برنشتاین حل کرد. علاوه بر این، عزتی و نجفعلی زاده از موجک کاس برای حل معادلات انتگرال ولترا-فردهولم در [9]استفاده کرده اند.

* **Corresponding author**
Email: ghiasi.at@fs.lu.ac.ir
ghazanfari.ba@Lu.ac.ir

این مقاله به شرح زیر تنظیم شده است. در ادامه این بخش، مفاهیم کلی در مورد توابع بلاک پالس و توابع بلاک پالس اصلاح شده اپسیلون و ماتریس عملیاتی مرتبط با معادله انتگرال را شرح می دهیم. در بخش سوم روش عددی با استفاده از ماتریس عملیاتی شرح داده می شود، بخش چهارم مرتبط به آنالیز خطا است در بخش پنجم مثال های عددی به همراه جدول نتایج و نمودارها ارائه می گردد و نتیجه کار را در بخش پایانی بیان میکنیم.

2. تعاریف و مقدمات

توابع بلاک پالس BPF ها در [10,11] به طور اختصاصی مورد مطالعه قرار گرفته اند و برای حل مسائل مختلف استفاده شده اند. هدف این بخش یادآوری نمادها و تعریف BPF هایی است که در بخش های بعدی استفاده می شود. توابع بلاک پالس در بازه زمانی $[0,T)$ به صورت

$$\varphi_i(t) = \begin{cases} 1, (i-1)\dfrac{T}{m} \le t \le i\dfrac{T}{m} \\ 0, \quad o.w \end{cases} \qquad (2)$$

که در آن $i = 1,\dots,m$ و برای راحتی $h = T/m$ توابع بلاک پالس روی $[0,T)$ دارای ویژگی های زیر هستند:

• **مجزا بودن:**

$$\varphi_i(t)\varphi_j(t) = \delta_{ij}\,\varphi_i(t)\,; \quad i,j = 1,\dots,m$$

δ_{ij} دلتا کرونکر می باشد.

•**متعامدبودن**

$$\int_0^T \varphi_i(t)\varphi_j(t)\,dt = h\delta_{ij}$$

• **کامل بودن:**

$$\int_0^T f^2(t)\,dt = \lim_{m\to\infty} \sum_{i=0}^{m} f_i^2 \|\varphi_i(t)\|^2$$

$$f_i = \frac{1}{h}\int_0^T f(t)\varphi_i(t)\,dt \qquad (3)$$

همچنین ضرایب فوریه f_i و توابع بلاک پالس به m بستگی دارد. مجموعه توابع بلاک پالس ممکن است به صورت بردار $\Phi(t)$ نوشته می شود

$$\Phi(t) = (\varphi_1(t), \varphi_2(t), \dots, \varphi_m(t))^T, \qquad t\epsilon[0,T)$$

$$\Phi(t)\Phi^T(t) = \begin{bmatrix} \varphi_1(t) & 0 & \dots & 0 \\ 0 & \varphi_2(t) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \varphi_m(t) \end{bmatrix}_{(m)\times(m)}$$

$$\Phi^T(t)\Phi(t) = 1$$

$$\Phi(t)\Phi^T(t)F = D_F\,\Phi(t)$$

که در آن F یک تابع برداری است .بسط یک تابع f(t) روی [0, T) با توجه به $\varphi_i(t)$، $i = 1,\dots,m$، توسط

$$f(t) \simeq \sum_{i=1}^{m} f_i\,\varphi_i(t) = F^T\Phi(t) = \Phi^T(t)F \qquad F = (f_1, f_2, \dots, f_m)^T$$

با توجه به $k(s,t) \in L^2([0,T_1) \times [0,T_2))$ $BPFs$ بسط می یابد.

$$k(s,t) = \Phi^T(s)K\Psi(t)$$

که در آن که در آن $\Phi(s)$ و $\Psi(t)$ به ترتیب بردارهای BPF های m_1 و m_2 بعدی هستند و K ماتریس ضرایب بلاک پالس $m_1 \times m_2$ با مولفه های $k_{ij}, i = 1, \dots, m_1, g = 1, \dots, m_2$ است که برای راحتی $m_1 = m_2 = m$, $T_1 = T_2 = T$ در نظر می گیریم.

اکنون، ماتریس عملیات انتگرالی را به صورت زیر در نظر می گیریم و محاسبه می کنیم:

$$\int_0^t \varphi_i(s)\, ds = \begin{cases} 0\,, & 0 \le t \le (i-1)h \\ t-(i-1)h\,, & (i-1)h \le t \le ih \\ h\,, & ih \le t \le 1 \end{cases}$$

از آنجایی که $t - ih$ برابر است با $h/2$ در نقطه وسط، $[\mathrm{ih}, (\mathrm{i}+1)\mathrm{h})$ می توانیم تقریبی $t-(i-1)h$ ، برای $(i-1)h \le t < ih$ توسط $h/2$ را در نظر بگیریم. بنابراین

$$\int_0^t \varphi_i(s)\, ds = \left(0, \dots, 0, \frac{h}{2}, h, \dots, h\right) \Phi(t)$$

به طوریکه مولفه iام $\frac{h}{2}$ است.

$$\int_0^t \Phi(s)\, ds = P\Phi(t)$$

که ماتریس عملیاتی P به صورت زیر تبدیل می شود:

$$P = \frac{h}{2}\begin{pmatrix} 1 & 2 & 2 & \cdots & 2 \\ 0 & 1 & 2 & \dots & 2 \\ 0 & 0 & 1 & \dots & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$\int_0^t \mathrm{f}(s)\, ds = \int_0^t \mathrm{F}^T \Phi(s)\, ds = \mathrm{F}^T P \Phi(t) \quad (4)$$

توابع بلاک پالس اپسیلون اصلاح شده(EMBPF): مجموعه ای از توابع بلاک پالس اپسیلون اصلاح شده $\theta_i(t), i = 0, \dots, m$، در بازه $[0, \mathrm{T})$ تعریف می شوند

$$\theta_0(t) = \begin{cases} 1, & t\epsilon\left[0, \frac{T}{m} - \varepsilon\right) = I_0 \\ 0\,, & o.w \end{cases}$$

$$\theta_i(t) = \begin{cases} 1, & t\epsilon\left[i\frac{T}{m} - \varepsilon, (i+1)\frac{T}{m} - \varepsilon\right) = I_i\,, \quad i = 1, \dots, m-1 \\ 0\,, & o.w \end{cases}$$

$$\theta_m(t) = \begin{cases} 1, & t\epsilon[T-\varepsilon, T) = I_m \\ 0\,, & o.w \end{cases}$$

$EMBPF$ ها مشابه BPF ها، مهمترین خواص(ماتریس عملیاتی و بردارها) و ویژگی ها (مجزا بودن، متعامد بودن و کامل بودن) را با همان حالات دارا هستند

$$\Theta_{m+1}(t)\Theta^T{}_{m+1}(t) = \begin{bmatrix} \Theta_0(t) & 0 & \dots & 0 \\ 0 & \Theta_1(t) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & & \Theta_n(t) \end{bmatrix}_{(m+1)\times(m+1)}$$

$$\int_0^t \Theta_{m+1}(s)\, ds \simeq P\Theta_{m+1}(t) \quad (5)$$

$$P=\begin{bmatrix}\frac{h-\varepsilon}{2} & h-\varepsilon & \dots & h-\varepsilon\\ 0 & \frac{h}{2} & \cdots & h\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & \frac{\varepsilon}{2}\end{bmatrix}_{(m+1)\times(m+1)} \quad (6)$$

$$f_i=\frac{1}{\Delta I_i}\int_0^T f(t)\theta_i(t)\,dt\,;i=0,\dots,m \quad (7)$$

$$k_{ij}=\frac{1}{\Delta I_i\Delta I_i}\int_0^T\int_0^T k(s,t)\theta_i(s)\theta_j(t)dtds$$

$$\int_0^t \mathrm{f}(s)\,ds\simeq\int_0^t \mathrm{F}^T\Theta(s)\,ds\simeq \mathrm{F}^T P\Theta(t) \quad (8)$$

3. حل معادلات انتگرال خطی مختلط ولترا- فردهولم با استفاده از توابع پالس بلوک اصلاح شده

ما معادله انتگرال خطی مختلط ولترا- فردهولم (1) را در نظر می گیریم و توابع $k(s,t), X(t), \mathrm{f}(t)$ آن را تقریب می زنیم

$$X(t)\simeq X^T\Phi(t)=\Phi^T(t)X,$$
$$f(t)\simeq F^T\Phi(t)=\Phi^T(t)F,$$
$$K(x,s)\simeq\Phi^T(t)K\Phi(s)=\Phi(s)K\Phi^T(t)$$

در تقریب های بالا، F و X بردار ضرایب بلاک پالس اصلاح شده هستند و K که در آن ماتریس عملیاتی انتگرال $MBPF$ ها هستند. بنابراین می توانیم با جایگزینی روابط فوق در معادله (1)، داریم

$$X^T\Phi(t)\simeq F^T\Phi(t)+\int_0^t\int_a^b\Phi^T(x)K\Phi(s)\Phi^T(s)Xdsdx$$
$$X^T\Phi(t)\simeq F^T\Phi(t)+\int_0^t\Phi^T(x)K\left(\int_a^b\Phi(s)\Phi^T(s)ds\right)Xdx$$
$$X^T\Phi(t)\simeq F^T\Phi(t)+\int_0^t\Phi^T(x)KhI\,Xdx$$
$$X^T\Phi(t)\simeq F^T\Phi(t)+X^T(hK)^T\int_0^t\Phi^T(x)\,dx$$
$$X^T\Phi(t)\simeq F^T\Phi(t)+X^T(hK)^TQ\Phi(t)$$

$$X^T\simeq F^T+X^T(hK)^TQ$$
$$X^T-X^T(hK)^TQ\simeq F^T$$
$$X^T(I-(hK)^TQ)\simeq F^T$$

بنابراین با جایگزینی $M=(I-(hK)^TQ)^T$ و تبدیل $\simeq$ به $=$، خواهیم داشت

$$MX=F$$

4. آنالیز خطا:

با استفاده از قضایای زیر و با فرض، $T=1, h=\frac{T}{m}=\frac{1}{m}$

قضیه 4.1 اگر $\hat{f}_m(t) = \sum_{i=0}^{m} f_i\,\psi_i(t)$ و $f_i = \frac{1}{\Delta(I_i)}\int_0^1 f(t)\psi_i(t)\,dt, i = 0, \dots, m$ آنگاه

a) $\delta = \int_0^1 (f(t) - \sum_{i=0}^{m} f_i\,\psi_i(t))^2\,dt$ ، به حداقل مقدار خود می رسد.

b) $\{\hat{f}_m(t)\}$ به سمت $f(t)$ نزدیک می شود

c) $\int_0^1 f^2(t)\,dt = \sum_{i=0}^{\infty} f^2{}_i\,\|\psi_i\|^2$

. **اثبات** در [12] بیان می شود، اما فواصل انتگرال باید براساس I_i، $i = 0, \dots, m$, دوباره تعریف شوند

قضیه 4.2 فرض کنید

a) $f(t)$. پیوسته و قابل تفکیک در بازه $[-\mathrm{h}, 1 + \mathrm{h}]$ با مشتق محدود باشد، یعنی $|f'(t)| < M$

b) $\hat{f}_{\frac{ih}{k}}(t), i = 0,1, \dots, k-1$ به ترتیب BPF ها ، $\frac{h}{k}$ MBPF ها،...، $\frac{(k-1)h}{k}$ MBPF بسط های $f(t)$ بر اساس $m + 1\ MBPF$ در بازه زمانی $[0,1)$ هستند.

c) $\bar{f}(t) = \frac{1}{k}\sum_{i=0}^{k-1} \hat{f}_{\frac{ih}{k}}(t)$

آنگاه در بازه $[h, 1-h]$

$$\left\|f(t) - \hat{f}_{\frac{ih}{k}}(t)\right\| = o(h) \qquad \|f(t) - \bar{f}(t)\| = o\left(\frac{h}{k}\right)$$

اثبات. بیا کمک قاعده ذوزنقه ای برای انتگرال داریم

$$\int_a^b f(t)dt = \frac{b-a}{2}\big(f(a)+f(b)\big) - \frac{(b-a)^3 f''(\eta)}{12} = \frac{b-a}{2}\big(f(a)+f(b)\big) + E,\ \ \eta\epsilon[a,b] \quad (8)$$

که در آن E خطای انتگرال گیری است. فرض کنید $t_i = \frac{i}{m} = ih$ و $I_i = [\,t_{i-1}, t_i]$

خطای نمایش زمانی که $f(t)$ با یک سری BPF در هر زیر بازه $\left[t_i, t_i + \frac{h}{k}\right]$، $i = 0, \dots, m-1$ نشان داده می شود

$$e_i(t) = f(t) - f_i\psi_i(t) = f(t) - f_i$$

به طوریکه $f_i = \frac{1}{h}\int_{ih}^{(i+1)h} f(t)dt$ طبق رابطه (8)

$$f_i = \frac{1}{2}(f(t_i) + f(t_i + h) + E$$

بدیهی است که اگر $f(t) = t$ (ثابت)، پس $f(t) = C$ $e_i(t) = 0$.بنابراین، خطا محاسبه می شود در بازه $\left[t_i, t_i + \frac{h}{k}\right]$

برای بازه $i = 1, \dots, m-1$ برای این تابع $E = 0$ است. در اینصورت

$$e_i(t) = |t - f_i| = \left|t - \frac{t_i + t_{i+1}}{2}\right| = \left|t - (t_i + \frac{h}{2})\right| \le \frac{h}{2}$$

آنگاه خطای BPFها برابر $\frac{h}{2}M$ است.

به طور مشابه، خطای زمانی که $f(t)$ در یک سری از $MBPF$ ها در هر زیر بازه $\left[t_i, t_i + \frac{h}{k}\right]$ قرار می گیرد.

$$e_i(t)=\left|t-\left(\frac{\sum_{j=0}^{k-1}(t_i-(\frac{jh}{k})+t_{i+1}\ -(\frac{jh}{k})}{2k}\right)\right|=\left|t-\left(\frac{\sum_{j=0}^{k-1}(t_i-(\frac{jh}{k})+t_i+h\ -(\frac{jh}{k})}{2k}\right)\right|$$
$$=\left|t-\left(t_i+\frac{h}{2}\right)-\frac{(k-1)h}{2k}\right|\leq\frac{h}{2k}$$

بنابراین خطای $\varepsilon MBPF$ها $\frac{h}{2k}M$ است و برای I_0 در بازه $\left[0,\frac{h}{k}\right]$ داریم

$$e_i(t)=\left|t-\sum_{j=0}^{k-1}\frac{h-(\frac{jh}{k})}{2k}\right|=\left|t-\left(\frac{h}{2}-\frac{(k-1)h}{4k}\right)\right|=\left|t-\left(\frac{h}{4}+\frac{h}{4k}\right)\right|=o(\frac{h}{4})$$

بنابراین خطا $o(\frac{h}{4})$ است و برای بازه I_n نیز به همین صورت حاصل می شود.

حالا

$$\|e_i(t)\|^2=\int_{t_i}^{t_i+\frac{h}{k}}|e_i(t)|^2dt=\int_{t_i}^{t_i+\frac{h}{k}}\frac{h^2}{4k^2}\,M^2dt=\frac{h^3}{4k^3}\,M^2,$$

$$\|e\|^2=\int_0^1e^2(t)dt=\int_0^1\left(\sum_{i=1}^{n}\sum_{j=0}^{k-1}e_i(t)\right)^2dt=\sum_{i=1}^{n}\sum_{j=0}^{k-1}\int_0^1\left(e_i(t)\right)^2dt=\sum_{i=1}^{n}\sum_{j=0}^{k-1}\|e_i(t)\|^2$$
$$=\frac{1}{h}.k.\frac{h^3}{4k^3}\,M^2=\frac{h^2}{4k^2}\,M^2$$

خطای نمایش بین $f(s,t)$ و بسط $2D-\varepsilon MBPF$ها آن f_{ij} در هر زیرناحیه D_{ij} را تعریف می کنیم، به صورت زیر معرفی می کنیم.

$$e_{ij}(s,t)=f(s,t)-f_{ij}$$

به طوریکه

$$D_{ij}:=\left\{(s,t)\middle|t_i\leq s\leq t_i+\frac{h}{k},\ t_j\leq t\leq t_j+\frac{h}{k}\right\}$$

با بسط تیلور و تشابه به بحث فوق،

$$\|e(s,t)\|=\frac{h}{2k}M.$$

قضیه4.3 فرض کنید که

$$P(\omega\epsilon\Omega:\|u(\omega,t)\|<\mathrm{C})=1\qquad\|k_i\|<\mathrm{C}\ ,i=1,2$$

آنگاه

$$\sup(E\ (\|u-\bar{u}\|^2))^{\frac{1}{2}}=o\left(\frac{h}{k}\right)\quad t\epsilon[h,1-h]\ ,0\leq t\leq T$$

اثبات. برای اثبات کامل به[13] رجوع کنید

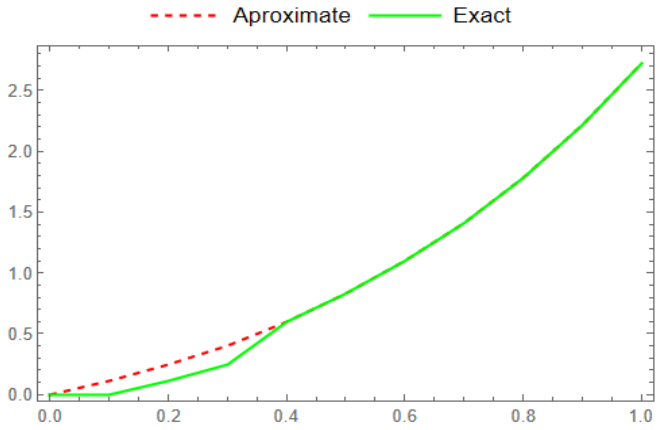
5. مثال های عددی

مثال5.1 معادله انتگرال خطی مختلط ولترا- فردهولم زیر را در نظر بگیرید.

$$X(t)=\sin(t)-\frac{1}{2}(t^2+2t)+\int_0^t\int_0^{\frac{\pi}{2}}(1+sx)X(s)dsdx\ ;\quad 0\leq t\leq 1$$

جواب دقیق این معادله $X(t)=\sin(t)$ می باشد

t_i \ $m = 1025$	Approximate $X(t_i)$	Exact solution $X(t_i)$
0	1.1100000e-07	0
0.1	0.1105170918	0.1105173029
0.2	0.2442805516	0.2442804182
0.3	0.4049576399	0.4049576839
0.4	0.5967297980	0.5967299999
0.5	0.8243607353	0.8243605244
0.6	1.0932712819	1.0932710072
0.7	1.4096268952	1.4096268228
0.8	1.7804327427	1.7804328799
0.9	2.2136428001	2.2136425812
1.0	2.7182818248	2.7182820090

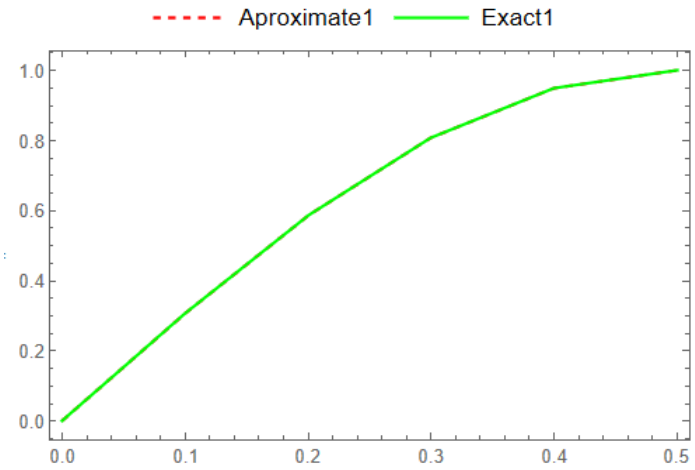


مثال5.2 معادله انتگرال خطی مختلط ولترا- فردهولم زیر را در نظر بگیرید.

$$X(t) = te^t - \frac{t^2}{2} + \int_0^t \int_0^1 x\, X(s) ds dx\,; \quad 0 \le t \le 1$$

دارای جواب تقریبی $X(t) = te^t$ می باشد

t_i \ $m = 1025$	Approximate $X(t_i)$	Exact solution $X(t_i)$
0	-0.000000175	0
0.1	0 0.309016874	0.309017127
0.2	0.587785364	0.587785120
0.3	0.809016978	0.809016968
0.4	0.951056625	0.951056312
0.5	1.000000000	0.999999670



6. نتیجه گیری

حل عددی معادلات انتگرال خطی ترکیبی ولترا- فردهلم مبتنی بر توابع بلاک پالس اصلاح شده با در نظر گرفتن $\varepsilon = \frac{1}{l}, l > m$ و ماتریس عملیات انتگرالی آنها معادله را به یک سیستم معادلات جبری کاهش می دهد که منجربه تسهیل و تسریع در محاسبات می شود. برنامه نویسی موازی (در این مقاله از نرم افزار متمتیکا استفاده شده است) براساس توابع بلاک پالس برای این روش بسیار مفید است. کارایی روش براساس توابع بلاک پالس اصلاح شده و درجه دقت خوب با مثالهای عددی نشان می دهد.

7. مراجع

[1] A. Aghajani and Y. Jalilian, Existence and global attractivity of Solution of a nonlinear functional Integral Equations, Communications in Nonlinear science and Numerical Simulation 15 , 3306-3312, 2010.

[2] H. Tidke and Iexistence and Uniqueness of Continuous Solution of Mixed Type Integral Equations in Cone Metric Space, Kathmandu University Journal of Science, Engineering and Technology,7(1), 48-55, 2011.

[3] M.A. Abdou and G.M. Abd Al-Kader, Mixed Type of FredholmVolterra Integral Equation, Le Matematiche, LX, pp. 41-58, 2005.

[4] M.A. Abdou, Integral Equation of Mixed Type and Integrals of Orthogonal Polynomials, J.Comp. Appl. Math. 138, 273-285, 2002.

[5] M.A. Abdou, On Asymptotic Method for Fredholm-Volterra Integral Equation of the Second Kind in Contact problem, J. Com. Appl. Math. 154, 431-446, 2003.

[6] H. Ibrahim, F. Attah, and G.T. Gyegwe, On the solution of Volterra-Fredholm and mixed Volterra-Fredholm integral equations using the new iterative method. Applied Mathematics, 6 (1): 1-5 2016.

[7] K. Wang and Q. Wang, Taylor Ollocation Method and Convergnce Analysis for the Volterra-Fredholm Integral Equations, Journal of Computational and Applied Mathematics, 260 ,294-300, 2014.

[8] M. Shahooth, Numerical Solution for Mixed Volterra-Fredhlm Integral Equations of the Second Kind By Bernstein Polyno- mials Method, Mathematical Theory and Modeling, 5 (10) 154-162,2015.

[9] R. Ezzati and S. Najafalizadeh, Numerical Methods for Solving Linear and Nonlinear Volterra-Fredholm Integral Equations by Using Cas Wavelets, World Applied Sciences Journal 18 (12): 1847-1854, 2012.

[10] K. Maleknejad and B. Rahimi, "Modification of block pulse functions and their application to solve numerically Volterra integral equation of the first kind," Communications in Nonlinear Science ear Science and Numerical Simulation, vol. 16, no. 6, pp. 2469– 2477, 2011.

[11] K. Maleknejad, M. Shahrezaee, and H. Khatami, "Numerical solution of integral equations system of the second kind by Block-Pulse functions," Applied Mathematics and Computation, vol. 166, no. 1, pp. 15–24, 2005.

[12] K. Maleknejad and M. Khodabin, and F. Hosseini Shekarabi, 'Modified Block Pulse Functions for Numerical Solution of Stochastic Volterra Integral Equations', Journal of Applied Mathematics, vol.4, pp. 1-10, 2014.

[13] Deb and Anish and Srimanti Roychoudhury, Control System Analysis and Identification with MATLAB: Block Pulse and Related Orthogonal Functions. New York: CRC Press, 2019.

https://aparat.com/v/frmx918

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

On Euler Sombor index of Hexagonal systems

Amir Karimi, Zahra Samiei
Department of Mathematics, Faculty of Sciences,
Golestan University, Gorgan, Iran
Amir.krm265@gmail.com; samieizahra96@gmail.com

Fateme Movahedi[1]
Department of Mathematics, Faculty of Sciences,
Golestan University, Gorgan, Iran
f.movahedi@gu.ac.ir

ABSTRACT

Let $G = (V, E)$ be a simple graph with vertex set V and edge set E. More recently a new degree-based topological index called the Euler Sombor index is defined as

$$EU(G) = \sum_{uv \in E} \sqrt{d_u^2 + d_v^2 + d_u d_v},$$

where d_u is denoted by the degree of $u \in V$.

In this paper, we investigate the Euler Sombor index for hexagonal systems and characterize graphs with the minimum and maximum values of this index among all hexagonal systems. Furthermore, we give the exact formula of the Euler Sombor index for Hexagonal networks and Non-Kekulean Benzenoid Hydrocarbon.

KEYWORDS: Euler Sombor index, Hexagonal network, Hexagonal system, Topological index, Non-Kekulean Benzenoid Hydrocarbon.

1 INTRODUCTION

Suppose that $G = (V, E)$ is a simple graph with vertex set V and edge set E. For a vertex $x \in V(G)$, the degree of the vertex x, denoted by $d(x)$, is the number of vertices adjacent to x. Denote δ and Δ for the minimum and maximum degree in the graph G.

A topological index is a number calculated from a chemical structure. These indices are useful in chemistry, medicine, and materials science, providing quick and insightful ways to study molecules and forecast their properties. For a detailed review of recent findings on topological indices and their applications, refer to [1-6].

More recently, Tang and Deng [7] introduced a new degree-based topological index namely the Euler Sombor index, defined as

$$EU(G) = \sum_{xy \in E} \sqrt{d(x)^2 + d(y)^2 + d(x)d(y)}.$$

For recent results in the mathematical properties and the applications of the Euler Sombor index, we refer to [7-10].

In this paper, we investigate the Euler Sombor index for a hexagonal system, a hexagonal network and a non-kekulean benzenoid hydrocarbon.

[1] Corresponding author

The hexagon unit cell is defined by a single line, a six-fold symmetry axis, about which cells can be turned by $60A°$ or $120A°$ without changing their appearance. Hexagons are a universal part of digital reality systems that combine sensors, software, and self-driving technologies [11].

2 MAIN RESULTS

We suppose that $E_{ij} = \{uv \in E : d(u) = i \text{ and } d(v) = j\}$ and $m_{i,j} = |E_{ij}|$. Therefore, using the edge-partition method, the definition of the Euler Sombor index of graph G is equivalent to

$$EU(G) = \sum_{\delta \le i \le j \le \Delta} m_{i,j}\sqrt{i^2 + j^2 + ij}.$$

First, we consider the graphs related to the hexagonal system. Hexagonal systems, which are natural graphical representations of benzenoid hydrocarbons, form a significant category of chemical graphs. We used the notations defined in [12]. The quantities of fissures, bays, coves, and fjords of a hexagonal system H depicted in Figure 1(a) are represented by $f = f(H)$, $B = B(H), C = C(H)$, and $F = F(H)$. The number of inlets is

$$r = r(H) = f + B + C + F.$$

We denote by $n = n(H)$ the number of vertices of $H, n_i = n_i(H)$ the number of internal vertices of H, and by $h = h(H)$ the number of hexagons of H.

Let L_h and E_h be a linear hexagonal chain and a catacondensed hexagonal system with h hexagonal, respectively (see Figure 1 (b, c)). Note that a catacondensed hexagonal system H is a hexagonal system such that $n_i(H) = 0$. Now, we state the following result that will be used in the next theorems.

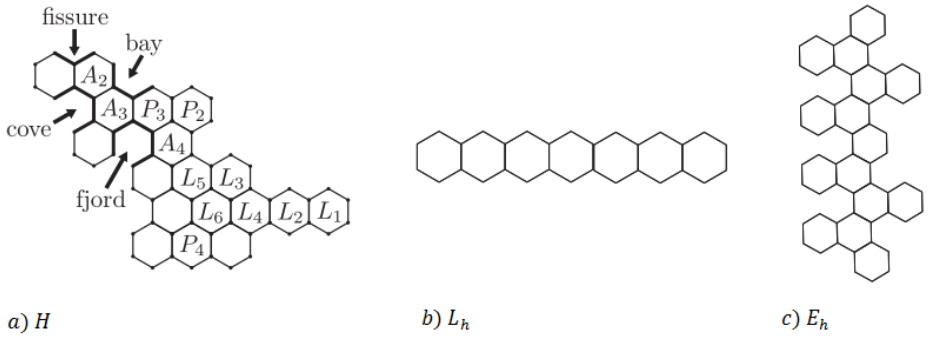


Figure 1: a) A hexagonal system H with structural features, b) Linear hexagonal system L_h, c) Catacondensed hexagonal system E_h.

Lemma 2.1 [13] *For a hexagonal system H with h hexagons,*

$$r(H) \le 2(h-1) = r(L_h).$$

Lemma 2.2 [14] *If H is a catacondensed hexagonal system with h hexagons, then*

$$r(E_h) = \left\lceil \frac{h}{2} + 1 \right\rceil \le r(H).$$

Table 1: The cardinality of edge-partition sets of the hexagonal system H.

Edge subsets	E_{22}	E_{23}	E_{33}
Cardinality	$2h - r - n_i + 4$	$2r$	$3h - r - 3$

Theorem 2.3 *Let H be a hexagonal system with h hexagons, r inlets and $n_i$internal vertices. Then*

$$EU(H) = 13\sqrt{3}h + \left(2\sqrt{19} - 5\sqrt{3}\right)r - 2\sqrt{3}n_i - \sqrt{3}.$$

Proof. According to the structure of the graph H, the degrees of vertices in this graph are 2 and 3. Using the edge-partition method and the results obtained in [12,15], the number of edges of edge subsets $E_{ij}$for $2 \le i \le j \le 3$ is shown in Table 1. Therefore, we get

$$\begin{aligned} EU(H) &= 3\sqrt{2}m_{2,2} + \sqrt{19}m_{2,3} + 3\sqrt{3}m_{3,3} \\ &= 3\sqrt{2}(2h - r - n_i + 4) + \sqrt{19}(2\mathrm{r}) + 3\sqrt{3}(3h - r - 3) \\ &= 13\sqrt{3}h + \left(2\sqrt{19} - 5\sqrt{3}\right)\mathrm{r} - 2\sqrt{3}\mathrm{n_i} - \sqrt{3}. \end{aligned}$$

■

Next, we characterize the graphs among all hexagonal systems with h hexagons that attain the maximal and minimal EU index.

Theorem 2.4 *Let H be a hexagonal system with h hexagons. Then*

$$EU(H) \le \left(3\sqrt{3} + 4\sqrt{19}\right)h + 9\sqrt{3} - 4\sqrt{19}.$$

with the equality if and only if H is the linear hexagonal chain with h hexagonal.

Proof. According to the structure of L_h shown in Figure 1(b), we have $r(L_h) = 2(h-1)$ and $n_i(L_h) = 0$. Therefore using Theorem 2.3, we get

$$EU(L_h) = (3\sqrt{3} + 4\sqrt{19})h + 9\sqrt{3} - 4\sqrt{19}.$$

On the other hand, using Lemma 2.1 and since $2\sqrt{19} - 5\sqrt{3} > 0$, we have

$$EU(L_h) - EU(H) = (2\sqrt{19} - 5\sqrt{3})(2(h-1) - r(H)) + 2\sqrt{3}n_i(H) \ge 0.$$

■

Theorem 2.5 *Let H be a catacondensed hexagonal system with h hexagons. Then*

$$EU(E_h) \le EU(H) \le EU(L_h).$$

Proof. The upper bound is deduced from Theorem 2.4. For lower bound, since $n_i(E_h) = 0$ and using Lemma 2.1 and Theorem 2.3, we get

$$EU(E_h) = 13\sqrt{3}h + (2\sqrt{19} - 5\sqrt{3})\lceil \tfrac{h}{2} + 1 \rceil - \sqrt{3}.$$

According to the structure of the catacondensed hexagonal system H, we have $n_i(H) = 0$. Therefore, using Theorem 2.3 and since $2\sqrt{19} - 5\sqrt{3} > 0$, we have

$$EU(H) - EU(E_h) = (2\sqrt{19} - 5\sqrt{3})(r - \lceil \tfrac{h}{2} + 1 \rceil) \ge 0.$$

■

Another important class of hexagonal systems is hexagonal chains. Assuming the number of L_1-type, L_2-type, A_2-type, and A_3-type hexagons are denoted by $l_1 = l_1(H)$, $l_2 = l_2(H)$, $a_2 = a_2(H)$, and $a_3 = a_3(H)$, respectively (see Figure 1 (a)). Hexagonal chains are catacondensed hexagonal systems where $a_3(H) = 0$.

Table 2: The cardinality of edge-partition sets of the hexagonal system H.

Edge subsets	E_{22}	E_{23}	E_{33}
Cardinality	$a_2 + 6$	$4(h-1) - 2a_2$	$h - 1 + a_2$

Theorem 2.6 *If H is a hexagonal chain with h hexagons, then*

$$EU(H) = (3\sqrt{3} + 4\sqrt{19})h + (5\sqrt{3} - 2\sqrt{19})a_2 + 9\sqrt{3} - 4\sqrt{19}.$$

Proof. According to the structure of the hexagonal chain and the results obtained in [16], the number of edges of edge subsets E_{ij} for $2 \le i \le j \le 3$ is shown in Table 2.

Therefore, we get

$$\begin{aligned} EU(H) &= 3\sqrt{2}m_{2,2} + \sqrt{19}m_{2,3} + 3\sqrt{3}m_{3,3} \\ &= 3\sqrt{2}(a_2 + 6) + \sqrt{19}(4(h-1) - 2a_2) + 3\sqrt{3}(h - 1 + a_2) \\ &= (3\sqrt{3} + 4\sqrt{19})h + (5\sqrt{3} - 2\sqrt{19})a_2 + 9\sqrt{3} - 4\sqrt{19}. \end{aligned}$$

■

Theorem 2.7 *Let H be a hexagonal chain with h hexagons. Then*

$$EU(F) \le EU(H) \le EU(L_h),$$

where F is a fibonacene chain.

Proof. By applying Theorem 2.4 it is sufficient to prove the left inequality. If H is a hexagonal chain with h hexagons, then

$$a_2(H) \le h - 2, \tag{1}$$

and the equality holds if and only if H is a hexagonal chain such that $l_2(H) = 0$. That is H is a fibonacene chain [17]. For any fibonacene chain F, using theorem 2.6 we have

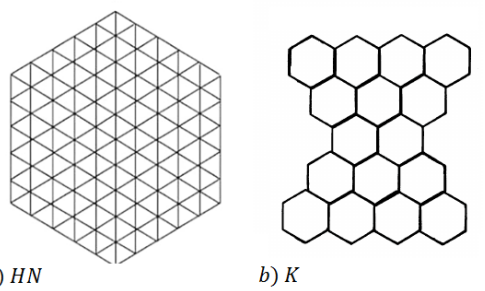
$$EU(F) = (8\sqrt{3} + 2\sqrt{19})h - \sqrt{3}.$$

Let Z be a fibonacene chain. Therefore, using Theorem 2.6, (1) and since $5\sqrt{3} - 2\sqrt{19} < 0$, we deduce that

$$EU(H) - EU(Z) = (5\sqrt{3} - 2\sqrt{19})[a_2 - (h-2)] \ge 0.$$

■

The hexagonal network is a major structural category where crystalline structures are defined using four axes: three mutually perpendicular axes at $120\hat{A}^\circ$ and a fourth axis perpendicular to the other three (see Figure 2 (a)). This system establishes a lattice that outlines the boundaries of an orderly arrangement of unit cells. Within these cells, atoms or molecular groups are represented by points connected by lines.



$a)\ HN$ $b)\ K$

Figure 2: a) A hexagonal network and b) Non-Kekulean Benzenoid Hydrocarbon.

Let HN be a graph of the hexagonal network. According to the structure of the graph HN, this graph contains $3n(n-1)+1$ vertices and $(9n-15)+6$ edges for $n \geq 3$. Table 3 shows the size of edge subsets E_{ij}.

Table 3: The cardinality of edge-partition sets of the hexagonal network HN.

Edge subsets	E_{34}	E_{36}	E_{44}	E_{46}	E_{66}
Cardinality	12	6	$6(n-3)$	$12(n-2)$	$9n^2-33n+30$

Theorem 2.8 *Let HN be a hexagonal network. Then*

$$EU(HN) = 12\sqrt{37} + 18\sqrt{7} + 24(n-2)\sqrt{19} + 6\sqrt{3}(9n^2-29n+18)\sqrt{3}.$$

Proof. According to Table 3 and the definition of the Euler Sombor index, we get

$$\begin{aligned} EU(HN) &= 12\sqrt{9+16+12} + 6\sqrt{9+36+18} \\ &\quad +6(n-3)\sqrt{16+16+16} + 12(n-2)\sqrt{16+36+24} \\ &\quad +(9n^2-33n+30)\sqrt{36+36+36} \\ &= 12\sqrt{37} + 18\sqrt{7} + 24(n-3)\sqrt{3} + 24(n-2)\sqrt{19} \\ &\quad +6(9n^2-33n+30)\sqrt{3}. \end{aligned}$$

By simplifying the above relationship, the result is obtained. ■

Finally, we investigate the graph of the Non-Kekulean Benzenoid Hydrocarbon, denoted by K and compute the Euler Sombor index of the graph K. According to the structure of the graph K shown in Figure 2 (b), this graph has $12n+1$ vertices and $17n+14$ edges where $n \geq 3$. Table 4 shows the number of the edges in subsets $E_{i,j}$.

Table 4: The cardinality of edge-partition sets of a non-Kekulean Benzenoid Hydrocarbon.

Edge subsets	E_{23}	E_{34}	E_{44}	E_{45}	E_{46}	E_{55}	E_{56}	E_{66}
Cardinality	8	8	8	4	$2n+4$	2	4	$11\mathrm{n}-16$

Theorem 2.9 *Let K be a Non-Kekulean Benzenoid Hydrocarbon. Then*

$$EU(K) = 4\sqrt{19}(n+4) + 2\sqrt{3}(41n-43) + 8\sqrt{37} + 4\sqrt{91} + 4\sqrt{61}.$$

Proof. According to Table 4, we have

$$\begin{aligned} EU(K) &= m_{2,3}\sqrt{19} + m_{3,4}\sqrt{37} + 4m_{4,4}\sqrt{3} + m_{4,5}\sqrt{61} \\ &+2m_{46}\sqrt{19} + 5m_{5,5}\sqrt{3} + m_{5,6}\sqrt{91} + 6m_{6,6}\sqrt{3} \\ &= 8\sqrt{19} + 8\sqrt{37} + 16n\sqrt{3} + 4\sqrt{61} + 2(2n+4)\sqrt{19} \\ &+10\sqrt{3} + 4\sqrt{91} + 6(11n-16)\sqrt{3} \\ &= 4\sqrt{19}(n+4) + 2\sqrt{3}(41n-43) + 8\sqrt{37} + 4\sqrt{91} + 4\sqrt{61}. \end{aligned}$$

■

3 CONCLUSION

Topological indices are powerful tools for describing and comparing molecular structures, playing a significant role in computational chemistry. In this paper, we delved into the Euler Sombor index, a novel degree-based topological index, and its application to hexagonal systems. We characterized the graphs that attain the minimum and maximum values of this index within the class of hexagonal systems. Additionally, we derived exact formulas for the Euler Sombor index of Hexagonal networks and Non-Kekulean Benzenoid Hydrocarbons. These findings contribute to a deeper understanding of the structural properties of these chemical graphs and provide valuable insights for future research in chemical graph theory.

4 REFERENCES

[1] I. Gutman, Geometric approach to degree-based topological indices: Sombor indices, MATCH Commun. Math. Comput. Chem, 86 (2021), 11-16.

[2] F. Movahedi, M. H. Akhbari, Degree-based topological indices of the molecular structure of hyaluronic acid-methotrexate conjugates in cancer treatment, Int. J. Quantum Chem, 123(12) (2023), p.e27106.

[3] H. Liu, I. Gutman, L. You, Y. Huang, Sombor index: Review of extremal results and bounds, J. Math. Chem, 66 (2022), 771-798.

[4] J. Rada, J.M. Rodr´ıguez, J.M. Sigarreta, Sombor index and elliptic Sombor index of benzenoid systems, Appl. Math. Comput, 475 (2024), Article ID: 128756.

[5] A.A.S. Ahmad Jamri, F. Movahedi, R. Hasni, R. Gobithaasan, M. H. Akhbari, Minimum Randić index of trees with fixed total domination number, Mathematics, 10(20) (2022), 3729.

[6] S. Bermudo, R. Hasni, F. Movahedi, J. E. Nápoles, The Geometric-Arithmetic index of trees with a given total domination number, Discret. Appl. Math, 345 (2024), 99-113.

[7] Z. Tang, Y. Li, H. Deng, The Euler Sombor index of a graph, Int. J. Quantum Chem, 124(9) (2024), p.e27387.

[8] B. Kirana, M.C. Shanmukha, A. Usha, On the Elliptic Sombor and Euler Sombor indices of Corona product of certain graphs, (2024), arXiv preprint arXiv:2406.15861.

[9] I. Gutman, B. Furtula, M.S. Oz, Geometric approach to vertexdegreebased topological indices-Elliptic Sombor index, theory and application, Int. J. Quantum Chem, 124(2) (2024), p.e27346.

[10] F. Movahedi, A. Karimi, Z. Samiei, Euler Sombor index of chemical graphs and its applications, 2024, submitted.

[11] H. Kanj, H. Iqbal, M. H. Aftab, H. Raza, K. Jebreen, M. I. Sowaity, Topological characterization of hexagonal network and non-kekulean benzenoid hydrocarbon, European Journal of Pure and Applied Mathematics, 16(4) (2023), 2187-2197.
[12] I. Gutman, S.J. Cyvin, Introduction to the Theory of Benzenoid Hydrocarbons, Springer, Berlin, 1989.
[13] R. Cruz, I. Gutman, J. Rada, Convex hexagonal systems and their topological indices, MATCH Commun. Math. Comput. Chem. 68 (2012) 97-108.
[14] J. Rada, Bounds for the randić index of catacondensed systems, Util. Math. 62 (2002) 155-162.
[15] J. Rada, O. Araujo, I. Gutman, Randić index of benzenoid systems and phenylenes, Croat. Chem. Acta 74 (2001) 225-235.
[16] I. Gutman, B. Furtula, K.C. Das, E. Milovanović, I. Milovanović (Eds.), Extremal Properties of Hexagonal Systems. Bounds in Chemical Graph Theory Mainstreams, Univ. Kragujevac, Kragujevac, 2017, 239-286.
[17] I. Gutman, S. Klavžar, Chemical graph theory of fibonacenes, MATCH Commun. Math. Comput. Chem. 55 (2006) 39-54.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Frame Extraction from Videos for Deepfake Detection using Machine Learning Approaches

K.C. Shilpa[1]
Department of AI & ML, PES Institute of Technology and Management, Shivamogga, 577204, India

R.P. Rajath[2], S.N. Shreya[3], R.H. Rakeen[4], A. Suchith[5]
Department of AI & ML, PES Institute of Technology and Management, Shivamogga, 577204, India

Abstract

The last few decades have seen a significant rise in Artificial Intelligence (AI) and Machine Learning (ML), promoting the development of deepfake technology. Deepfakes are synthetic media created using AI techniques, altering audio, images, and videos to appear authentic but are fabricated. Employing concepts like Generative Adversarial Networks (GANs), deepfake creation involves a competitive process where one model produces forgeries while another aims to identify them. Detecting deepfakes presents a significant challenge, prompting exploration into various methodologies. Convolutional Neural Networks (CNNs) stand as a prominent tool, with studies comparing different architectures such as DenseNet, VGGNet, ResNet, and custom CNNs. Additionally, autoencoders, particularly Variational Auto encoders, offer utility in reducing data dimensionality and editing facial features in images. Transfer learning, where pre-trained models like InceptionV3 are adapted for deepfake detection, and multi-model approaches combining CNNs with Long-Short Term Memory Networks (LSTMs) have shown promising results. Furthermore, novel techniques like CapsuleNets and ensemble methods, which combine multiple base models, are explored for their efficacy. CapsuleNets facilitate spatial inconsistency detection, while ensembling aims to enhance model robustness.

Keywords: Machine learning, deep fake, convolution nureal network, generative adversarial networks

1 Introduction

A deepfake is an AI-based technology that uses deep learning technology to create or alter audio, video, and images to make them appear real. More specifically, it usually requires a neural network that has been trained on vast data based on the target person's voice, facial expressions, and mannerisms [1]. Although deepfakes have limitless promising avenues in entertainment and education, it has major dangers issues. They will support misinformation and making non-consensual lewd content based on privacy violations, fraud and impersonation are supported [2]. Current research is ongoing into the development of effective detection methods and technologies that might mitigate such risks [3].

Deepfake technology is a product of the rapid development of artificial intelligence which can be traced back only a few years ago. Deepfake technology is whereby a person's likeness is reproduced to create movies or audio content that are difficult to differentiate from actual footage. However, this invention has been abused in several ways and has given rise to numerous ethical and legal issues [4]. Repeatedly and ironically, the absence of ethical standards has permitted people to create more harm than good using the fantastic tools available to them. Drawing on existing literature, the efficacy of the prevalent deepfake technology will be challenged by embracing an automated approach for detection and analysis. Using state-of-the-art

[1]speaker

technologies including computer vision, machine learning, and forensic analysis, the system aims to identify false media content accurately [5]. Made up of three broad components which are technical, legal, and ethical, this paper mitigate the proliferation of deepfake abuse and safeguard the purity of digital content.

1.1 Addressing the Growing Challenge of Deepfake Detection and Mitigation

The generation of deepfakes has raised some noteworthy concerns as they can be abused. These videos and audio recordings that are synthesized by an AI can as well be used to relay false information, alter public opinion, meddle with the electoral process, and create fake details that may incriminate certain people, more so the politicians. Even more, the issue is compounded by the availability of deepfake production tools that enable people of low-level technical expertise to generate credible fake media. It can be noted that the issue of deepfake detection is harder and harder with every passing day owing to the development of techniques used to create them. Present technologies that aid in the identification of also considering legal approaches do not support enough contemporary DeepFake technology which deals with artificial and real content merging. This begs the question of how to build a system capable of detecting deep fake content, limiting its distribution, and protecting the integrity of the media in a reality where its security is increasingly threatened by manipulative schemes [6].

1.2 Developing an Adaptive ML-based Framework

The major goals of this paper are as follows:

- **Detect deepfakes in video content:** Create a solid mitigation measure that seeks to develop technologies for the verification of manipulated media with an emphasis on video forgery detection especially face forgery [7].
- **Face extraction and forensic analysis:** Methodically proceed with the extraction of faces from the video every second for one frame and study the forensic content for any possible manipulation of the videos.
- **Machine learning uses:** Formulate an optimized model to separate real and fabricated image or video media utilizing machine learning especially deep learning techniques such as CNNs [8].
- **Ensure adaptability:** Develop a system that can be modified and adapted faster than the advancement of new, complex deepfake procedures in the near future [9].
- **Mitigate misinformation:** Help in combating misinformation by developing a tool to easily detect such media for use in the various sectors including the media, government, and law enforcement.

1.3 Scope of the Paper

The scope of this paper covers the following:

- **Data Collection and Preprocessing:** Textual information will be obtained from different databases such as newspapers, ethnographic interviews, and field notes. The data was cleaned by scanning through the video clips, locating the facial features, and cropping them out, changing the angle of these faces, and so on to enhance the data.
- **Model Training and Validation:** A CNN model will be trained using the processed data which aims at discrimination of the real and the fake faces. Should the efficacy of the model be established using the so collected data [10].
- **Integration of Temporal Consistency Checks:** The system will incorporate consistency in time checks which are annotations that search for motion dynamics in order to circumvent the deceptions of deepfake synthesis through checking frames in a video [11, 12].

- **Implementation of Real-Time Detection:** The first system will be prohibiting the analysis of video content, aiming at only post-processing video content for the deepfake identification, whereas subsequent releases shall focus on building the detection systems that will be able to process the content live as it is streamed [13–15].
- **User Interface Development:** Social media platforms such as a phone application that will enable every user including institutions and even law enforcement agencies to upload videos for deepfake detection will be developed [16, 17].

1.4 Generation Process of Deepfakes

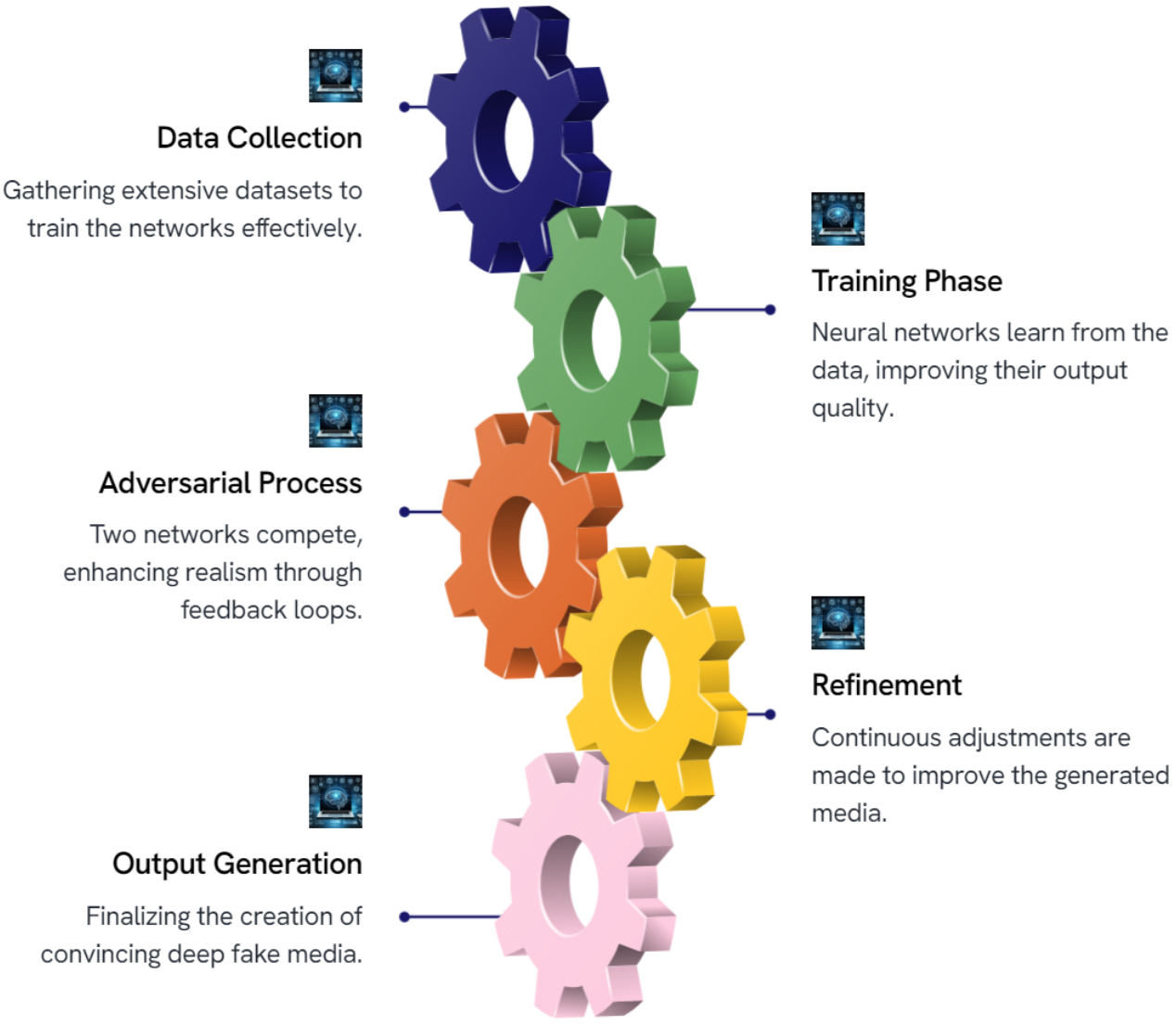


Figure 1: Exploring the Role of GANs in Creating Realistic Media

The figure 1 depicts the step-by-step procedure in the making of a deepfake. It begins with **Data Collection** in which an enormous volume of the datasets are collected to train the neural networks [18–21]. Then is the **Training Phase** where the end defining is done based on the data available allowing the networks to decrease the errors in the quality of output. The **Adversarial Process** features two competing networks enhancing realism-usually in Generative Adversarial Networks (GANs)-through iterative processes.

The next one is the **Refinement Stage** where the output media images are edited and modified over a period to enhance quality. To wrap it up is the **Output Generation** where the production is deepfake as the final visual is produced aiming for the highest realistic quality. Hence each of these steps plays a big role towards the development of photorealistic and realistic deepfakes [22, 23].

2 Methodology

1. **Data Preprocessing**: Preprocessing includes such simple actions as cutting the faces from the video frames, which is the first step. To achieve homogeneity across the dataset, video frames are captured via OpenCV at constant intervals of one frame per second. Thereafter, the Multi-Task Cascaded Convolutional Networks (MTCNN) is used to locate the faces on these frames, where the faces are then scaled and graduated to the same size. In this section, the methods of augmentation that include but are not limited to image flipping, rotation and brightness changes are in order to make the training data more interesting and increase representative ability of the model [24, 25].

2. **Feature Extraction**: The face images, which have been preprocessed, are passed into the CNN model, where the specific features forensic manipulations are targeted. It encompasses the study of the texture, lighting editing, twisted edges and others that reveal a sign of deepfake media. Convolutional layers of the model via multiple filters categorically learn how to discriminate between real and fake images [26, 27].

3. **Model Training and Validation**: The dataset includes three subsets namely training dataset, validation dataset and test dataset. The CNN model is trained on the training dataset where the model is able to differentiate between real and fake faces based on features extracted. The validation set is basically employed for tuning the model and its parameters in such a way that one does not over fit the model to the training data. Once the model has been still improved on, the test set is applied to assess the deepfake detection in terms of accuracy, precision, and recall [28–31].

4. **Temporal Consistency Analysis**: The other approach that serves to increase the detection accuracy is temporal consistency analysis that works by detecting sudden changes between two consecutive video frames that are unexpected [32–36]. There are many deepfake videos which have a lot of artifacts such as light and shadows and facial features change from frame to frame, and this step helps to rectify the model from such changes making the model more accurate in fake media detection [37].

2.1 Frame Extraction through MTCNN Algorithm

The figure 2 provides details of the first phase architecture of the deep fake detection, which is based on video frames and how the dataset is created [38,39]. The first step in the process is Video Frame Extraction and involves processing video files contained in the "Deepfake Detection Challenge" dataset. The videos include both real face and face simulated contents. Each of the frames is extracted and saved in a specific folder that is the main source of data. Then the Resizing Frames step makes sure that every frame, both the initial and any further processed, have the same size and resolution which is important to maintain the consistency of the model training. Where the facial regions are removed from the standard frames resulting in cropped images which are targeted more on the region of interest for deep fake detection.

2.2 2024 Market Analysis and Applications

The figure 3 shows the deepfake applications market analysis for the year 2024 along the vertical line and across different verticals along the horizontal line. Entertainment has the highest adoption with 35% first place, which is followed by Fraud Detection second place at 25% that gives insight into its application in combating deceit. Cyber security takes over 20%, which underscores the application of the technology in the solution of security complications. Advertising comes in at 15% whereby it has been established that this technology is used to develop interactive adverts and Healthcare is at a dismal 5%, suggesting that the use of this technology in the medical sector is still developing and not widely embraced. Each sphere,

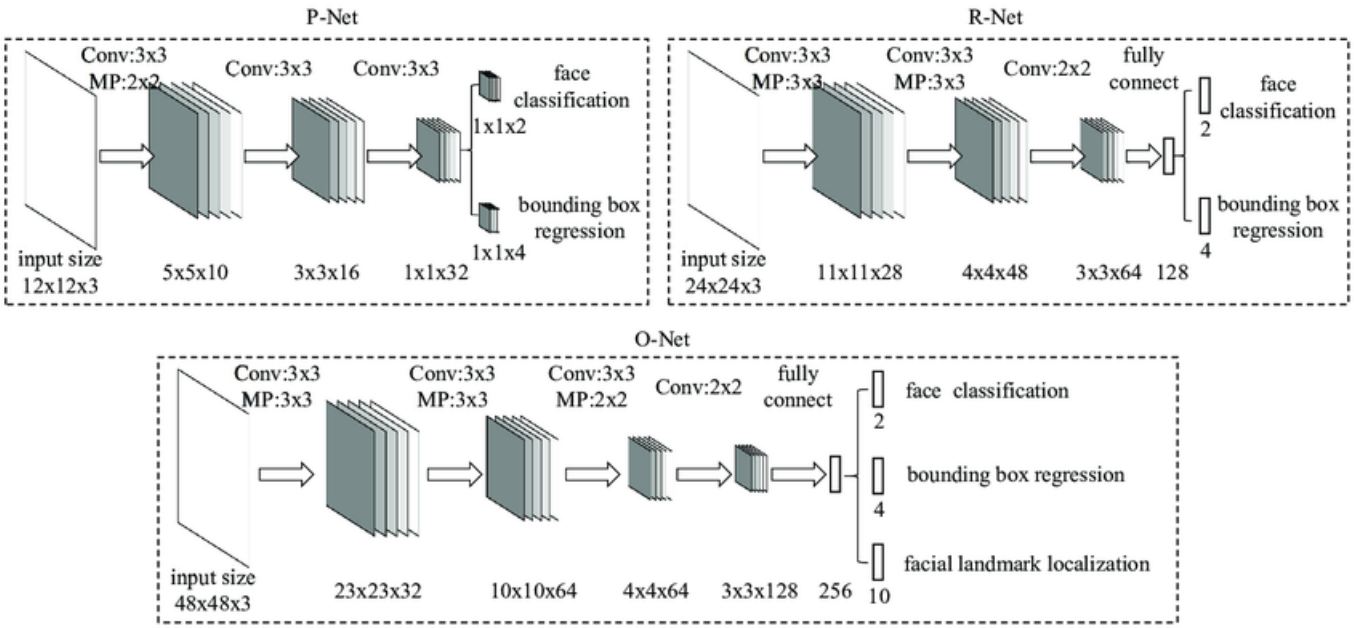


Figure 2: MTCNN

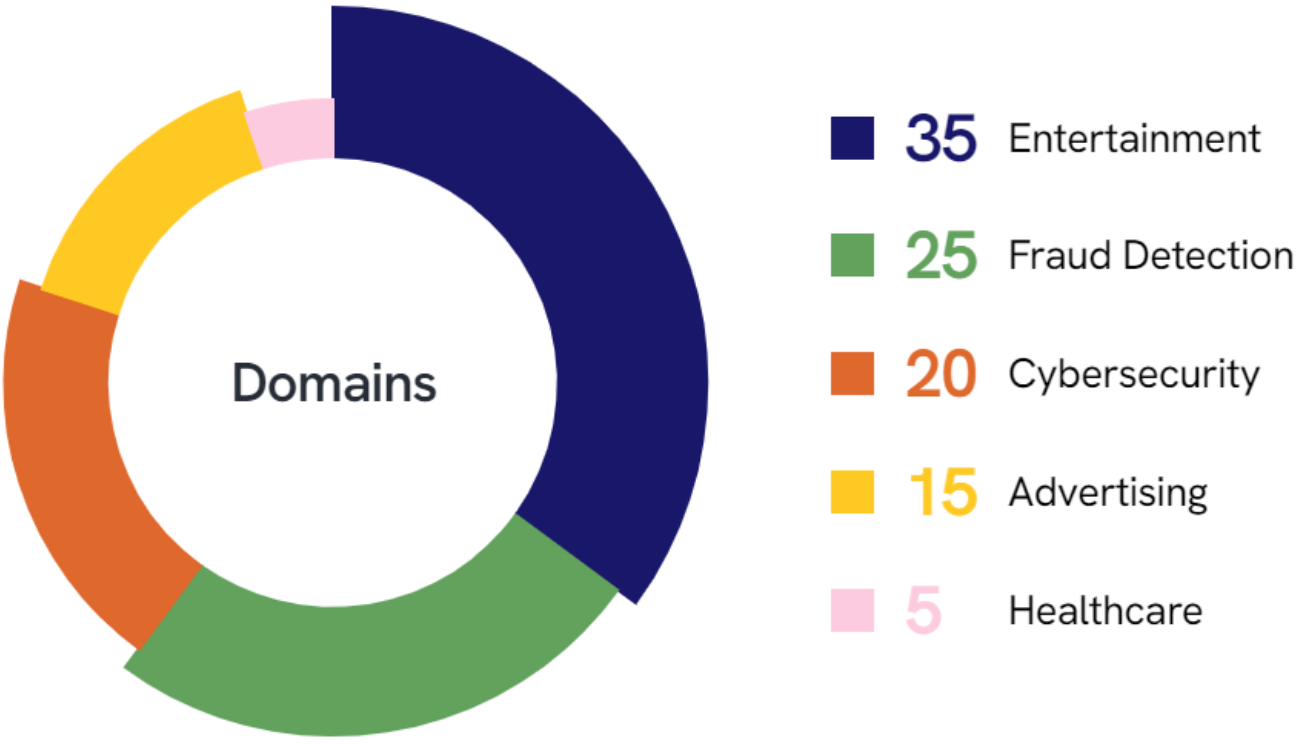


Figure 3: Market Research Report 2024

in turn, showcases different examples of deepfake technology commercialization and explains the diverse market scope of the deepfake technology [40, 41].

3 Results and Discussion

Technology for the detection of deepfake is key to everybody in the contemporary world where content can be synthesized and used to commit fraud [42–44]. This paper provides evidence that machine learning as well as computer vision techniques can be employed for the purpose of deepfake detection [45–47].

By effective preprocessing, forensic detection and provision of temporal consistency checks, this system gave satisfactory results in terms of deepfakes detection [48–53]. However, deepfake technology is constantly evolving, necessitating continuous improvements to detection techniques. Future work must focus on keeping detection systems up-to-date with the latest developments in deepfake generation while ensuring the system remains computationally efficient.

3.1 2024 Market Analysis and Applications

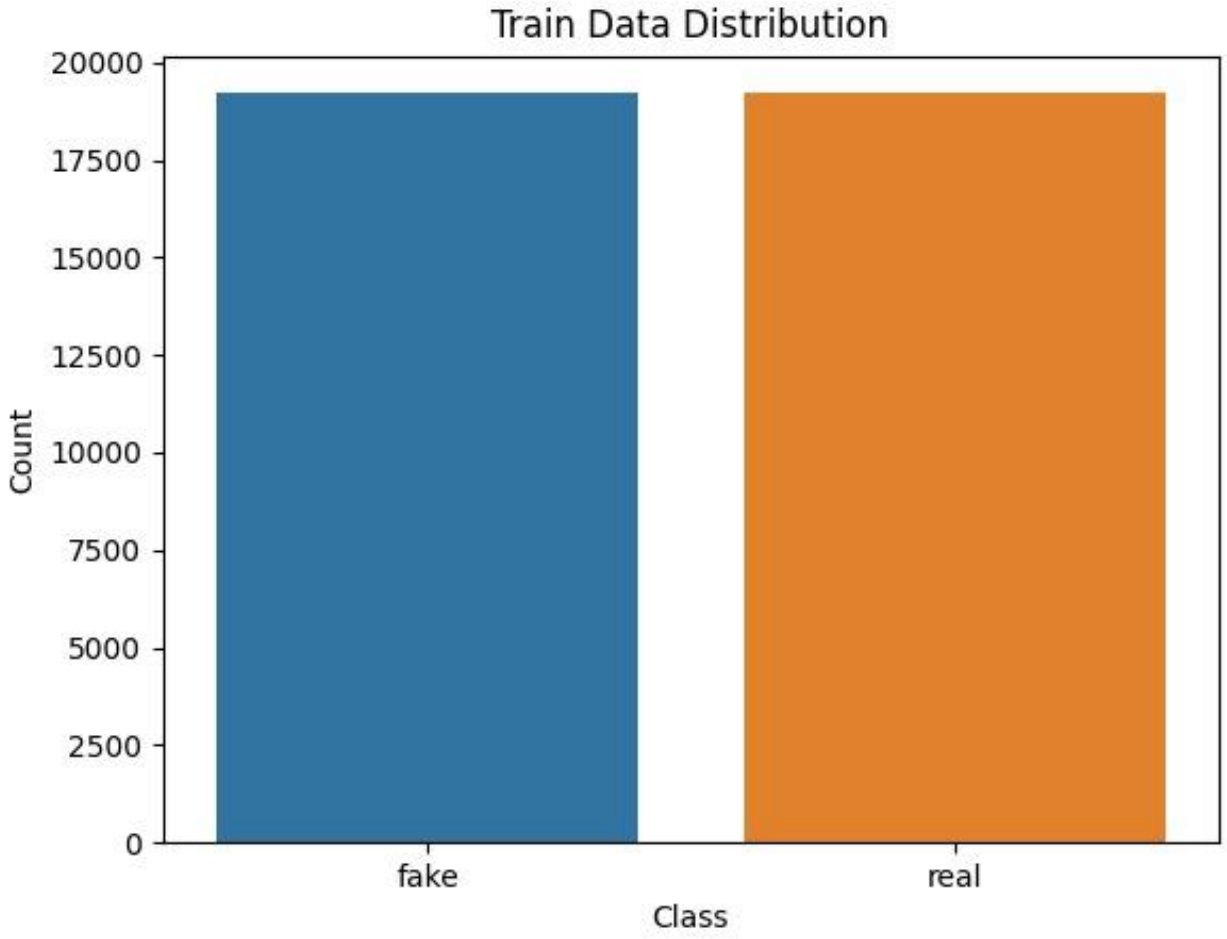


Figure 4: Train Data Distribution

Conclusion

A deepfake is an AI-based technology that uses deep learning technology to create or alter audio, video, and images to make them appear real. Detecting deepfakes presents a significant challenge, prompting exploration into various methodologies. This work uses the DenseNet, VGGNet, ResNet, and custom CNNs. Furthermore, novel techniques like CapsuleNets and ensemble methods, which combine multiple

base models, are explored for their efficacy. By effective preprocessing, forensic detection and provision of temporal consistency checks, this system gave satisfactory results in terms of deepfakes detection.

References

[1] Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. *IEEE Access*, 10, 25494-25513.

[2] Wubet, W. M. (2020). The deepfake challenges and deepfake video detection. *Int. J. Innov. Technol. Explor. Eng*, 9.

[3] Chadha, A., Kumar, V., Kashyap, S., & Gupta, M. (2021). Deepfake: an overview. In Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020 (pp. 557-566). Springer Singapore.

[4] Singh, A., Saimbhi, A. S., Singh, N., & Mittal, M. (2020). DeepFake video detection: a time-distributed approach. *SN Comput. Sci*, 1, 212.

[5] Katarya, R., & Lal, A. (2020, October). A study on combating emerging threat of deepfake weaponization. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 485-490). IEEE.

[6] Akhtar, Z. (2023). Deepfakes Generation and Detection: A Short Survey. *Journal of Imaging*, 9(1), 18.

[7] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion*, 64, 131-148.

[8] Shad, H. S., Rizvee, M. M., Roza, N. T., Hoq, S. M., Monirujjaman Khan, M., & Singh, Bourouis S. (2021). Comparative analysis of deepfake image detection method using convolutional neural network. *Comput. Intell. Neurosci.*, 2021.

[9] Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Comput. Surv.*, 54(1), 1-41.

[10] Kharbat, F. F., Elamsy, T., Mahmoud, A., & Abdullah, R. (2019, November). Image feature detectors for deepfake video detection. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-4). IEEE.

[11] Guera, D., & Delp, E. J. (2018, November). Deepfake video detection using recurrent neural networks. In 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (pp. 1-6). IEEE.

[12] Sabir, E., Cheng, J., Jaiswal, A., AbdAlmageed, W., Masi, I., & Natarajan, P. (2019). Recurrent convolutional strategies for face manipulation detection in videos. *Interfaces (GUI)*, 3(1), 80-87.

[13] Liang, Y., Wang, M., Jin, Y., Pan, S., & Liu, Y. (2023). Hierarchical Supervisions with Two-stream Network for Deepfake Detection. *Pattern Recognit. Lett.*.

[14] Suratkar, S., Kazi, F. (2023). Deep fake video detection using transfer learning approach. *Arabian J. Sci. Eng.*, 48(8), 9727-9737.

[15] Wang, Y., Wang, J., Liang, Y., Chen, X., & Guo, Y. (2023). Deepfake Video Detection via Facial Action Dependencies Estimation.

[16] Gowrisankar, B., & Thing, V. L. (2024). An adversarial attack approach for eXplainable AI evaluation on deepfake detection models. *Computers Security*, 139, 103684.

[17] Yu, Z., Cai, R., Li, Z., Yang, W., Shi, J., & Kot, A. C. (2024). Benchmarking joint face spoofing and forgery detection with visual and physiological cues. *IEEE Trans. Dependable Secure Comput.*.

[18] Zhang, T., Deng, L., Zhang, L., & Dang, X. (2020, August). Deep learning in face synthesis: A survey on deepfakes. In 2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET) (pp. 67-70). IEEE.

[19] Guarnera, L., Giudice, O., Guarnera, F., Ortis, A., Puglisi, G., Paratore, A., ... & Battiato, S. (2022). The face deepfake detection challenge. *Journal of Imaging*, 8(10), 263.

[20] Fischer, E. M. Formulation of the Variational Autoencoder and Evidence Lower Bound and an Application to the MNIST Dataset.

[21] Zhao, Y., & Linderman, S. (2023, July). Revisiting structured variational autoencoders. In International Conference on Machine Learning (pp. 42046-42057). PMLR.

[22] Makhzani, A., Shlens, J., Jaitly, N., Goodfellow, I., & Frey, B. (2015). Adversarial autoencoders. arXiv preprint arXiv:1511.05644.

[23] Li, D., Zhang, M., Chen, W., & Feng, G. (2018, August). Facial attribute editing by latent space adversarial variational autoencoders. In 2018 24th International Conference on Pattern Recognition (ICPR) (pp. 1337-1342). IEEE.

[24] Bondi, L., Cannas, E. D., Bestagini, P., & Tubaro, S. (2020, December). Training strategies and data augmentations in CNN-based deepfake video detection. In 2020 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.

[25] Waqas, N., Safie, S. I., Kadir, K. A., Khan, S., & Khel, M. H. K. (2022). DEEPFAKE image synthesis for data augmentation. *IEEE Access*, 10, 80847-80857.

[26] Caldelli, R., Galteri, L., Amerini, I., & Del Bimbo, A. (2021). Optical Flow based CNN for detection of unlearnt deepfake manipulations. *Pattern Recognition Letters*, 146, 31-37.

[27] Ramadhani, K. N., Munir, R., & Utama, N. P. (2024). Improving Video Vision Transformer for Deepfake Video Detection using Facial Landmark, Depthwise Separable Convolution and Self Attention. *IEEE Access*.

[28] Bonettini, N., Cannas, E. D., Mandelli, S., Bondi, L., Bestagini, P., & Tubaro, S. (2021, January). Video face manipulation detection through ensemble of CNNs. In 2020 25th International Conference on Pattern Recognition (ICPR) (pp. 5012-5019). IEEE.

[29] Kohli, A., & Gupta, A. (2021). Detecting deepfake, faceswap and face2face facial forgeries using frequency CNN. *Multimedia Tools Appl.*, 80, 18461-18478.

[30] Li, C., Huang, Z., Paudel, D. P., Wang, Y., Shahbazi, M., Hong, X., & Van Gool, L. (2023). A continual deepfake detection benchmark: Dataset, methods, and essentials. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (pp. 1339-1349).

[31] Guera, D., & Delp, E. J. (2018, November). Deepfake video detection using recurrent neural networks. In 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (pp. 1-6). IEEE.

[32] Liu, J., Zhu, K., Lu, W., Luo, X., & Zhao, X. (2021). A lightweight 3D convolutional neural network for deepfake detection. *Int. J. Intell. Syst.*, 36(5), 2313-2329.

[33] Prashanth, K., & Kundu, H. (2021). An adaptive neural network approach for deepfake detection. *J. Ambient Intell. Humaniz. Comput.*, 12, 5437-5445.

[34] Remya Revi, K., Vidya, K. R., & Wilscy, M. (2021). Detection of Deepfake Images Created Using Generative Adversarial Networks: A Review. In Second International Conference on Networks and Advances in Computational Technologies: NetACT 19 (pp. 25-35). Springer International Publishing.

[35] Ganguly, S., Mohiuddin, S., Malakar, S., Cuevas, E., & Sarkar, R. (2022). Visual attention-based deepfake video forgery detection. *Pattern Anal. Appl.*, 25(4), 981-992.

[36] Hooda, A., Mangaokar, N., Feng, R., Fawaz, K., Jha, S., & Prakash, A. (2024). D4: Detection of Adversarial Diffusion Deepfakes Using Disjoint Ensembles. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (pp. 3812-3822).

[37] Mehra, A. (2020). Deepfake detection using capsule networks with long short-term memory networks (Master's thesis, University of Twente).

[38] Ganiyusufoglu, I., Ngo, L. M., Savov, N., Karaoglu, S., & Gevers, T. (2020). Spatio-temporal features for generalized detection of deepfake videos. arXiv preprint arXiv:2010.11844.

[39] Walia, S., Kumar, K., & Kumar, M. (2023). Unveiling digital image forgeries using Markov based quaternions in frequency domain and fusion of machine learning algorithms. *Multimedia Tools Appl.*, 82(3), 4517-4532.

[40] Xiao, S., Lan, G., Yang, J., Lu, W., Meng, Q., & Gao, X. (2023). MCSGAN: A Different Understanding for Generalization of Deep Forgery Detection. *IEEE Trans. Multimedia*.

[41] Campbell, C., Plangger, K., Sands, S., Kietzmann, J., & Bates, K. (2022). How deepfakes and artificial intelligence could reshape the advertising industry: The coming reality of AI fakes and their potential impact on consumer behavior. *J. Advert. Res.*, 62(3), 241-251.

[42] Leyva, R., Sanchez, V., Epiphaniou, G., & Maple, C. (2024). Detecting Face Synthesis Using a Concealed Fusion Model. arXiv preprint arXiv:2401.04257.

[43] Nawaz, M., Javed, A., & Irtaza, A. (2023). ResNet-Swish-Dense54: a deep learning approach for deepfakes detection. *The Visual Computer*, 39(12), 6323-6344.

[44] Killi, C. B. R., Balakrishnan, N., & Rao, C. S. (2023). Deep Fake Image Classification Using VGG-19 Model. *Ingénierie des Systèmes d'Information*, 28(2).

[45] Han, X. Y., & Lewis, A. S. (2020). Disk matrices and the proximal mapping for the numerical radius. arXiv preprint arXiv:2004.14542.

[46] Coccomini, D., Caldelli, R., Falchi, F., & Gennaro, C. (2023). On the Generalization of Deep Learning Models in Video Deepfake Detection. *Journal of Imaging*, undefined.

[47] Prasad, S. S., et al. (2022). Human vs. Automatic Detection of Deepfake Videos Over Noisy Channels. In 2022 IEEE International Conference on Multimedia and Expo (ICME). IEEE.

[48] Lin, Y., et al. (2020). Exploring generalization capability for video forgery and detection based on generative adversarial network. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE.

[49] Yang, J., Li, A., Xiao, S., Lu, W., & Gao, X. (2021). MTD-Net: Learning to detect deepfakes images by multi-scale texture difference. *IEEE Trans. Inf. Forensics Security*, 16, 4234-4245.

[50] Xu, Y., Zhang, D. D., & Sun, C. (2023, June). Frequency domain deepfake detection based on two-stream neural network. In Fourteenth International Conference on Graphics and Image Processing (ICGIP 2022) (Vol. 12705, pp. 910-918). SPIE.

[51] BR, S. R., Pareek, P. K., Bharathi, S., & Geetha, G. (2023, February). Deepfake Video Detection System Using Deep Neural Networks. In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-6). IEEE.

[52] Hu, Y., Zhang, X., & Ren, J. (2023). Automatic detection of deepfake videos using convolutional neural networks in frequency domain. *Multimedia Tools Appl.*, 82(2), 1827-1847.

[53] Heidari, A., Jafari Navimipour, N., Dag, H., & Unal, M. (2024). Deepfake detection using deep learning methods: A systematic and comprehensive review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 14(2), e1520.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

A Study on various degree based topological indices for anti-hypertension, anti-congestive heart failure, and anti-heart attack drug : Lisinopril

M.C. Shanmukha[1]
Department of Mathematics, PES Institute of Technology and Management, Shivamogga, 577204, India

A. Usha
Department of Mathematics, Alliance School of Applied Mathematics, Alliance University, Bangalore, 562106, India

K.C. Shilpa
Department of AI & ML, PES Institute of Technology and Management, Shivamogga, 577204, India

Abstract

The most significant chronic health problem is hypertension. To manage hypertension, angiotensin-converting enzyme (ACE) inhibitor is used which is the drug named Lisinopril. This is used even in treating heart failure. Because of its efficacy, it is used in the treatment of cardiovascular related problems apart from hypertension. To administer Lisinopril, regular monitoring of blood pressure, level of potassium and the kidney function are to be taken care of. A mathematical measure that constitutes the inclusive structure of a molecule is called a topological index/graph-theoretic index. In the studies of quantitative structure-activity relationship (QSAR) and quantitative structure-property relationship (QSPR), the topological indices are utilized to hypothesis the physical features related to the bioactivities and chemical reactivities in certain molecules. In this article, Lisinopril drug is studied by computing various degree-based topological indices such as Forgotten index, Sombor index, reduced Sombor index, average Sombor index, elliptic Sombor index and Euler Sombor index.

Keywords: Lisinopril, topological index, Sombor indices, molecular graph of Lisinopril
Mathematics Subject Classification [2010]: 05C07, 05C10, 05C90

1 Introduction

The most common chronic health problem is hypertension which is estimated to be affected by one billion people. This number is estimated to increase by 60% by 2025. Hypertension is caused when systolic blood pressure is 140mmHg or more, according to World Health Organization. It may occur as isolated systolic or diastolic hypertension which can occur in the large arteries due to aging.

High blood pressure is the primary cause of hypertension in most of the cases. Other patients develop hypertension due to the disease of other organs and is referred to as secondary hypertension. The values of blood pressure estimate the severity of hypertension. A potent ACE inhibitor belonging to the third generation of ACE inhibitors is Lisinopril [1, 2]. It is administered to patients of hypertension and heart failure and diabetic nephropathy prophylaxis. 5 institutes related to health in Bosnia and Herzegovina evaluated patients suffering from hypertension in which Lisinopril was prescribed. The study included the dosage of medicine based on the mean blood pressure values in relation to gender, and age groups.

[1]speaker

An angiotensin-converting enzyme (ACE) inhibitor used for the management of hypertension and heart failure in clinical practice is Lisinopril. The first-line treatment which was introduced in the 1990s due to its safety profile, efficacy and prevention of cardiovascular events is Lisinopril [3]. Conversion of angiotensin I to a vasoconstrictor (angiotensin II) is done by Lisinopril. It helps manage hypertension and helps reduce the workload on the heart, benefitting the patients with heart failure.

Managing blood pressure can remarkably reduce the risk of heart attack, stroke and other problems related to Kidney. Lisinopril has improved the symptoms of heart failure and myocardial infarction by prolonging survival in patient. It could reduce glomerular pressure and slows down the progression of kidney ailments in diabetic patients. The common dosages range from 2.5 mg to 40 mg in which the hypertension starting dose is 10 mg once every day. The dosage can be adjusted depending on the blood pressure reading and the response from the patient. Common side effects include headache, dizziness, fatigue, and cough while serious side effects include angioedema which is caused due to the swelling of the deeper layers of the skin, renal impairment and hyperkalaemia. The efficacy and favourable profile of side effects of Lisinopril has established as a primary and sole medication for hypertension and heart failure [4]. Educating the patients continuously about the readings and its effects are essential to ensure best therapeutic outcomes to avoid potential risks associated with treatment.

Studies of American Heart Association hypertension in association with the 2017 American College of Cardiology guidelines estimated that 45% adults of US have hypertension. Angiotensin was considered as the first line therapy and most of the hypertension patients use ACEs, giving a greater response to the therapeutic use.

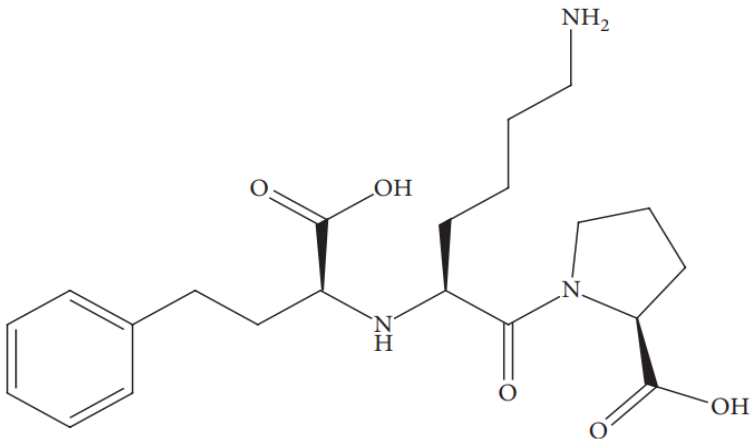


Figure 1: Molecular structure of Lisinopril.

To model a chemical compound and study the chemical phenomenon, a specialized branch of graph theory namely, chemical graph theory is applied. The chemical properties and the behaviour of molecular structures are analysed using topological indices. These indices play a significant role in graph theory thereby providing information about the chemical compound under the study [5–7].

Let G=(V, E) is a simple graph with V as vertex set and E as edge set. For a vertex u belonging to V, d_u indicates the degree of the vertex u [8–10]. Ivan Gutman in 2021, introduced a new addition to the tools in the field of chemical graph theory, namely Sombor index. Since its introduction, various studies have been conducted on this index and subsequently various versions of Sombor index are defined. In this work, the molecular structure of Lisinopril (Figure 1) is modelled as molecular graph for which 6 vertex degree-based topological indices are computed.

The considered degree-based indices such as Forgotten index, Sombor index, reduced Sombor index, average Sombor index, elliptic Sombor index and Euler Sombor index [11–15] are defined as follows

$$F(G) = \sum_{uv \in E(G)} (d_u)^2 + (d_v)^2,$$
$$SO(G) = \sum_{uv \in E(G)} \sqrt{(d_u)^2 + (d_v)^2},$$
$$SO_{Red}(G) = \sum_{uv \in E(G)} \sqrt{(d_u - 1)^2 + (d_v - 1)^2},$$
$$SO_{Avg}(G) = \sum_{uv \in E(G)} \sqrt{(d_u - \frac{2m}{n})^2 + (d_v - \frac{2m}{n})^2},$$
$$ESO(G) = \sum_{uv \in E(G)} (d_u + d_v)(\sqrt{(d_u)^2 + (d_v)^2}),$$
$$EU(G) = \sum_{uv \in E(G)} \sqrt{(d_u)^2 + (d_v)^2 + d_u d_v}.$$

2 Methodology

Initially, the molecular structure of Lisinopril is modelled as molecular graph and vertex and edge partitions are determined. The various degree-based topological indices are computed for the above said molecular graph. In this procedure, the methods used are vertex partition, edge partition and combinatorial computing.

3 Results for molecular graph of Lisinopril

From Figure 2, it is observed that, in general $|V(G)| = 29 = n$ and $|E(G)| = 30 = m$. The details of degrees of vertices and their edges are tabulated in Table 1 for the molecular graph of Lisinopril.

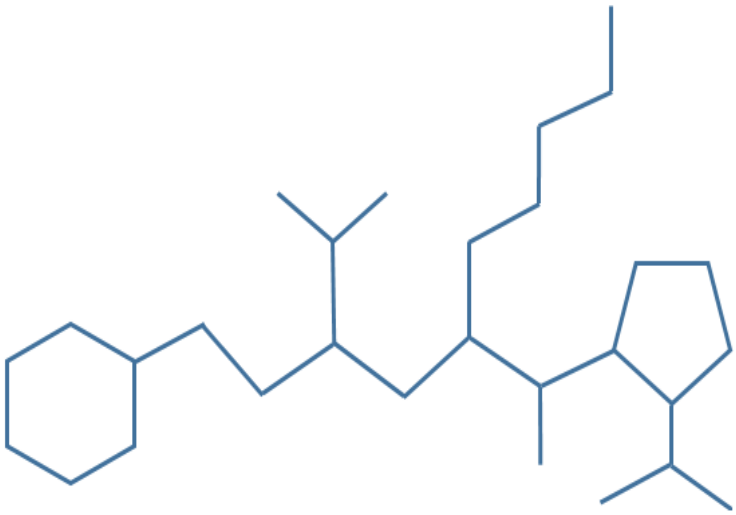


Figure 2: The molecular graph of Lisinopril.

Table 1: The edge partition of molecular graph of Lisinopril

(d_u, d_v) $where$ $uv \in E(G)$	$No.$ of $edges$
(1,2)	1
(1,3)	5
(2,2)	10
(2,3)	9
(3,3)	5

Theorem 3.1. *Consider a molecular graph G for Lisinopril, then*

$$\begin{aligned} F(G) &= \sum_{uv \in E(G)} (d_u)^2 + (d_v)^2 \\ &= 1\left\{(1)^2 + (2)^2\right\} + 5\left\{(1)^2 + (3)^2\right\} + 10\left\{(2)^2 + (2)^2\right\} + 9\left\{(2)^2 + (3)^2\right\} + 5\left\{(3)^2 + (3)^2\right\} \\ &= 1(5) + 5(10) + 10(8) + 9(13) + 5(18) \\ &= 342. \end{aligned}$$

Theorem 3.2. *Consider a molecular graph G for Lisinopril, then*

$$\begin{aligned} SO(G) &= \sum_{uv \in E(G)} \sqrt{(d_u)^2 + (d_v)^2} \\ &= 1\sqrt{\{(1)^2 + (2)^2\}} + 5\sqrt{\{(1)^2 + (3)^2\}} + 10\sqrt{\{(2)^2 + (2)^2\}} + 9\sqrt{\{(2)^2 + (3)^2\}} + 5\sqrt{\{(3)^2 + (3)^2\}} \\ &= 1(\sqrt{5}) + 5(\sqrt{10}) + 10(\sqrt{8}) + 9(\sqrt{13}) + 5(\sqrt{18}) \\ &= 99.995. \end{aligned}$$

Theorem 3.3. *Consider a molecular graph G for Lisinopril, then*

$$\begin{aligned} SO_{Red}(G) &= \sum_{uv \in E(G)} \sqrt{(d_u - 1)^2 + (d_v - 1)^2} \\ &= 1(\sqrt{1}) + 5(\sqrt{4}) + 10(\sqrt{2}) + 9(\sqrt{5}) + 5(\sqrt{8}) \\ &= 63.409. \end{aligned}$$

Theorem 3.4. *Consider a molecular graph G for Lisinopril, then*

$$\begin{aligned} SO_{Avg}(G) &= \sum_{uv \in E(G)} \sqrt{(d_u - \frac{2m}{n})^2 + (d_v - \frac{2m}{n})^2} \\ &= 1(1.071) + 5(1.417) + 10(0.097) + 9(0.933) + 5(1.317) \\ &= 24.113. \end{aligned}$$

Theorem 3.5. *Consider a molecular graph G for Lisinopril, then*

$$\begin{aligned} ESO(G) &= \sum_{uv \in E(G)} (d_u + d_v)(\sqrt{(d_u)^2 + (d_v)^2}) \\ &= 1(6.708) + 5(12.649) + 10(11.313) + 9(18.028) + 5(12.358) \\ &= 407.125. \end{aligned}$$

Theorem 3.6. *Consider a molecular graph G for Lisinopril, then*

$$\begin{aligned} EU(G) &= \sum_{uv \in E(G)} \sqrt{(d_u)^2 + (d_v)^2 + d_u d_v} \\ &= 1(2.646) + 5(3.605) + 10(3.464) + 9(4.36) + 5(5.196) \\ &= 120.531. \end{aligned}$$

4 Comparisons

Table 2: Numerical representation of the computed indices of Lisinopril

$F(G)$	$SO(G)$	$SO_{Red}(G)$	$SO_{Avg}(G)$	$ESO(G)$	$EU(G)$
342	99.995	63.409	24.113	407.125	120.531

Conclusion

This study is focussed on computing various degree based topological indices such as Forgotten index, Sombor index, reduced Sombor index, average Sombor index, elliptic Sombor index and Euler Sombor index of the anti-hypertension, anti-congestive heart failure, and anti-heart attack drug Lisinopril. Topological indices play a significant role in understanding and extracting the data about a chemical compound. This study may be useful for research carried on Lisinopril by chemists and pharmacists.

References

[1] Lancaster, S. G., & Todd, P. A. (1988). Lisinopril: a preliminary review of its pharmacodynamic and pharmacokinetic properties, and therapeutic use in hypertension and congestive heart failure. Drugs, 35, 646-669.

[2] Shionoiri, H. (1993). Pharmacokinetic drug interactions with ACE inhibitors. Clinical pharmacokinetics, 25, 20-58.

[3] De Souza, M. C., Diniz, L. F., Franco, C. H., & Diniz, R. (2018). Synthesis and crystalline structure of zinc complexes with antihypertensive drug lisinopril. Journal of Chemistry, 2018(1), 8910242.

[4] Simpson, K., & Jarvis, B. (2000). Lisinopril: a review of its use in congestive heart failure. Drugs, 59, 1149-1167.

[5] Trinajstic, N. (2018). Chemical graph theory. CRC press.

[6] Bonchev, D. (2018). Chemical graph theory: introduction and fundamentals. Routledge.

[7] Gutman, I. (2013). Degree-based topological indices. Croatica chemica acta, 86(4), 351-361.

[8] Imran, M., Farahani, M. R., Cancan, M., Alaeiyan, M., & Akgül, A. (2024). On topological indices of certain families of graphs. Physica Scripta.

[9] Gao, W., Siddiqui, M. K., Imran, M., Jamil, M. K., & Farahani, M. R. (2016). Forgotten topological index of chemical structure in drugs. Saudi pharmaceutical journal, 24(3), 258-264.

[10] Farahani, M. R. (2012). Some connectivity indices and Zagreb index of polyhex nanotubes. Acta Chim. Slov, 59(4), 779-783.

[11] B. Furtula and I. Gutman, A Forgotten Topological Index, Journal of Mathematical Chemistry, 53(2015), 1184-1190.

[12] Gutman, I., Furtula, B., & Elphick, C. (2014). Three new/old vertex-degree-based topological indices. MATCH communications in mathematical and in computer chemistry.

[13] Gutman, I., Furtula, B., & Oz, M. S. (2024). Geometric approach to vertex-degree-based topological indices–Elliptic Sombor index, theory and application. International Journal of Quantum Chemistry, 124(2), e27346.

[14] Ivan, G. (2024). Relating Sombor and Euler indices. Vojnotehnički glasnik, 72(1), 1-12.

[15] Shanmukha, M. C., Usha, A., Kulli, V. R., & Shilpa, K. C. (2024). Chemical applicability and curvilinear regression models of vertex-degree-based topological index: Elliptic Sombor index. International Journal of Quantum Chemistry, 124(9), e27376.

نقشه راهی جهت انعطاف‌پذیری امنیت سایبری برای افزایش تداوم کسب و کار

مریم صادقی[۱*]، مرتضی قائدی بارده[۲]

۱- دانشجوی دکتری، گروه مدیریت، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۲- دانشجوی کارشناسی ارشد، دانشکده فنی مهندسی، دانشگاه قم، قم، ایران.

چکیده

این مطالعه یک نقشه راه انعطاف‌پذیری امنیت سایبری را ارائه می‌دهد که برای تقویت دفاع سازمانی در برابر چشم انداز در حال تحول تهدیدات سایبری و در عین حال افزایش تداوم کسب و کار طراحی شده است. هدف ارائه یک استراتژی قوی و انطباقی برای کسب‌وکارها است که فراتر از پارادایم‌های سنتی امنیت سایبری است. این مطالعه از یک روش مبتنی بر بررسی ادبیات امنیت سایبری گسترده برای اطلاع از مفهوم‌سازی و توسعه تکراری یک نقشه راه انعطاف‌پذیر، ادغام عناصر کلیدی از منابع تثبیت‌شده و همسویی با خرد صنعت استفاده می‌کند. با ادغام اصول حاکمیت و رهبری، همکاری با ذینفعان خارجی و نظارت مستمر، این نقشه راه رویکردی به انعطاف‌پذیری سایبری را تقویت می‌کند. این مطالعه با استفاده از دیدگاه رفتاری، عوامل انسانی، آگاهی کاربر، و فرآیندهای تصمیم‌گیری را بررسی می‌کند و نقش حیاتی فرهنگ سازمانی را در تقویت اخلاقیات آگاه از امنیت سایبری تشخیص می‌دهد. یافته‌ها نقشه راهی را نشان می‌دهند که شامل انعطاف‌پذیری فناوری، ممیزی‌های منظم و ارزیابی‌ها، با تأکید بر بهبود مبتنی بر شواهد است. این نقشه راه به محدودیت‌های منابع، تنوع مقرراتی و چشم‌انداز تهدید پویا می‌پردازد و سازگاری را در مواجهه با زمینه‌های سازمانی متنوع ارتقا می‌دهد. اهمیت این مطالعه در کمک آن به تکامل مداوم استراتژی‌های انعطاف‌پذیری سایبری است که به سازمان‌ها راهنمای عملی برای هدایت پیچیدگی‌های قلمرو دیجیتالی ارائه می‌دهد. از آنجایی که کسب‌وکارها به طور فزاینده‌ای بر فناوری‌های به هم پیوسته متکی هستند، این نقشه راه به عنوان ابزاری حیاتی برای افزایش امنیت، حفاظت از دارایی‌های حیاتی و تضمین تداوم در مواجهه با چشم‌انداز تهدید سایبری در حال تغییر است.

کلمات کلیدی: امنیت سایبری، امنیت کسب و کار، تداوم کسب وکار، تهدیدات، نقشه راه انعطاف‌پذیری.

۱. مقدمه

توسعه سریع فناوری در چند دهه گذشته پیشرفت‌های بی‌سابقه‌ای را به همراه داشته است و اساساً نحوه عملکرد و تعامل کسب‌وکارها با جهان را تغییر داده است. با این حال، این سرعت سرسام آور تکامل فناوری بدون مجموعه‌ای از چالش‌ها نبوده است. مسائل امنیتی به طور فزاینده‌ای رایج شده‌اند، زیرا تهدیدات و آسیب‌پذیری‌های سایبری همگام با پیشرفت فناوری

* Sadeghi_maryam_IT@yahoo.com

افزایش می‌یابند [۱]. به هم پیوستگی سیستم های مدرن و حجم عظیم انتقال داده ها، زمینه مناسبی را برای عوامل مخرب ایجاد می‌کند تا از نقاط ضعف سوء استفاده کنند [۲]. از حملات سایبری پیچیده گرفته تا نقض داده‌ها، چشم انداز دیجیتال مملو از خطرات بالقوه است. از آنجایی که سازمان‌ها به طور فزاینده‌ای بر سیستم‌های به هم پیوسته و فرآیندهای مبتنی بر داده‌ها تکیه می‌کنند، نیاز به اقدامات امنیتی سایبری قوی‌تر از همیشه می‌شود [۱]. در برابر این پس‌زمینه پیچیدگی فن‌آوری و افزایش خطرات امنیتی است که کسب‌وکارها باید برای اطمینان از یکپارچگی، محرمانه بودن و در دسترس بودن دارایی‌های دیجیتال خود حرکت کنند [۲]. در دنیای پویا و به هم پیوسته تجارت، نیاز به اقدامات امنیت سایبری قوی هرگز به این اندازه حیاتی نبوده است. سازمان‌ها در حال حاضر به شدت به پلتفرم‌ها و شبکه‌های دیجیتال برای فعالیت‌های روزانه خود متکی هستند، که آنها را در معرض طیف وسیعی از تهدیدات سایبری قرار می‌دهد [۳]. عواقب یک حمله سایبری موفقیت آمیز می‌تواند شدید باشد، از خسارات مالی گرفته تا آسیب به شهرت. با شناخت ریسک‌های ذاتی، کسب‌وکارها باید ایجاد یک چارچوب امنیت سایبری انعطاف‌پذیر را برای اطمینان از بقا و موفقیت مستمر خود در یک چشم‌انداز دیجیتالی در حال تکامل در اولویت قرار دهند [۴]. ادغام یک سیستم امنیت سایبری قوی در چارچوب سازمانی برای مقابله با حملات الکترونیکی و حفظ پایداری کسب و کار بسیار مهم است [۴]. چنین سیستمی به عنوان سنگری در برابر تهدیدات بالقوه عمل می کند و تداوم و رشد بدون وقفه را امکان پذیر می‌سازد [۴]. همانطور که اکوسیستم دیجیتال پیچیده‌تر می‌شود، کسب و کارها باید در اقدامات پیچیده امنیتی سایبری برای کاهش خطرات و تقویت دفاع خود در برابر هجوم بی‌امان دشمنان سایبری سرمایه گذاری کنند [۵]. امنیت سایبری صرفاً یک مکانیسم دفاعی نیست. این یک توانمندساز استراتژیک است که اعتماد را در بین ذینفعان، مشتریان و شرکا تقویت می کند. وضعیت امنیت سایبری به خوبی تثبیت شده نه تنها در برابر تهدیدات بالقوه محافظت می‌کند، بلکه سازمان را به عنوان یک شریک قابل اعتماد و امن در بازار دیجیتال قرار می دهد [۶]. در سال‌های اخیر، مفهوم انعطاف‌پذیری سایبری به عنوان یک جنبه حیاتی از استراتژی امنیت سایبری ظاهر شده است [۷]. علی‌رغم اهمیت آن، بسیاری از کسب‌وکارها هنوز به طور کامل چارچوب انعطاف‌پذیری سایبری را پذیرفته‌اند و آنها را در برابر تاکتیک‌های در حال تکامل مجرمان سایبری آسیب‌پذیر می‌کند [۴]. فقدان یک رویکرد منسجم و انطباقی برای انعطاف‌پذیری سایبری می‌تواند منجر به آسیب‌پذیری‌های قابل‌توجهی شود، که مانع از توانایی کسب‌وکار برای بازیابی سریع و ادامه عملیات پس از یک حمله سایبری می‌شود. انعطاف‌پذیری سایبری فراتر از اقدامات امنیتی سنتی است. این توانایی یک سازمان برای پیش بینی، پاسخگویی و بازیابی از طیف متنوعی از تهدیدات سایبری را در بر می گیرد. این یک رویکرد کل نگر است که امنیت سایبری، مدیریت ریسک، و تداوم کسب و کار را برای تضمین دفاعی جامع در برابر چشم انداز تهدید در حال تکامل یکپارچه می کند [۸].

برای پرداختن به ماهیت در حال تحول تهدیدات سایبری، وجود چارچوب‌های انعطاف‌پذیری سایبری قابل اجرا ضروری است. این چارچوب‌ها نه تنها باید در برابر تهدیدات شناخته شده محافظت کنند، بلکه باید انعطاف‌پذیر و سازگار با چشم‌انداز در حال تغییر امنیت سایبری باشند [۴]. چالش در توسعه و به روز رسانی مداوم این چارچوب‌ها برای همگام شدن با پیشرفت‌های سریع در فناوری و ماهیت پیچیده‌تر حملات الکترونیکی نهفته است. رویکرد سنتی اقدامات ایستا امنیت سایبری دیگر کافی نیست. کسب‌وکارها به چارچوب‌های پویا نیاز دارند که بتوانند در کنار چشم‌انداز تهدید تکامل یابند. ادغام اطلاعات تهدید، نظارت مستمر، و مکانیسم‌های واکنش تطبیقی برای ایجاد انعطاف‌پذیری در برابر تهدیدات سایبری نوظهور بسیار مهم است. انگیزه پشت این تحقیق از ماهیت فزاینده و پویا تهدیدات سایبری ناشی می‌شود که سازمان‌ها در چشم انداز دیجیتال امروزی با آن مواجه هستند. تاکتیک‌های در حال تکاملی که توسط بازیگران مخرب به کار می‌رود، نیازمند رویکردی جامع و سازگار با امنیت سایبری است. فراوانی و پیچیدگی روزافزون حملات سایبری چالش‌های مهمی را برای انعطاف‌پذیری سیستم‌ها و داده‌های سازمانی ایجاد می‌کند. با تشخیص ضرورت یک استراتژی پیشگیرانه و کل نگر، هدف این تحقیق ارائه یک چارچوب ساختاریافته و همه کاره است که سازمان‌ها را در تقویت دفاع سایبری و مکانیسم‌های

واکنش راهنمایی می‌کند. از طریق تقویت دفاع و افزایش تداوم، چارچوب به دنبال رفع شکاف‌های موجود در استراتژی‌های امنیت سایبری کنونی است و به کسب‌وکارها یک رویکرد تطبیقی همسو با چشم‌انداز تهدید در حال تحول ارائه می‌دهد.

۲. بررسی ادبیات

در عصری که تحت سلطه پیشرفت‌های سریع تکنولوژیکی و چشم انداز دیجیتالی در حال گسترش است، کسب و کارها با سطح بی سابقه‌ای از تهدیدات سایبری مواجه هستند [۶]. نیاز به یک چارچوب انعطاف‌پذیری امنیت سایبری قوی برای محافظت در برابر ماهیت در حال تکامل و پیچیده حملات سایبری [۴]، بسیار مهم شده است. امروزه کسب‌وکارها در محیطی بسیار بهم پیوسته و وابسته به یکدیگر فعالیت می‌کنند و آنها را در برابر تهدیدات سایبری مختلف آسیب‌پذیر می‌کند که می‌تواند داده‌های حساس را به خطر بیاندازد، عملیات را مختل و شهرت را خدشه‌دار کند [۸]. از این رو، ایجاد یک چارچوب جامع انعطاف پذیری امنیت سایبری برای تقویت دفاع و اطمینان از تداوم عملیات تجاری ضروری است. برای شروع، یک چارچوب انعطاف‌پذیری امنیت سایبری یک رویکرد ساختاریافته برای شناسایی، ارزیابی و کاهش خطرات احتمالی سایبری ارائه می‌کند [۹]. با درک جامع چشم انداز تهدید، کسب و کارها می توانند به طور فعال اقدامات امنیتی را اجرا کنند که نه تنها آسیب‌پذیری‌های فعلی را برطرف می‌کند، بلکه چالش‌های آینده را نیز پیش بینی می‌کند. این موضع پیشگیرانه در محیطی که تهدیدات سایبری پویا و به طور مداوم در حال تکامل هستند، ضروری است و کسب و کارها را ملزم می‌کند که برای حفظ یک محیط عملیاتی ایمن از خطرات بالقوه جلوتر باشند [۱۰].

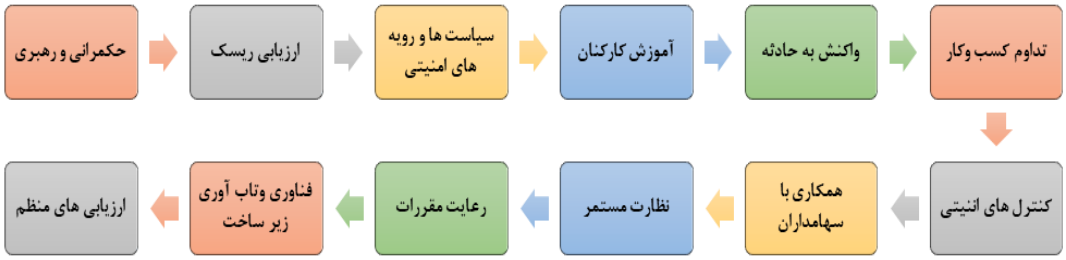
علاوه بر این، یک چارچوب امنیت سایبری انعطاف پذیر به طور قابل توجهی به استراتژی کلی مدیریت ریسک یک کسب و کار کمک می کند. با ادغام امنیت سایبری در چارچوب مدیریت ریسک گسترده‌تر، سازمان‌ها می‌توانند اقدامات امنیتی خود را با اهداف استراتژیک همسو کنند [۱۱]. این همسویی تضمین می‌کند که سرمایه‌گذاری‌های امنیت سایبری نه تنها به‌عنوان یک ضرورت برای انطباق در نظر گرفته می‌شوند، بلکه به‌طور استراتژیک در استراتژی کسب‌وکار تعبیه می‌شوند و انعطاف‌پذیری کلی سازمان را افزایش می‌دهند [۱۲]. علاوه بر کاهش خطرات، چارچوب انعطاف‌پذیری امنیت سایبری نقشی اساسی در تقویت مکانیسم‌های دفاعی یک کسب و کار ایفا می‌کند [۱۳]. این نه تنها شامل اقدامات تکنولوژیکی است، بلکه بر ایجاد یک فرهنگ آگاه از امنیت سایبری در سازمان نیز تمرکز دارد [۱۴]. کارکنان اغلب به عنوان اولین خط دفاع در نظر گرفته می‌شوند [۱۵]، و یک چارچوب انعطاف‌پذیر بر اهمیت آموزش امنیت سایبری و برنامه‌های آگاهی برای توانمندسازی افراد در سازمان برای شناسایی و پاسخگویی مؤثر به تهدیدات بالقوه تأکید می کند [۱۶].

علاوه بر این، ماهیت به هم پیوسته عملیات تجاری مدرن نیازمند یک رویکرد جامع به انعطاف پذیری امنیت سایبری است. یک چارچوب جامع نه تنها تهدیدهای داخلی بلکه عوامل خارجی از جمله آسیب پذیری های زنجیره تامین و خطرات شخص ثالث را نیز در نظر می‌گیرد. با گسترش اقدامات امنیتی فراتر از مرزهای سازمان، کسب و کارها می‌توانند انعطاف‌پذیری خود را در برابر طیف وسیعی از تهدیدات بالقوه که می‌تواند یکپارچگی عملیات آنها را به خطر بیندازد، افزایش دهند [۱۱]. یکی دیگر از جنبه‌های حیاتی چارچوب انعطاف‌پذیری امنیت سایبری، نقش آن در تضمین تداوم کسب و کار است [۴]. حملات سایبری می‌تواند عواقب شدیدی داشته باشد و منجر به اختلال در عملیات و خسارات مالی شود. یک چارچوب انعطاف‌پذیر، استراتژی‌هایی را برای حفظ عملکردهای ضروری کسب‌وکار در طول و بعد از یک حادثه سایبری در خود دارد [۱۷]. این شامل مکانیسم‌های پشتیبان‌گیری و بازیابی قوی، طرح‌های واکنش به حادثه، و استراتژی‌های ارتباطی برای به حداقل رساندن تأثیر حوادث سایبری بر عملیات تجاری است [۱۰]. در نتیجه، نیاز به یک چارچوب انعطاف پذیری امنیت سایبری برای مشاغل در چشم انداز دیجیتال امروز ضروری است. چنین چارچوبی نه تنها مکانیسم‌های دفاعی در برابر تهدیدات سایبری را تقویت می‌کند، بلکه به استراتژی کلی مدیریت ریسک کمک می‌کند، یک فرهنگ آگاه از امنیت سایبری ایجاد می‌کند، آسیب‌پذیری‌های زنجیره تامین را برطرف می‌کند و تداوم کسب‌وکار را تضمین می‌کند. در محیطی که

چشم‌انداز تهدید به طور مداوم در حال تغییر است، اتخاذ یک چارچوب جامع انعطاف‌پذیری امنیت سایبری نه تنها یک رویه تجاری محتاطانه بلکه یک ضرورت اساسی برای حفظ عملیات ایمن و انعطاف‌پذیر است. اکوسیستم دیجیتال در حال رشد، مملو از نوآوری و اتصال، به طور همزمان سازمان‌ها را در معرض تهدیدات سایبری در حال تکامل قرار می‌دهد. در این چشم‌انداز خیانت‌آمیز، چارچوب‌های امنیت سایبری قوی به‌عنوان زره ضروری عمل می‌کنند و ابزارها و استراتژی‌هایی را برای کاهش خطرات و حفاظت از دارایی‌هایشان در اختیار سازمان‌ها قرار می‌دهند [۴].

۳. ترسیم نقشه راه/ چارچوب

در ترسیم نقشه راه برای انعطاف‌پذیری سایبری، یک رویکرد روشمند اتخاذ شده است که مراحل متمایز متعددی را در بر می‌گیرد، شکل ۱.



شکل ۱- رویکرد ترسیم نقشه راه

۳-۱ حکمرانی و رهبری

تمرکز اولیه مرحله اولیه بر حکمرانی و رهبری است، با شناخت نقش حیاتی که ساختارهای حاکمیت سازمانی و شیوه‌های رهبری در تقویت انعطاف‌پذیری سایبری ایفا می‌کنند. در این مرحله اساسی، سه شاخص محوری برای راهنمایی و ارزیابی ایجاد یک چارچوب تاب آوری سایبری موثر، شناسایی شده است.

حکمرانی امنیت سایبری مستند: برای پرورش انعطاف‌پذیری سایبری قوی، توسعه و مستندسازی سیاست‌ها و رویه‌های حاکمیت امنیت سایبری شفاف و جامع است [۹]. این شاخص اول بر ضرورت ایجاد یک چارچوب ساختاریافته که اصول کلی، دستورالعمل‌ها و پروتکل‌های رویه‌ای حاکم بر امنیت سایبری را در چارچوب سازمانی مشخص می‌کند، تأکید می‌کند. وجود خط مشی های مستند نه تنها به عنوان یک نقطه مرجع اساسی برای همه ذینفعان عمل می کند، بلکه یک رویکرد استاندارد و یکپارچه برای مدیریت خطرات و چالش‌های امنیت سایبری را تضمین می‌کند. مجموعه ای دقیق و مستند از سیاست های حاکمیتی امنیت سایبری، نقشه راهی را برای سازمان فراهم می‌کند که هنجارها و شیوه‌های پذیرفته شده را روشن می‌کند. این مستندات به عنوان یک مصنوع اساسی عمل می‌کند و به انتشار بهترین شیوه‌های امنیت سایبری کمک می‌کند و درک جمعی را در بین ذینفعان تقویت می‌کند. علاوه بر این، تلاش‌های انطباق را تسهیل می‌کند و مبنایی را برای بررسی‌ها و به‌روزرسانی‌های دوره‌ای فراهم می‌کند، و تضمین می‌کند که چارچوب امنیت سایبری با مناظر تهدید در حال تکامل سازگار است.

نقش‌های رهبری امنیت سایبری تعریف شده: بر اساس استقرار سیاست‌های حاکمیتی، دومین شاخص بر اهمیت نقش‌ها و مسئولیت‌های تعریف‌شده اولیه برای رهبری امنیت سایبری تأکید می‌کند. تاب‌آوری سایبری مستلزم یک پاسخ هماهنگ و کارآمد به تهدیدات بالقوه است و این امر مستلزم تشریح واضح عملکردها و مسئولیت‌ها در میان افراد یا تیم‌های مسئول امنیت سایبری است [۹]. در این زمینه، نقش‌ها و مسئولیت‌های به خوبی تعریف شده به کارایی سازمانی در

مقابله با تهدیدات سایبری کمک می کند. وظایف مشخص شده تضمین می‌کند که هر جنبه‌ای از مدیریت امنیت سایبری، از ارزیابی ریسک تا واکنش به حادثه، توسط طرف‌های ذیصلاح و پاسخگو مدیریت می‌شود. این وضوح نه تنها توانایی سازمان را برای پاسخگویی سریع و مؤثر به حوادث سایبری افزایش می‌دهد، بلکه فرهنگ امنیت سایبری فعال و مشارکتی را ترویج می‌کند. با تشریح واضح مسئولیت‌های رهبری امنیت سایبری، سازمان‌ها می‌توانند چارچوبی برای پاسخگویی ایجاد کنند و فرهنگی را تقویت کنند که در آن افراد نقش خود را در حفاظت از دارایی‌های دیجیتال درک کنند. این شاخص پرورش نیروی کار آگاه از امنیت سایبری را ارتقا می‌دهد و سازمان را قادر می‌سازد تا از تخصص جمعی متخصصان امنیت سایبری خود به شیوه ای هدفمند و استراتژیک استفاده کند.

امنیت سایبری در تصمیمات استراتژیک: شاخص سوم، بعد استراتژیک انعطاف‌پذیری سایبری را با تأکید بر ضرورت ادغام ملاحظات امنیت سایبری در ساختار تصمیم‌های استراتژیک تجاری تقویت می‌کند. از آنجایی که سازمان‌ها در یک چشم‌انداز دیجیتالی فزاینده حرکت می‌کنند، همسویی امنیت سایبری با اهداف استراتژیک گسترده‌تر بسیار مهم می‌شود [۱۸]. این شاخص بر ضرورت تعبیه امنیت سایبری به عنوان یک جزء اساسی و جدایی‌ناپذیر از فرآیندهای برنامه‌ریزی استراتژیک برای سازمان‌ها تاکید می کند. دستیابی به یکپارچگی یکپارچه امنیت سایبری در تصمیم‌گیری استراتژیک مستلزم شناخت و ترکیب دیدگاه های امنیت سایبری در آغاز ابتکارات استراتژیک است. با انجام این کار، سازمان‌ها اطمینان حاصل می‌کنند که امنیت سایبری به عنوان یک عملکرد منزوی یا واکنشی تلقی نمی‌شود، بلکه در ساختار چشم انداز استراتژی سازمان بافته می‌شود. این ادغام فعال سازمان را قادر می‌سازد تا چالش‌های بالقوه امنیت سایبری را پیش‌بینی کرده و به طور پیشگیرانه به آن رسیدگی کند و وضعیت انعطاف پذیرتر و سازگارتر را تقویت کند. علاوه بر این، ادغام ملاحظات امنیت سایبری در تصمیمات استراتژیک، شناسایی هم افزایی و مبادله بین اهداف تجاری و الزامات امنیتی را تسهیل می‌کند. این همسویی سازمان‌ها را قادر می‌سازد تا تعادلی بین نوآوری، رشد و کاهش ریسک ایجاد کنند و اطمینان حاصل شود که امنیت سایبری به عنوان یک مانع تلقی نمی‌شود، بلکه بیشتر به عنوان یک عامل برای موفقیت استراتژیک تلقی می‌شود.

۳-۲ ارزیابی ریسک

مرحله دوم بر ارزیابی ریسک، یک مؤلفه حیاتی که مدیریت مؤثر امنیت سایبری را پایه‌ریزی می‌کند، تمرکز دارد. در این مرحله، تاکید بر ارزیابی و درک چشم‌انداز پویای خطرات امنیت سایبری از طریق یک رویکرد ساختاریافته و جامع است. مرحله دوم شامل سه شاخص کلیدی است که هر کدام برای تقویت توانایی سازمان برای ارزیابی و مدیریت پیشگیرانه خطرات امنیت سایبری طراحی شده است.

ارزیابی‌های ریسک امنیت سایبری به‌روزرسانی شده: سنگ بنای انعطاف‌پذیری مؤثر سایبری در ایجاد ارزیابی‌های ریسک امنیت سایبری به‌طور منظم و مستند شده نهفته است [۱۹]. این شاخص بر نیاز به ارزیابی مستمر و سیستماتیک تهدیدها و آسیب‌پذیری‌های بالقوه که می‌تواند بر دارایی‌های دیجیتالی سازمان تأثیر بگذارد، تأکید می‌کند. به‌روزرسانی‌های منظم ارزیابی‌های ریسک تضمین می‌کند که سازمان در جریان تهدیدات سایبری در حال تحول، پیشرفت‌های فناوری و تغییرات در چشم‌انداز عملیاتی خود قرار می‌گیرد.

اولویت بندی ریسک: مدیریت موثر ریسک های امنیت سایبری نیازمند یک رویکرد استراتژیک برای اولویت بندی است. این شاخص بر اهمیت اولویت بندی سیستماتیک ریسک‌های شناسایی شده بر اساس تأثیر بالقوه و احتمال وقوع آنها تأکید می کند. با دسته‌بندی ریسک‌ها بر اساس شدت و احتمال، سازمان‌ها می‌توانند منابع را به‌طور عاقلانه و با تمرکز بر کاهش بحرانی‌ترین و قریب‌الوقوع تهدیدات تخصیص دهند [۱۹].

ارزیابی مداوم: خطرات امنیت سایبری پویا هستند و تحت تأثیر بسیاری از عوامل داخلی و خارجی هستند [۲۰]. این شاخص بر اهمیت در نظر گرفتن و تجزیه و تحلیل مستمر این عوامل برای حفظ درک جامع از چشم انداز ریسک در

حال تحول تأکید می کند. عوامل داخلی ممکن است شامل تغییرات در ساختار سازمانی، زیرساخت‌های فناوری، یا پویایی نیروی کار باشد [۲۰]، در حالی که عوامل خارجی می‌توانند تهدیدات سایبری نوظهور، تغییرات نظارتی، یا تغییرات در چشم انداز ژئوپلیتیکی را دربر گیرند. در نظر گرفتن مداوم این عوامل تضمین می‌کند که ارزیابی‌های ریسک مرتبط و منعکس‌کننده وضعیت فعلی سازمان هستند. همچنین امکان شناسایی خطرات جدیدی را که ممکن است در نتیجه تغییرات در محیط داخلی یا خارجی پدیدار شوند، فراهم می‌کند. با هماهنگی با این عناصر زمینه‌ای، سازمان‌ها می‌توانند استراتژی‌های امنیت سایبری خود را به موقع تطبیق دهند و توانایی خود را برای مقابله فعالانه با تهدیدات و چالش‌های نوظهور افزایش دهند.

۳-۳ سیاست‌ها و رویه های امنیتی

با پیشروی به مرحله سوم چارچوب برای انعطاف‌پذیری سایبری، تمرکز اکنون به سیاست‌ها و رویه‌های امنیتی معطوف می‌شود - یک جنبه حیاتی در ترویج فرهنگ امنیت سایبری در سازمان. این مرحله به تدوین، ارتباط، و حفظ سیاست‌ها و رویه‌های جامع طراحی شده برای محافظت در برابر تهدیدات سایبری اختصاص دارد. سه شاخص کلیدی برای تقویت توانایی سازمان برای ایجاد و حفظ سیاست‌ها و رویه‌های امنیتی موثر شناسایی شده است.

دسترسی و آگاهی: محور اثربخشی سیاست های امنیتی، دسترسی و آگاهی از این سیاست‌ها در میان کارکنان است. این شاخص بر اهمیت حصول اطمینان از اینکه سیاست‌های امنیت سایبری نه تنها به خوبی مستند شده است بلکه به راحتی برای همه اعضای سازمان قابل دسترسی است، تأکید می‌کند. دسترس‌پذیری درک جمعی از دستورالعمل‌های تعیین‌شده را تسهیل می‌کند و مسئولیت مشترکی را برای امنیت سایبری بین کارکنان ایجاد می‌کند [۹]. آگاهی، در این زمینه، نه تنها شامل در دسترس قرار دادن خط‌مشی‌ها، بلکه ارتباط فعالانه و ترویج درک اهمیت آنها نیز می‌شود. سازمان‌ها از طریق کانال‌های مختلف مانند کتاب‌های راهنمای کارکنان، پلتفرم‌های اینترانت و جلسات آموزشی می‌توانند اطلاعاتی در مورد سیاست‌های امنیت سایبری منتشر کنند. پرورش نیروی کار آگاه و آگاه، پایبندی به پروتکل های امنیتی تعیین شده را افزایش می‌دهد و احتمال نقض سهوی امنیتی را کاهش می‌دهد [۲۱].

ارتباط منظم: با تکیه بر شاخص اول، سیاست‌های امنیتی مؤثر مستلزم ابتکارات ارتباطی و آموزشی مداوم است. ارتباط منظم تضمین می‌کند که کارکنان در مورد به روز رسانی سیاست‌ها، تهدیدات نوظهور و بهترین شیوه‌ها مطلع می‌مانند [۴]. این رویکرد پیشگیرانه به تعبیه یک ذهنیت امنیت سایبری در فرهنگ سازمانی کمک می‌کند و احساس مسئولیت مشترک برای حفاظت از دارایی‌های دیجیتال را تقویت می‌کند.

به‌روزرسانی‌های خط‌مشی برای فناوری و تهدیدها: ماهیت پویای چشم‌انداز امنیت سایبری، سازمان‌ها را ملزم می‌کند تا چابکی خود را در پاسخ به پیشرفت‌های فناوری و تهدیدات نوظهور حفظ کنند [۲۲]. این شاخص بر نیاز به به روز رسانی به موقع سیاست‌ها و رویه‌های امنیتی برای پرداختن به خطرات در حال تحول تاکید می‌کند. بررسی‌ها و بازنگری‌های منظم باید انجام شود تا سیاست‌ها را با آخرین پیشرفت‌های فناوری، استانداردهای صنعت و چشم‌انداز تهدید در حال تغییر همسو کند. به‌روزرسانی‌های به‌موقع همچنین شامل درس‌های آموخته‌شده از حوادث و نقض‌های امنیتی است. سازمان‌ها با تجزیه و تحلیل و تطبیق سیاست‌های مبتنی بر تجربیات دنیای واقعی، توانایی خود را برای جلوگیری از حوادث مشابه در آینده افزایش می‌دهند. این فرآیند تکراری تضمین می‌کند که سیاست‌های امنیت سایبری قوی، مرتبط و پاسخگو به ماهیت پویای تهدیدات سایبری هستند.

۳-۴ آموزش و آگاهی کارکنان

این مرحله مهم، نقش محوری کارکنان آگاه و هوشیار را در تقویت انعطاف‌پذیری سایبری کلی سازمان به رسمیت می‌شناسد. برای دستیابی به این هدف، سه شاخص کلیدی شناسایی شده است که هر کدام با هدف پرورش نیروی کار آگاه از امنیت سایبری قادر به کاهش خطرات به طور موثر است.

تعداد جلسات آموزشی و حضور و غیاب: یکی از سنگ بنای ایجاد یک فرهنگ آگاه از امنیت سایبری، ارائه منظم جلسات آموزشی به کارکنان است. این شاخص بر اهمیت فراوانی و حضور در این جلسات آموزشی تاکید می‌کند. جلسات آموزشی منظم و مکرر تضمین می‌کند که کارکنان به طور مداوم در معرض جدیدترین اطلاعات امنیت سایبری، تهدیدها و بهترین شیوه‌ها قرار دارند [۲۳]. حضور و غیاب به عنوان یک معیار محسوس عمل می‌کند که نشان دهنده مشارکت و تعهد کارکنان به ابتکارات امنیت سایبری سازمان است. با اندازه‌گیری دفعات جلسات آموزشی و نظارت بر میزان مشارکت، سازمان‌ها می‌توانند سطح قرار گرفتن در معرض و انتشار دانش را ارزیابی کنند و پرورش نیروی کاری را تسهیل کنند که به اصول امنیت سایبری آشنا باشد.

آگاهی از تهدیدات سایبری و بهترین شیوه‌ها: هدف اصلی آموزش کارکنان، افزایش آگاهی از تهدیدات رایج سایبری و القای بهترین شیوه ها برای کاهش خطرات است. این شاخص بر لزوم حضور کارکنان نه تنها در جلسات آموزشی بلکه برای نشان دادن درک جامع از تهدیدات سایبری رایج و اقدامات پیشگیرانه مربوطه تاکید می‌کند. سازمان‌ها می‌توانند این آگاهی را از طریق ارزیابی‌ها، آزمون‌ها یا نظرسنجی‌هایی که درک کارکنان از مفاهیم ضروری امنیت سایبری را ارزیابی می‌کنند، بسنجند.

شواهد گزارش‌دهی فعالیت‌های مشکوک: پرورش فرهنگ آگاه از امنیت سایبری فراتر از حفظ دانش به مشارکت فعال در حفاظت از دارایی‌های سازمانی گسترش می‌یابد [۸]. این شاخص ایجاد فرهنگی را ارزیابی می‌کند که در آن کارکنان به طور فعال با گزارش فعالیت‌های مشکوک یا حوادث امنیتی احتمالی در تلاش‌های امنیت سایبری مشارکت می‌کنند. سازمانی با فرهنگ قوی آگاه از امنیت سایبری، کارکنان را تشویق می‌کند تا در شناسایی و گزارش ناهنجاری‌ها فعال باشند. این می‌تواند شامل گزارش تلاش‌های فیشینگ، پرچم‌گذاری رفتار غیرعادی شبکه، یا گزارش فوری دستگاه‌های گمشده باشد. شواهدی از چنین مکانیسم‌های گزارش‌دهی واقعی رویدادها به‌عنوان مدرکی ملموس بر فرهنگی است که در آن امنیت سایبری در اخلاق سازمانی ریشه دوانده است.

۳-۵ طرح واکنش به حادثه

با پیشروی به مرحله پنجم چارچوب تاب آوری سایبری، تمرکز بر توسعه و اجرای طرح واکنش به حادثه[۱] معطوف می‌شود. این مرحله به آماده‌سازی سازمان برای واکنش‌های موثر در صورت وقوع یک حادثه امنیت سایبری اختصاص دارد. سه شاخص کلیدی شناسایی شده است تا اطمینان حاصل شود که سازمان برای شناسایی، پاسخگویی و بازیابی حوادث به خوبی مجهز است.

وجود و دسترسی طرح واکنش به حادثه: پایه و اساس یک قابلیت واکنش موثر حادثه در وجود یک طرح واکنش به حادثه مستند نهفته است [۴]. این شاخص بر اهمیت داشتن یک برنامه جامع، با تشریح روش‌ها و پروتکل‌هایی که باید در صورت وقوع یک حادثه امنیت سایبری دنبال شود، تأکید می‌کند. دسترسی به این طرح برای ذینفعان مربوطه در داخل سازمان نیز بسیار مهم است.

---

[۱] (IRP) Incident Response Plan

آزمایش و به روز رسانی منظم: ماهیت پویای تهدیدات سایبری و چشم انداز فناوری در حال تحول، آزمایش و به روز رسانی منظم طرح واکنش به حادثه را ضروری می‌کند [۱۴]. این شاخص بر اهمیت انجام تمرین‌ها و آزمایش‌های شبیه‌سازی شده برای اعتبارسنجی اثربخشی IRP در سناریوهای دنیای واقعی تأکید می‌کند. همچنین بر نیاز به بررسی‌ها و به‌روزرسانی‌های دوره‌ای تأکید می‌کند تا برنامه را با چشم‌انداز تهدید در حال تغییر و پیشرفت‌های فناوری هماهنگ نگه دارد. آزمایش منظم به سازمان‌ها اجازه می‌دهد تا زمینه‌های بهبود را شناسایی کنند، رویه‌های پاسخ را به دقت تنظیم کنند و اطمینان حاصل کنند که IRP مرتبط و مؤثر باقی می‌ماند. با ترکیب درس‌های آموخته شده از شبیه‌سازی‌ها، سازمان‌ها توانایی خود را برای واکنش سریع و قاطع در طول حوادث واقعی افزایش می‌دهند. این فرآیند تکراری آزمایش و به‌روزرسانی، انعطاف‌پذیری کلی قابلیت‌های واکنش به حوادث سازمان را تقویت می‌کند.

هماهنگی و ارتباط موثر: فراتر از وجود و آزمایش IRP، اثربخشی واکنش به رویداد به هماهنگی و ارتباط بستگی دارد. این شاخص بر نیاز سازمان‌ها به انجام تمرین‌های پاسخگویی به حادثه شبیه‌سازی شده تأکید می‌کند که نه تنها رویه‌های فنی را آزمایش می‌کند، بلکه هماهنگی و ارتباط بین تیم‌های واکنش به حادثه و ذینفعان مربوطه را نیز ارزیابی می‌کند. هماهنگی مؤثر شامل همکاری بی‌وقفه تیم‌های مختلف از جمله فناوری اطلاعات، امنیت، حقوقی و ارتباطات است تا از پاسخ یکپارچه به حادثه اطمینان حاصل شود [۲۱].

۳-۶ تداوم کسب و کار و بازیابی بلایا

با ورود به مرحله ششم چارچوب پیشنهادی انعطاف‌پذیری سایبری، تمرکز بر تداوم کسب‌وکار و بازیابی فاجعه تغییر می‌کند - یک جنبه حیاتی که توانایی سازمان را برای حفظ عملکردهای اساسی در مواجهه با اختلالات تضمین می‌کند. سه شاخص کلیدی برای ایجاد و ارزیابی آمادگی سازمان برای حفظ عملیات در طول و بعد از یک حادثه امنیت سایبری شناسایی شده است.

مستندسازی اقدامات: در هسته تداوم کسب و کار و بازیابی بلایا[۱] مستندسازی اقداماتی است که تداوم عملکردهای حیاتی را تضمین می کند [۱۴]. این شاخص بر ضرورت وجود برنامه‌ها و استراتژی‌های جامع برای تداوم عملیات ضروری در طول و پس از یک رویداد مخرب تأکید می‌کند. این اقدامات باید نه تنها سیستم‌های فناوری اطلاعات، بلکه فرآیندها و منابع کلیدی کسب‌وکار را نیز دربرگیرد.

آزمایش و نتایج طرح‌های بازیابی: یک عنصر حیاتی تداوم کسب‌وکار و آمادگی برای بازیابی بلایا، آزمایش منظم طرح‌های بازیابی بلایا است. این شاخص بر اهمیت انجام آزمایش‌های سیستماتیک برای ارزیابی اثربخشی طرح‌های بازیابی، از جمله بازسازی سیستم‌های فناوری اطلاعات و فرآیندهای حیاتی تأکید می‌کند. فراوانی و دقیق بودن این آزمون ها به عنوان معیارهای کلیدی برای ارزیابی آمادگی سازمان عمل می‌کند.

شواهد بازیابی موفقیت آمیز: اعتبار نهایی اقدامات تداوم کسب و کار و بازیابی فاجعه از شواهدی مبنی بر بازیابی موفق پس از یک حادثه شبیه سازی شده یا واقعی حاصل می شود [۲۱]. این شاخص بر اهمیت ردیابی و مستندسازی مواردی تاکید می‌کند که سازمان با موفقیت عملکردهای حیاتی خود را پس از یک اختلال بازیابی می‌کند، خواه این حادثه شبیه سازی شده باشد یا در یک سناریوی واقعی رخ داده باشد.

[۱] Business Continuity and Disaster Recovery (BCDR)

۳-۷ کنترل های امنیتی

با انتقال به مرحله هفتم از چارچوب پیشنهادی انعطاف‌پذیری سایبری، تمرکز بر روی کنترل‌های امنیتی - یک جزء ضروری در حفاظت از دارایی‌های دیجیتال سازمان است. این مرحله شامل اجرا و مدیریت اقدامات با هدف پیشگیری، شناسایی و پاسخ به تهدیدات امنیتی است. سه شاخص کلیدی برای ارزیابی توانایی سازمان برای حفظ کنترل‌های امنیتی موثر شناسایی شده است.

به روز رسانی منظم کنترل امنیتی: پایه و اساس کنترل‌های امنیتی قوی در به روز رسانی منظم و اصلاح اقدامات امنیتی نهفته است. این شاخص بر اهمیت به روز نگه داشتن کنترل‌های امنیتی برای مقابله با تهدیدات، آسیب‌پذیری‌ها و تکنیک‌های بهره‌برداری نوظهور تأکید می‌کند. به‌روزرسانی‌های منظم تضمین می‌کند که مکانیسم‌های دفاعی سازمان برای مقاومت در برابر تهدیدات سایبری در حال تحول مجهز هستند [۴]. استفاده به موقع از وصله های امنیتی و به روز رسانی برای بستن آسیب پذیری های احتمالی در نرم افزار، سخت افزار و سایر اجزای زیرساخت ضروری است. نادیده گرفتن این جنبه می‌تواند سازمان را در معرض سوء استفاده‌های شناخته شده قرار دهد. این شاخص بر تعهد سازمان به حفظ وضعیت امنیتی پیشگیرانه با به روز رسانی و اصلاح منظم کنترل‌های امنیتی تاکید می‌کند.

پیاده‌سازی و اثربخشی احراز هویت: یک جنبه جدایی ناپذیر از افزایش کنترل‌های امنیتی، پیاده‌سازی و اثربخشی احراز هویت چند عاملی[۱] است [۷]. این شاخص بر اهمیت استفاده از فاکتورهای احراز هویت اضافی فراتر از رمزهای عبور برای افزایش امنیت دسترسی تاکید می‌کند. MFA با الزام کاربران به ارائه چندین اشکال شناسایی مانند رمز عبور، بیومتریک یا توکن‌های امنیتی، یک لایه حفاظتی اضافی اضافه می‌کند.

نظارت بر گزارش کنترل امنیتی برای ناهنجاری ها: شناسایی پیشگیرانه تهدیدات امنیتی با نظارت مستمر و تجزیه و تحلیل گزارش‌های کنترل امنیتی برای ناهنجاری‌ها تسهیل می‌شود [۱۴]. این شاخص بر اهمیت بازبینی فعال گزارش‌های تولید شده توسط کنترل‌های امنیتی، مانند فایروال‌ها، سیستم‌های تشخیص نفوذ و راه‌حل‌های آنتی ویروس تأکید می‌کند. تجزیه و تحلیل این گزارش‌ها، سازمان را قادر می‌سازد تا الگوها یا رفتارهای غیرعادی را شناسایی کند که ممکن است نشان‌دهنده حوادث امنیتی بالقوه باشد.

۳-۸ همکاری با سهامداران

با ورود به مرحله هشتم چارچوب پیشنهادی تاب‌آوری سایبری، تمرکز اکنون بر روی همکاری با سهامداران گسترش می‌یابد - یک جزء حیاتی در افزایش توانایی جمعی برای شناسایی، پیشگیری و پاسخ به تهدیدات امنیت سایبری. این مرحله بر اهمیت ایجاد مشارکت و به اشتراک گذاری اطلاعات با نهادهای خارجی برای تقویت انعطاف پذیری سایبری سازمان تأکید می‌کند. سه شاخص کلیدی برای ارزیابی اثربخشی تلاش های همکاری شناسایی شده است.

مستندسازی تلاش‌های همکاری: مرکز همکاری مؤثر، مستندسازی تلاش‌هایی است که در مشارکت با ذینفعان خارجی انجام می‌شود [۲۴]. این شاخص بر اهمیت حفظ سابقه ابتکارات مشترک، مشخص کردن ماهیت و دامنه تعامل با نهادهای خارجی تاکید می‌کند. اسناد ممکن است شامل توافقات رسمی، پروژه‌های مشترک یا منابع مشترک با هدف تقویت قابلیت های امنیت سایبری باشد. ثبت تلاش‌های همکاری نه تنها مرجعی ملموس برای ارزیابی تعهد سازمان به تقویت مشارکت‌هایی که به انعطاف‌پذیری سایبری کمک می‌کنند، ارائه می‌کند، بلکه به عنوان منبع ارزشمندی برای انتقال دستاوردها و استراتژی‌های مشترک سازمان به ذینفعان داخلی و خارجی عمل می‌کند. این همکاری‌های ثبت‌شده به اسنادی

---

[۱] multi-factor authentication (MFA)

ضروری تبدیل می‌شوند که تلاش‌های هماهنگ انجام شده برای ایجاد یک محیط امن را برجسته می‌کند و تعهد سازمان را برای رسیدگی به چالش‌های امنیت سایبری از طریق ابتکارات یکپارچه نشان می‌دهد.

به اشتراک گذاری اطلاعات تهدید: سنگ بنای همکاری موثر، به اشتراک گذاری اطلاعات تهدید و بهترین شیوه‌ها با گروه‌های صنعتی است [۲۵]. این شاخص بر اهمیت مشارکت فعال و بهره مندی از دانش جمعی در صنعت تاکید می‌کند. با به اشتراک گذاشتن اطلاعات در مورد تهدیدات نوظهور، بردارهای حمله و استراتژی‌های دفاعی موثر، سازمان‌ها می‌توانند به طور جمعی وضعیت امنیت سایبری خود را ارتقا دهند.

شواهد همکاری: یک جنبه ضروری از همکاری برای افزایش انعطاف‌پذیری سایبری شامل تعامل با مجری قانون و سازمان‌های امنیت سایبری است. این شاخص بر اهمیت ایجاد و حفظ روابط مشترک با نهادهایی که در مبارزه با جرایم سایبری و ارتقای امنیت سایبری در مقیاس وسیع‌تر نقش دارند، تأکید می‌کند. شواهد همکاری با سازمان‌های مجری قانون و امنیت سایبری ممکن است شامل تحقیقات مشترک، مکانیسم‌های به اشتراک‌گذاری اطلاعات، یا مشارکت در کمپین‌های آگاهی‌رسانی امنیت سایبری باشد. تلاش‌های مشترک در این حوزه با همسو کردن منافع در پرداختن به تهدیدات سایبری در سطح سیستمی، به انعطاف‌پذیری سایبری کلی سازمان و جامعه گسترده‌تر کمک می‌کند.

۳-۹ نظارت مستمر

با شروع مرحله نهم از چارچوب پیشنهادی انعطاف‌پذیری سایبری، اکنون تمرکز بر نظارت مستمر - یک مؤلفه مهم در شناسایی فعال و پاسخ به تهدیدات امنیت سایبری بالقوه است. این مرحله بر اهمیت نظارت و تجزیه و تحلیل مداوم برای حفظ وضعیت امنیت سایبری هوشیار تاکید می‌کند. سه شاخص کلیدی برای ارزیابی قابلیت سازمان برای نظارت مستمر شناسایی شده است.

پیاده سازی و کارکرد: هسته اصلی نظارت مستمر، پیاده سازی و عملکرد سیستم هایی است که برای ردیابی و تجزیه و تحلیل محیط دیجیتال سازمان به طور مداوم طراحی شده اند [۷]. این شاخص بر اهمیت وجود راه حل های نظارت مستمر قوی و موثر در محل تأکید می‌کند. این سیستم‌ها باید طیف وسیعی از دارایی‌ها، از جمله شبکه‌ها، نقاط پایانی، برنامه‌های کاربردی و مخازن داده‌ها را در بر گیرند.

استفاده از ابزار تحلیل: یک فناوری کلیدی در حوزه نظارت مستمر، مدیریت اطلاعات امنیتی و رویداد[۱] است [۲۶]. این شاخص بر اهمیت استفاده منظم از ابزارهای SIEM برای تجزیه و تحلیل بلادرنگ رویدادهای امنیتی تاکید می‌کند. سیستم‌های SIEM داده‌ها را از منابع مختلف جمع‌آوری و به هم مرتبط می‌کنند و دید جامعی از وضعیت امنیتی سازمان ارائه می‌دهند. استفاده منظم از ابزارهای SIEM به سازمان‌ها اجازه می دهد تا حوادث امنیتی، ناهنجاری ها و تهدیدهای بالقوه را شناسایی کرده و به سرعت به آنها پاسخ دهند. استفاده مؤثر از این ابزارها نه تنها مستلزم استقرار آنها، بلکه بهینه‌سازی مداوم برای همسویی با چشم انداز تهدید در حال تحول سازمان است. این شاخص تعهد سازمان به استفاده از فناوری SIEM را به عنوان یک اقدام پیشگیرانه برای نظارت مستمر ارزیابی می‌کند.

شواهد نظارت پیشگیرانه: تکمیل نظارت مستمر مبتنی بر فناوری، شواهدی از تلاش‌های انسان محور فعالانه، از جمله ممیزی‌های منظم و بررسی گزارش‌ها است [۲۲]. این شاخص بر اهمیت ایجاد یک روال برای بازرسی دستی سیاهه‌ها، پیکربندی‌ها و کنترل‌های امنیتی تأکید می‌کند. این ممیزی ها به شناسایی آسیب پذیری های بالقوه، فعالیت های غیرمجاز و شکاف‌ها در وضعیت امنیتی کمک می‌کند.

[۱] Security Information and Event Management (SIEM)

۳-۱۰ رعایت مقررات

این مرحله بر اهمیت همسویی شیوه های امنیت سایبری با مقررات قابل اجرا برای اطمینان از اجرای تعهدات قانونی و نظارتی تأکید می کند. سه شاخص کلیدی برای ارزیابی تعهد سازمان به رعایت مقررات شناسایی شده است.

آگاهی از مقررات امنیت سایبری: اساس انطباق با مقررات در آگاهی و درک مقررات مربوط به امنیت سایبری نهفته است [۲۷]. این شاخص بر اهمیت آگاه ماندن در مورد چشم انداز نظارتی قابل اجرا در صنعت و موقعیت جغرافیایی سازمان تأکید می کند. آگاهی فراتر از دانش صرف به درک عمیق مفاهیم و الزامات این مقررات گسترش می‌یابد. سازمان‌ها باید به‌روزرسانی‌ها، تغییرات و مقررات جدیدی را که ممکن است بر رویه‌های امنیت سایبری تأثیر بگذارد، فعالانه نظارت کنند [۲۱]. این شاخص تعهد سازمان را به حفظ یک موضع فعال در درک محیط نظارتی و آگاه ماندن از هرگونه تغییری که می‌تواند بر تعهدات انطباق تأثیر بگذارد، ارزیابی می‌کند.

ارزیابی‌های انطباق منظم: انطباق یک فرآیند مداوم است که نیاز به ارزیابی‌های منظم و مستندسازی وضعیت انطباق سازمان دارد. این شاخص بر اهمیت انجام ارزیابی‌های سیستماتیک برای سنجش پایبندی به مقررات مربوط به امنیت سایبری تاکید می‌کند. ارزیابی‌های منظم تضمین می‌کند که سازمان همچنان مطابقت دارد و می‌تواند تعهد خود را به استانداردهای نظارتی نشان دهد. مستندسازی وضعیت انطباق شامل نگهداری سوابق دقیق ارزیابی‌ها، نتایج ممیزی و هرگونه اقدام اصلاحی انجام شده است. این مستندات به عنوان شواهدی ملموس از تلاش های سازمان برای پایبندی به الزامات نظارتی عمل می‌کند و پایه‌ای برای ارتباط شفاف با مقامات نظارتی و ذینفعان فراهم می‌کند.

تعدیل رویه‌ها: با تکامل چشم‌اندازهای نظارتی، سازمان‌ها باید سازگار باشند و برای اطمینان از انطباق مداوم، رویه‌های خود را اصلاح کنند [۲۸]. این شاخص بر نیاز سازمان‌ها برای شناسایی فعالانه و اجرای تغییرات در شیوه‌های امنیت سایبری خود در پاسخ به الزامات نظارتی در حال تحول تأکید می‌کند. تنظیمات ممکن است شامل به‌روزرسانی‌های خط‌مشی‌ها، رویه‌ها و کنترل‌های فنی برای همسویی با مقررات جدید یا اصلاح‌شده باشد. سازمان‌ها باید مکانیسم‌هایی را برای نظارت بر تغییرات نظارتی و ارزیابی تأثیر آنها بر رویه‌های امنیت سایبری ایجاد کنند. این شاخص توانایی سازمان را برای چابک ماندن و پاسخگو بودن ارزیابی می‌کند و اطمینان می‌دهد که اقدامات امنیت سایبری آن مطابق با آخرین انتظارات نظارتی است.

۳-۱۱ فناوری و تاب آوری زیرساخت

این مرحله بر اهمیت تقویت فناوری و زیرساخت‌ها برای مقاومت در برابر اختلالات و آسیب‌پذیری‌ها تأکید می‌کند. سه شاخص کلیدی برای ارزیابی قابلیت سازمان برای فناوری و انعطاف پذیری زیرساخت شناسایی شده است.

وجود معیارهای افزونگی: در هسته فناوری و انعطاف پذیری زیرساخت، وجود معیارهای افزونگی در سیستم های فناوری حیاتی است [۲۹]. این شاخص بر اهمیت پیاده‌سازی مکانیزم‌های پشتیبان‌گیری و خرابی برای اطمینان از تداوم عملیات در صورت بروز اختلال یا خرابی سیستم تأکید می‌کند. اقدامات افزونگی یک شبکه ایمنی را فراهم می‌کند و به عملکردهای حیاتی اجازه می‌دهد حتی اگر سیستم‌های اولیه با مشکلاتی مواجه شوند، ادامه پیدا کنند. وجود اقدامات افزونگی نشان دهنده تعهد سازمان به ایجاد پایه های فناورانه انعطاف پذیر است. این شامل ملاحظاتی مانند سرورهای اضافی، پشتیبان گیری از داده ها، و کانال های ارتباطی جایگزین است. این شاخص تلاش های پیشگیرانه سازمان را برای کاهش تأثیر اختلالات احتمالی در سیستم های فناوری حیاتی ارزیابی می‌کند.

نتایج تست زیرساخت: اطمینان از انعطاف پذیری زیرساخت مستلزم آزمایش منظم برای ارزیابی توانایی سازمان برای مقاومت در برابر سناریوها و چالش‌های مختلف است [۷]. این شاخص بر اهمیت انجام آزمایش‌های سیستماتیک برای

ارزیابی انعطاف‌پذیری اجزای زیرساخت، از جمله شبکه‌ها، سرورها و سایر دارایی‌های حیاتی تأکید می‌کند. آزمایش‌های منظم به سازمان‌ها اجازه می‌دهد تا آسیب‌پذیری‌ها را شناسایی کنند، اثربخشی طرح‌های اضطراری را تأیید کنند، و استراتژی‌ها را برای حفظ انعطاف‌پذیری زیرساخت اصلاح کنند. نتایج این آزمایش‌ها بینش‌هایی درباره آمادگی سازمان برای مقابله با اختلالات و زمینه‌های بالقوه برای بهبود ارائه می‌دهد. این شاخص تعهد سازمان به اعتبارسنجی فعال و افزایش انعطاف‌پذیری فناوری و زیرساخت خود را ارزیابی می‌کند.

به‌روزرسانی‌های سخت‌افزار و نرم‌افزار: انعطاف‌پذیری فناوری و زیرساخت نیز به به‌روزرسانی به‌موقع سخت‌افزار و نرم‌افزار برای رفع آسیب‌پذیری‌ها بستگی دارد. این شاخص بر اهمیت به روز ماندن وصله‌ها، به‌روزرسانی‌ها و پیشرفت‌های امنیتی برای کاهش خطرات احتمالی تأکید می‌کند. به روز رسانی‌های به موقع برای بستن آسیب‌پذیری‌هایی که می‌توانند توسط عوامل مخرب مورد سوء استفاده قرار گیرند ضروری هستند [۳۰]. اقدامات پیشگیرانه برای رفع آسیب‌پذیری‌ها شامل اعمال سریع وصله‌های امنیتی، به روز رسانی سیستم عامل و ارتقاء نرم افزار به آخرین نسخه‌ها است. این شاخص تعهد سازمان را به حفظ یک محیط فناوری ایمن و انعطاف پذیر از طریق به روز رسانی به موقع ارزیابی می‌کند و احتمال حملات سایبری موفق را کاهش می‌دهد.

۳-۱۲ ممیزی‌ها و ارزیابی‌های منظم

با ورود به آخرین مرحله چارچوب تاب‌آوری سایبری پیشنهادی، تمرکز بر ممیزی‌ها و ارزیابی‌های منظم - یک مؤلفه جدایی‌ناپذیر در حفظ وضعیت امنیت سایبری قوی است. این مرحله بر اهمیت ارزیابی‌ها، ممیزی‌ها و ارزیابی‌های سیستماتیک برای شناسایی آسیب‌پذیری‌ها، ارزیابی کنترل‌ها و ایجاد بهبود مستمر تاکید می‌کند. سه شاخص کلیدی برای ارزیابی تعهد سازمان به ممیزی‌ها و ارزیابی‌های منظم شناسایی شده است.

فرکانس ممیزی و نتایج: هسته اصلی حفظ وضعیت امنیت سایبری انعطاف‌پذیر، انجام منظم ممیزی‌های امنیت سایبری است. این شاخص بر اهمیت ممیزی‌های برنامه ریزی شده سیستماتیک برای ارزیابی پایبندی سازمان به خط‌مشی‌ها، الزامات نظارتی و بهترین شیوه‌های امنیت سایبری تاکید می‌کند. فراوانی ممیزی‌ها بینش‌هایی را در مورد تعهد سازمان به بررسی مداوم کنترل‌های امنیت سایبری ارائه می‌دهد [۱۴]. نتایج این ممیزی‌ها دیدگاه جامعی از اثربخشی اقدامات امنیت سایبری، شناسایی نقاط ضعف بالقوه و وضعیت کلی انطباق ارائه می‌دهد. با ارزیابی فراوانی و نتایج ممیزی‌های امنیت سایبری، سازمان‌ها می‌توانند توانایی خود را برای حفظ رویکردی فعال و هوشیارانه برای حاکمیت امنیت سایبری بسنجند.

ارزیابی آسیب‌پذیری و تست نفوذ: برای شناسایی فعالانه و رفع ضعف‌های بالقوه در زیرساخت امنیت سایبری، سازمان‌ها باید ارزیابی‌های آسیب‌پذیری و تست نفوذ را انجام دهند [۳۱]. این شاخص بر اهمیت جستجوی فعالانه آسیب‌پذیری‌ها و نقاط ضعف در سیستم‌ها، شبکه‌ها و برنامه‌ها تاکید می‌کند. شواهد ارزیابی آسیب‌پذیری و آزمایش نفوذ شامل گزارش‌های مستند، یافته‌ها و تلاش‌های اصلاحی است. مشارکت منظم در این فعالیت‌ها، موضع فعال سازمان را در شناسایی و رسیدگی به خطرات امنیتی بالقوه نشان می‌دهد. این شاخص تعهد سازمان به ارزیابی منظم دفاع از امنیت سایبری و تقویت انعطاف پذیری آن در برابر تهدیدات در حال تحول را ارزیابی می کند.

مستندسازی پیشرفت‌ها: انجام ممیزی و ارزیابی تنها در صورتی ارزشمند است که یافته‌ها موجب بهبودهای ملموس شوند [۲۲]. این شاخص بر اهمیت مستندسازی اقدامات خاص انجام شده برای رسیدگی به آسیب‌پذیری‌ها، تقویت کنترل‌ها و اجرای اقدامات اصلاحی بر اساس یافته‌های حسابرسی و ارزیابی تأکید می‌کند. مستندسازی پیشرفت‌ها سابقه شفافی از تعهد سازمان به یادگیری از ارزیابی‌ها و ممیزی‌ها ارائه می‌کند. همچنین به عنوان راهنمای پیشرفت‌های آینده عمل می‌کند و تضمین می‌کند که وضعیت امنیت سایبری سازمان در پاسخ به تهدیدات نوظهور و تغییر چشم‌انداز خطر تکامل می‌یابد.

٤. اجرای عملی چارچوب

اجرای عملی چارچوب تاب آوری سایبری شامل یک فرآیند چند وجهی است که مستلزم ادغام سیستماتیک مراحل و شاخص‌های آن در بافت سازمانی است. حکمرانی و رهبری اساسی هستند و مستلزم ایجاد یک ساختار حاکمیتی امنیت سایبری قوی با نقش‌ها و مسئولیت‌های مشخص شده است. ملاحظات امنیت سایبری باید به طور یکپارچه در فرآیندهای تصمیم‌گیری استراتژیک، با تأکید بر تعهد رهبری برای رویکردی از بالا به پایین که فرهنگ انعطاف‌پذیری سایبری را در سراسر سازمان تقویت می‌کند، در هم تنیده شود. دقت شاخص‌های ارزیابی ریسک، زمانی که به‌طور مؤثر پیاده‌سازی شوند، در توانایی آنها برای ارائه درک جامع و پویا از چشم‌انداز امنیت سایبری است. ارزیابی‌های ریسک امنیت سایبری که به‌طور منظم به‌روزرسانی می‌شوند، به عنوان یک عنصر اساسی عمل می‌کنند و تضمین می‌کنند که سازمان‌ها در مورد تهدیدات در حال تحول و پیشرفت‌های فناوری مطلع می‌شوند. مستندسازی این ارزیابی‌ها نه تنها تصمیم‌گیری آگاهانه و تلاش‌های انطباق را تسهیل می‌کند، بلکه شفافیت را در میان ذینفعان ارتقا می‌دهد. فرآیند اولویت‌بندی ریسک کلید تخصیص منابع است و به سازمان‌ها اجازه می‌دهد تا روی کاهش ریسک‌های پرتأثیر کارآمد تمرکز کنند. این رویکرد هدفمند تضمین می‌کند که تلاش‌ها به سمت آسیب‌پذیری‌ها با مهم‌ترین پیامدهای بالقوه هدایت می‌شوند و یک وضعیت امنیت سایبری تطبیقی را تقویت می‌کنند. علاوه بر این، تاکید بر ارزیابی مداوم، ماهیت پویای خطرات امنیت سایبری را با در نظر گرفتن عوامل داخلی و خارجی تایید می کند. تجزیه و تحلیل مستمر امکان شناسایی ریسک‌های جدید را فراهم می‌آورد و سازمان‌ها را قادر می‌سازد تا استراتژی‌های خود را به طور فعال تطبیق دهند و انعطاف‌پذیری خود را در برابر تهدیدها و چالش‌های نوظهور افزایش دهند.

مرحله حساس بعدی شامل آموزش و آگاهی کارکنان است. سازمان‌ها باید یک برنامه آموزشی جامع امنیت سایبری برای همه کارمندان ایجاد کنند و به طور منظم کمپین‌های آگاهی را اجرا کنند. هدف این ابتکارات آگاه نگه داشتن نیروی کار در مورد ماهیت پویای تهدیدات سایبری است. تجهیز کارمندان به دانش و پروتکل‌های گزارش فعالیت‌های مشکوک، فرهنگ آگاهی از امنیت سایبری را تقویت می‌کند و هر فرد را به یک مشارکت‌کننده فعال در دفاع سازمان در برابر تهدیدات سایبری تبدیل می‌کند. مدیریت ریسک یک مرحله محوری در فرآیند پیاده سازی است که نیاز به ارزیابی منظم ریسک برای شناسایی و اولویت بندی تهدیدات بالقوه دارد. سازمان باید استراتژی هایی را برای کاهش خطرات شناسایی شده توسعه دهد و آنها را به طور یکپارچه در فرآیندهای عملیاتی ادغام کند. ایجاد یک تیم اختصاصی پاسخگویی به ریسک، رویکردی سریع و هماهنگ برای مقابله با تهدیدات نوظهور را تضمین می‌کند و تاب‌آوری کلی سازمان را افزایش می‌دهد.

مراحل بعدی شامل اجرای عملی طرح های واکنش به حادثه، تداوم کسب و کار و اقدامات بازیابی بلایا و کنترل های امنیتی است. اینها مستلزم توسعه و آزمایش منظم طرح‌های جامع، مستندسازی اقدامات، و اجرای کنترل‌های امنیتی، از جمله بکارگیری به‌روزرسانی‌های به موقع و اثربخشی روش‌های احراز هویت است. همکاری با ذینفعان و نظارت مستمر به همان اندازه حیاتی است و نیازمند تلاش‌های مشترک مستند، مشارکت فعال در گروه‌های صنعتی، و شواهد نظارت فعال انسانی از طریق ممیزی‌های منظم است. مرحله اجرای نهایی شامل انطباق با مقررات، فناوری و انعطاف پذیری زیرساخت و ممیزی و ارزیابی منظم است. سازمان‌ها باید از مقررات مربوط به امنیت سایبری مطلع باشند، ارزیابی‌های انطباق منظم را انجام دهند، و به طور فعال اقدامات را برای همسویی با الزامات نظارتی در حال تغییر تنظیم کنند. اطمینان از انعطاف پذیری فناوری و زیرساخت شامل اقدامات اضافی، آزمایش منظم و به روز رسانی به موقع است. ممیزی‌های منظم، ارزیابی‌های آسیب‌پذیری، و آزمایش‌های نفوذ به بهبودهای مداوم کمک می‌کنند، و مستندسازی اقدامات خاص انجام‌شده برای رسیدگی به آسیب‌پذیری‌ها ضروری است. این استراتژی پیاده‌سازی جامع، پایه‌ای انعطاف‌پذیر امنیت سایبری را تشکیل می‌دهد و سازمان‌ها را برای هدایت پیچیدگی‌های قلمرو دیجیتال و تقویت دفاع خود در برابر عدم قطعیت‌های چشم‌انداز تهدید سایبری، موقعیت می‌دهد.

علاوه بر این، به‌روزرسانی‌های منظم در هر مرحله از چارچوب در پاسخ به تهدیدات نوظهور، نقشی اساسی در افزایش کارایی و انعطاف‌پذیری آن ایفا می‌کند. با همگام ماندن با چشم‌انداز تهدید در حال تحول، این چارچوب می‌تواند جدیدترین اقدامات امنیت سایبری را تطبیق داده و ترکیب کند و اطمینان حاصل کند که برای مقابله با چالش‌های معاصر مناسب است. نظارت و تجزیه و تحلیل مستمر تهدیدات جدید، تعدیل به موقع آستانه های ریسک را امکان پذیر می‌کند و امکان رویکردی فعال و پویا را برای مدیریت ریسک فراهم می‌کند. ادغام به‌روزترین اطلاعات تهدیدات در پروتکل‌های چارچوب تضمین می‌کند که استراتژی‌های کاهش با خطرات امنیت سایبری فعلی همسو هستند. این فرآیند تکراری نه تنها اثربخشی چارچوب را در خنثی کردن تهدیدات نوظهور تقویت می‌کند، بلکه پایه‌ای قوی برای انعطاف‌پذیری پایدار امنیت سایبری در زیرساخت‌های سازمانی ایجاد می‌کند.

۵. نتیجه‌گیری و تحقیقات آینده

این مطالعه یک نقشه راه به سمت انعطاف‌پذیری سایبری ترسیم کرده است، و چارچوبی قوی ارائه می‌کند که برای تقویت سازمان‌ها در برابر طیف همیشه در حال تکامل تهدیدات سایبری طراحی شده است. با پرداختن به ابعاد کلیدی، از حکمرانی و همکاری گرفته تا انعطاف‌پذیری فناوری و نظارت مستمر، این چارچوب رویکردی جامع ارائه می‌کند که فراتر از پارادایم‌های سنتی امنیت سایبری گسترش می‌یابد. سفر با حکمرانی و رهبری آغاز می‌شود، و یک پایه قوی مستلزم ادغام استراتژیک ملاحظات امنیت سایبری در تصمیم‌گیری سازمانی است. همکاری با ذینفعان خارجی، قدرت جمعی را در برابر تهدیدات سایبری تقویت می‌کند و بر ماهیت به هم پیوسته امنیت سایبری تأکید می‌کند. نظارت مستمر، انعطاف‌پذیری فناوری، و ممیزی‌های منظم مراحل مهمی را تشکیل می‌دهند و تضمین می‌کنند که سازمان‌ها در مواجهه با چشم‌اندازهای تهدید پویا هوشیار، سازگار، و فعال باقی می‌مانند. تاکید این چارچوب بر مستندات و بهبودهای مبتنی بر شواهد نشان دهنده تعهد به شفافیت، پاسخگویی و یادگیری مستمر است. در اصل، این مطالعه نه تنها یک نقشه راه برای ایجاد انعطاف‌پذیری سایبری ارائه می‌کند، بلکه بر اهمیت یک تغییر فرهنگی تأکید می‌کند. فراتر از فن‌آوری‌ها و فرآیندها، این فراخوانی است برای سازمان‌ها برای القای اخلاقیات آگاه از امنیت سایبری، و تبدیل امنیت سایبری از یک چک باکس انطباق به یک جنبه جدایی ناپذیر از DNA سازمانی[۱]. همانطور که سازمان‌ها این سفر را به سمت انعطاف پذیری سایبری آغاز می‌کنند، نه تنها خود را برای مقاومت در برابر چشم انداز تهدید فعلی مجهز می‌کنند، بلکه برای تکامل با آن نیز تجهیز می شوند. این چارچوب به عنوان یک راهنمای پویا عمل می‌کند و سیال بودن چالش‌های امنیت سایبری را تأیید می‌کند و قطب‌نمایی را برای سازمان‌ها فراهم می‌کند تا به سمت آینده‌ای تقویت‌شده در برابر عدم قطعیت‌های حوزه دیجیتال حرکت کنند.

هدف پژوهش‌های آتی در زمینه انعطاف‌پذیری سایبری، اصلاح استراتژی‌ها، پرداختن به چالش‌ها از طریق درک رفتار انسان در امنیت سایبری، ادغام فناوری‌های پیشرفته هوش مصنوعی و یادگیری ماشین، ایجاد معیارهای قابل سنجش، تقویت همکاری‌های بین‌صنعتی، و انطباق با الزامات انعطاف‌پذیری فناوری‌های نوظهور است. علاوه بر این، اجرای ارزیابی خودکار ریسک با استفاده از هوش مصنوعی یک جهت امیدوارکننده برای غلبه بر چالش‌های مربوط به درک ناکافی آستانه‌های ریسک قابل قبول در ارزیابی‌های ریسک سنتی است. این رویکرد با استفاده از الگوریتم‌های یادگیری ماشین، دقت و اثربخشی ارزیابی‌های ریسک را افزایش می‌دهد، بر محدودیت‌های انسانی غلبه می‌کند و فرآیندها را برای کارایی پاسخ‌دهی به مناظر در حال تحول امنیت سایبری ساده می‌کند. علاوه بر این، یک جهت تحقیق آینده توصیه شده شامل ارزیابی‌های تجربی، مانند بررسی انعطاف‌پذیری سایبری، برای ارزیابی جامع کاربرد عملی چارچوب ، به‌ویژه در ارزیابی اثربخشی سیاست‌ها و رویه‌های امنیتی است. این رویکرد نه تنها تطبیق پذیری چارچوب را غنی می‌کند، بلکه آن را با استانداردهای امنیت سایبری شناخته شده در سطح جهانی همسو می‌کند و راه را برای یک چارچوب انعطاف پذیری قوی‌تر و قابل اجراتر هموار می‌کند.

[۱] فرهنگ سازمانی، DNA پنهانی است که بر همه جنبه‌های عملکرد یک سازمان تأثیر می‌گذارد.

۶. مراجع

[1] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.

[2] A. N. Lone, S. Mustajab, and M. Alam, "A comprehensive study on cybersecurity challenges and opportunities in the iot world," *Security ‹ind Privacy*, vol. 6, no. 6, p. e318, 2023.

[3] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alab- dulatif, H. Arshad et al., "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers Mr Security*, vo1. 112, p. 102494, 2022.

[4] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023.

[5] A. Hawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, and G. Al- Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," *Solid State Technolog y*, vol. 63, no. 5, pp. 7894—7899, 2020.

[6] A. Kanaan, A. AL-Hawamleh, A. Abulfaraj, H. Al-Kaseasbeh, and A. Alorfi, "The effect of quality, security and privacy factors on trust and intention to use e-government services," *International Journal of Data and Network Science*, vol. 7, no. 1, pp. 185—198, 2023.

[7] A. M. Alhawamleh, "Advanced spam filtering in electronic mail using hybrid the mini batch k-means normalized mutual information feature elimination with elephant herding optimization technique," *International Journal of Computing and Digital Systems*, vol. 13, no. 1, pp. 1—1, 2023.

[8] A. Alqudhaibi, S. Deshpande, S. Jagtap, and K. Salonitis, "Towards a sustainable future: developing a cybersecurity framework for manufacturing," *Technological Sustainability*, vo1. 2, no. 4, pp. 372— 387, 2023.

[9] S. Slapničar, M. Axelsen, I. Bongiovanni, and D. Stockdale, "A pathway model to five lines of accountability in cybersecurity gov- ernance," *International journal of accounting infomiation systems*, vol. 51, p. 100642, 2023.

[10] A. Panda and A. Bower, "Cyber security and the disaster resilience framework," *Interiuitional Journal of Disaster Resilience in the Built Environment*, vol. 11, no. 4, pp. 507—518, 2020.

[11] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in it consulting industry," *Sustainability*, vol. 14, no. 3, p. 1269, 2022.

[12] I. F. De Arroyabe, C. F. Arranz, M. F. Arroyabe, and J. C. F. de Arroyabe, "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A uk survey for 2018 and 2019," *Computers Mr Security*, vol. 124, p. 102954, 2023.

[13] T. N. Alrumaih, M. J. Alenazi, N. A. AlSowaygh, A. A. Humayed, and I. A. Alablani, "Cyber resilience in industrial networks: A state of the art, challenges, and future directions," *Journal of King S‹iud University-Computer and Information Sciences*, p. 101781, 2023.

[14] H. M. Melaku, "A dynamic and adaptive cybersecurity governance framework," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327—350, 2023.

[15] A. AL-Hawamleh, "Exploring the satisfaction and continuance intention to use e-learning systems: An integration of the information systems success model and the technology acceptance model," *International journal of electrical and computer engineering systems*, vo1. 15, no. 2, pp. 201—214, 2024.

[16] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," *Computers & Security*, vo1. 132, p. 103372, 2023.

[17] F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," *Results in Control and Optimization*, vol. 12, p. 100268, 2023.

[18] Z. Jaradat, A. AL-Hawamleh, M. Altarawneh, H. Hikal, and A. Elfedawy, "The interplay between intellectual capital, business intelligence adoption, and the decision to innovate: Evidence from jordan," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1—12, 2024.

[19] J. Al-Gasawneh, A. AL-Hawamleh, A. Alorfi, and G. Al-Rawashde, "Moderating the role of the perceived security and endorsement on the relationship between per-ceived risk and intention to use the artificial intelligence in financial services," *International JournDl of Data and Network Science*, vol. 6, no. 3, pp. 743—752, 2022.

[20] D. Muneeb, A. Khattak, K. Wahba, S. Abdalla, and S. Z. Ahmad, "Dynamic capabilities as a strategic flexibility enabler: organizational responsiveness to covid-19," *Journal ofAsia Business Studies*, vol. 17, no. 4, pp. 824—849, 2023.

[21] A. AL-Hawamleh, M. Altarawneh, H. Hikal, and A. Elfedawy, "Blockchain technology and virtual asset accounting in the meta- verse: A comprehensive review

of future directions," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1—16, 2024.

[22] H. Naseer, K. Desouza, S. B. Maynard, and A. Ahmad, "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics," *European Journal of Information Systems*, pp. 1—21, 2023.

[23] A. M. Hawamleh and A. Ngah, "An adoption model of mobile knowledge sharing based on the theory of planned behavior," *Journal of Telecommunication, Electronic and Computer Engineering (ITEC)*, vo1. 9, no. 3-5, pp. 37—43, 2017.

[24] N. Stojéic, "Collaborative innovation in emerging innovation systems: Evidence from central and eastern europe," *The Journal of Technology Transer*, vol. 46, no. 2, pp. 531—562, 2021.

[25] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2525—2556, 2021.

[26] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach," *Applied Sciences*, vol. 13, no. 22, p. 12359, 2023.

[27] C. Donalds and K.-M. Osei-Bryson, "Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents," *International Journal of Information Management*, vo1. 51, p. 102056, 2020.

[28] Z. Jaradat, A. Al-Hawamleh, M. O. Al Shbail, and A. Hamdan, "Does the adoption of blockchain technology add intangible benefits to the industrial sector? evidence from jordan," *Journal of Financial Reporting and Accounting*, 2023.

[29] M. Belesioti, R. Makri, P. Karaivazoglou, E. Sfakianakis, I. Chochliouros, and A. Kyritsis, "Security and resilience in critical infrastructures," in *Technology Development for Security Practitioners. Springer*, 2021, pp. 317—333.

[30] W. Al Omari, N. Mai, H. S. Hin, and A. Al Hawamleh, "Enhancing learning process by applying cooperative learning supported with augmented reality environment," *International Journal*, vol. 10, no. 4, pp. 68—75, 2023.

[31] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability assessment for applications security through penetration simulation and testing," *Journal of Web Engineering*, vol. 21, no. 7, pp. 2187—2208, 2022.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Numerical Modelling of Carbon Dioxide Uptake by Planet Earth

Walter Jesus da Costa Martins Filho
My Institute/Company
Highway Augusto Montenegro km 10 S/N, Belém, Brazil
walterjcmf@gmail.com

ABSTRACT

Greenhouse gas emissions are a global concern, as they can have environmental consequences such as rising global temperatures and rising sea levels. The objective of this article is to numerically simulate the uptake of carbon dioxide emissions by the atmosphere, biosphere, and ocean. The theoretical framework used was the articles by Hoffert, Callegari & Hsieh (1980) and Oesheber et al (1974), which describe the use of the diffusion box model to describe the uptake of carbon dioxide by different media on planet Earth. Because of the uptake of carbon dioxide emissions, we have an increase in carbon concentrations in the atmosphere, biosphere, and ocean.

KEYWORDS: carbon dioxide emissions, numerically simulate, diffusion box model, increase in carbon concentrations

1 INTRODUCTION

The Industrial Revolution brought industrial and socioeconomic changes that were easily perceived. However, the Industrial Revolution brought more changes than those already mentioned. These changes took more than a century to be perceived. Among the main changes is the emission of greenhouse gases into the atmosphere, which, among other consequences, has increased the concentration of carbon in various environments on planet Earth.

To study how carbon dioxide emissions cause the increase in carbon concentration on the planet, it is necessary to build a model that describes this phenomenon. In this article, the diffusion box model was chosen, as described by the authors Hoffert, Callegari & Hsieh (1980), who use the diffusion box model to describe a global carbon cycle including the upwelling of inorganic carbon from the deep ocean, and Oesheber et al (1974), who use the diffusion box model to describe the natural carbon cycle with the emission of fossil fuels.

A model like this is described by a system of ordinary differential equations. To solve this system, we used the fourth-order Runge-Kutta method as described by Chapra and Canalle (2016). The resolution of this system of equations made it possible to construct a graph in which the increase in carbon concentrations in the Earth's environments was plotted as a function of the years.

Analysing a graph like this, even if it is not very accurate or requires better calibration of the data used, allows us to analyse what is happening on our planet with the emission of greenhouse gases such as carbon dioxide, and what the consequences of this are for the environment. Below is a description of the construction of the diffusion box model.

2 BOX-DIFFUSION CARBON CYCLE MODEL

We will divide the description of this process into two subtopics. In the first, we will describe how the diffusion box model works, and then, how the model used in this article was constructed.

2.1 Box Diffusion Model

The diffusion box model consists of representing each environment by boxes and following the physical principle that the environment with more mass gives mass to the environment with less mass. The mass flows are represented by arrows entering and leaving the boxes.

Since the mass flow is a variation of this quantity of physical magnitude in the studied environment, we represent this entry and exit of mass by the rate of variation of the mass concentration in this environment, which is equal to a percentage of capture times the difference in mass concentration in the two environments.

Figure 1 illustrates how a diffusion box model works.

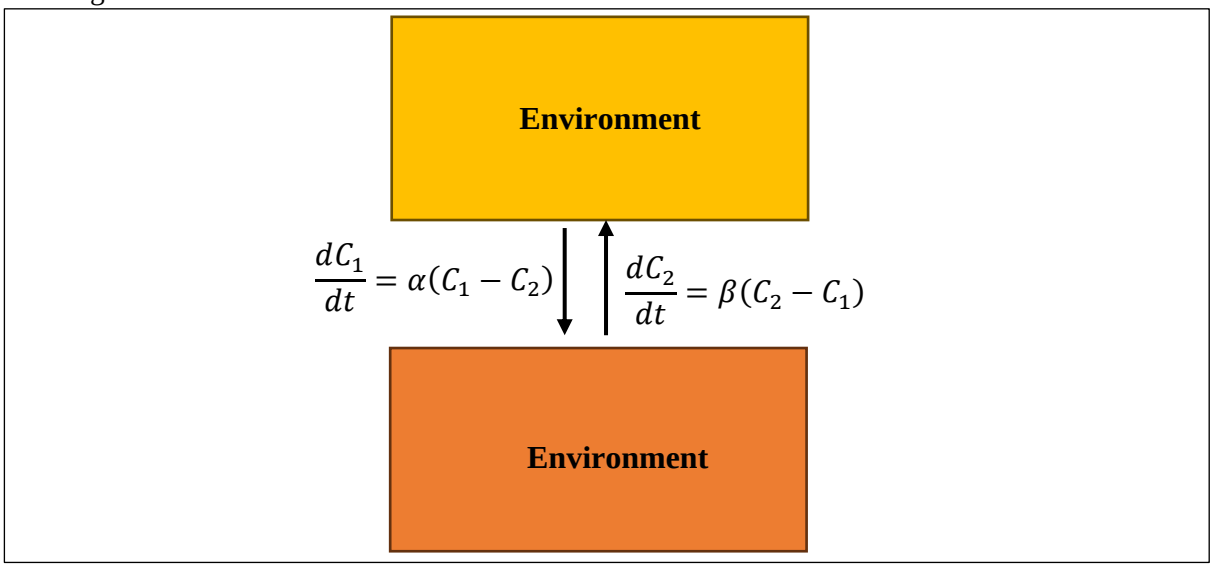


Figure 1: General representation of a diffusion box model.

2.2 Diffusion Box Model of Carbon Capture and Distribution

To construct the model for this article, the environments considered were the atmosphere, the ocean surface, the deep ocean, the biosphere formed by vegetation and the biosphere formed by the soil. The atmosphere is the first environment to receive the carbon dioxide emitted by industries, and then this mass of carbon is absorbed by vegetation and the ocean surface. Since vegetation performs photosynthesis, it also releases carbon dioxide into the atmosphere. This mass of carbon is then absorbed by the deep ocean and the soil.

Figure 2 illustrates how the diffusion box model works for the problem we are studying. In it, we can see that the atmosphere exchanges carbon mass directly with vegetation, soil and the ocean surface, but does not exchange carbon mass directly with the deep ocean.

Next, we have the description of the system of ordinary differential equations, which in our model, plays the role of carrying out the distribution of carbon in the mentioned environments.

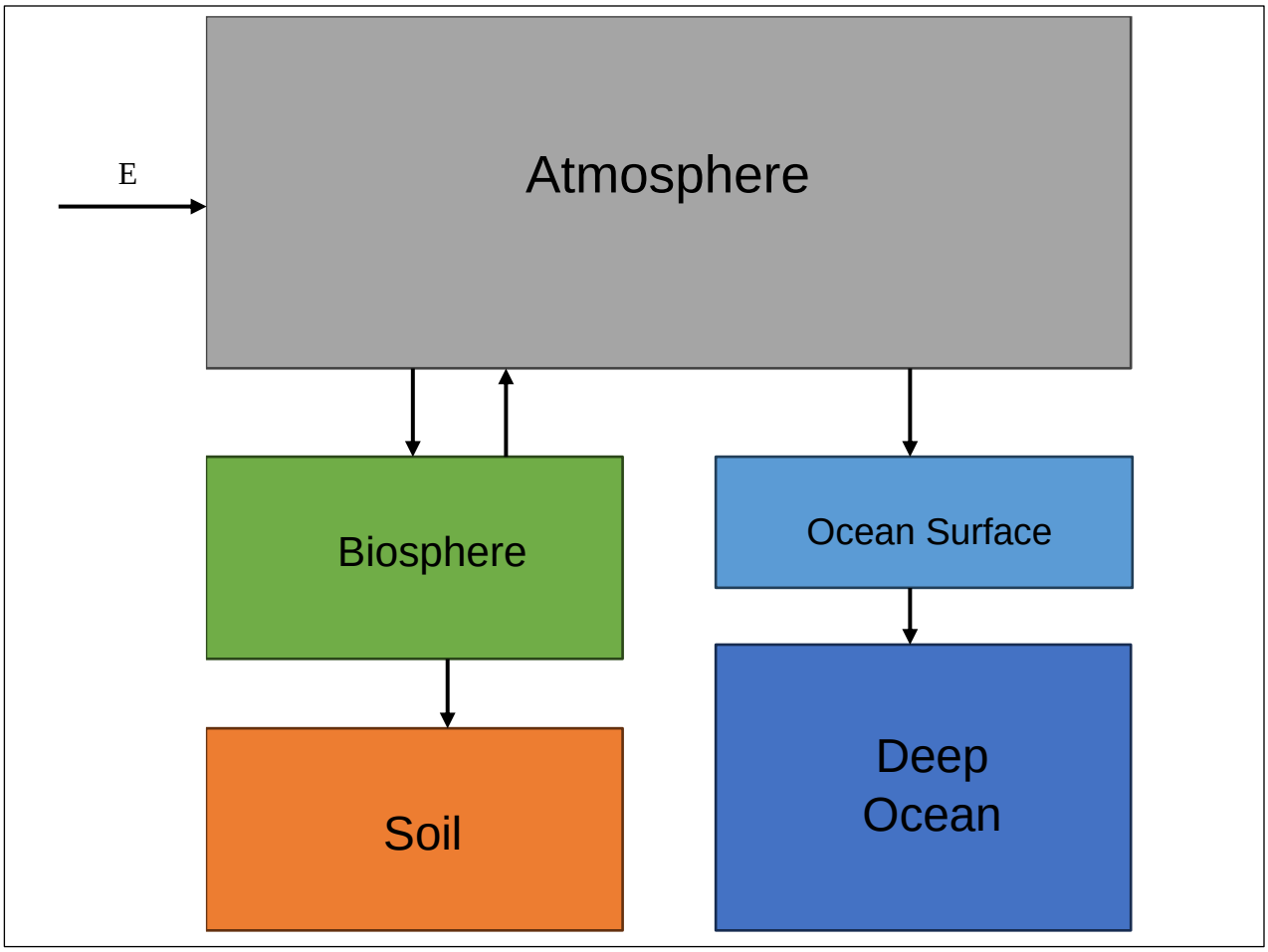


Figure 2: Diffusion box model used to describe the distribution of carbon in different environments on planet Earth.

2.3 System of Differential Equations Describing Carbon Distribution

According to the functioning of the diffusion box model described in subtopic 2.1, we can construct the system of ordinary differential equations related to the diffusion box model of subtopic 2.2. This system is presented in (1).

$$\begin{cases} \frac{dC_a}{dt} = E - \beta_1(C_a - C_s) - \gamma_1(C_a - C_{b1}) + \gamma_3(C_{b1} - C_a) \\ \frac{dC_s}{dt} = \beta_1(C_a - C_s) - \beta_2(C_s - C_p) \\ \frac{dC_p}{dt} = \beta_2(C_s - C_p) \\ \frac{dC_{b1}}{dt} = \gamma_1(C_a - C_{b1}) - \gamma_2(C_{b1} - C_{b2}) \\ \frac{dC_{b2}}{dt} = \gamma_2(C_{b1} - C_{b2}) - \gamma_3(C_{b2} - C_a) \end{cases} \quad (1)$$

The coefficients β_1 and β_2 represent the rates of carbon uptake by the ocean surface relative to the atmosphere and by the deep ocean relative to the ocean surface, respectively. While the coefficients γ_1, γ_2

and γ_3 represent carbon uptake by vegetation relative to the atmosphere, soil uptake relative to vegetation and atmospheric uptake relative to vegetation, respectively.

The parameter E represents the carbon dioxide emissions that are being released into the atmosphere. The carbon dioxide emissions used in this simulation are the historical carbon dioxide emissions.

This system of differential equations was solved using the fourth-order Runge-Kutta method. The description and execution of this method are not the objective of this article, but can be found in Chapra and Canalle (2016).

3 RESULTS

As a result of this numerical simulation using the diffusion box model and historical carbon dioxide emissions, we have the graph shown in Figure 3.

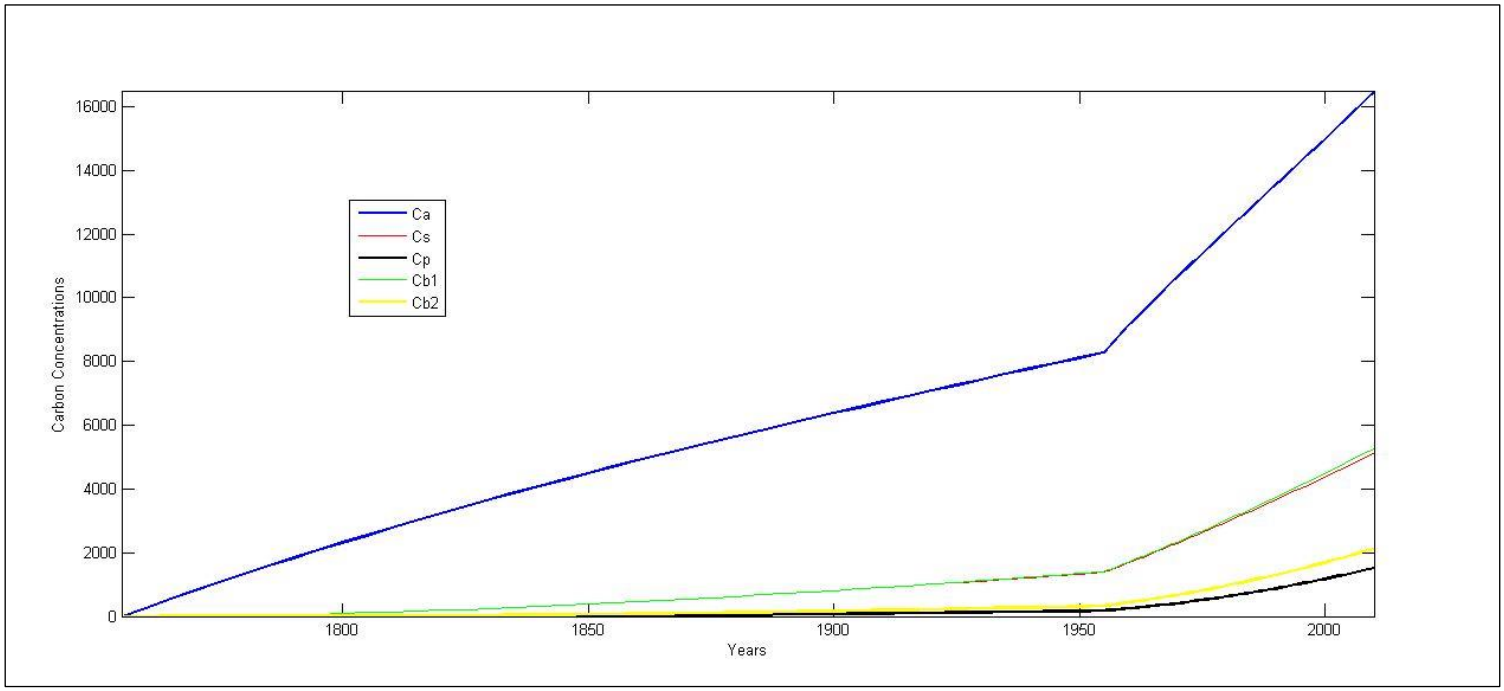


Figure 3: Diffusion box model used to describe the distribution of carbon in different environments on planet Earth.

In the graph in Figure 3, we have that, C_a represents the concentration of carbon in the atmosphere, C_s represents the concentration of carbon on the ocean surface, C_p represents the concentration of carbon in the deep ocean, C_{b1} represents the concentration of carbon in vegetation and C_{b2} represents the concentration of carbon in the soil.

4 CONCLUSION

As the main conclusion of this article, we have that since the beginning of the industrial revolution, carbon concentrations in various environments on planet Earth have been increasing and the trend continues to be upward.

Since historical carbon dioxide emissions were used, we can see from Figure 3 that the growth trend increased during the 1960s.

Steps must be taken to reduce carbon dioxide emissions, as this is the most likely cause of increased carbon concentrations in the environment.

5 ACKNOWLEDGEMENTS

I would like to thank professors Luís Aímola, Luiz Gylvan Meira Filho and the Vale Technological Institute who gave me the opportunity to study the topic addressed in this article.

REFERENCES

[1] H. Oeschger, U. Siegenthaler, U. Schotterer and A. Gugelmann, “A box diffusion model to study the carbon dioxide exchange in nature,” Tellus XXVII pp. 168–192, April 1975.

[2] M. I. Hoffert, A. J. Callegari, C. T. Hsieh, “A box diffusion carbon cycle model with upwelling, polar bottom water formation anda marine biosphere,” SCOPE 16 ed B Bolin (Chichester: Wiley) pp 287–306.

[3] CHAPRA, Steven C.; CANALE, Raymond P. Métodos numéricos para engenharia. 7. ed. Porto Alegre: AMGH, 2016. E-book. p.533. ISBN 9788580555691. Disponível em: https://bookplay.minhabiblioteca.com.br/reader/books/9788580555691/. Acesso em: 08 dez. 2024.

انتخاب مسیر با کمترین ریسک در شبکه های نامطمئن

فرحناز امیدی*، لیلا ترک زاده، بهزاد عباسی، کاظم نوری

دانشگاه سمنان، سمنان، ایران.

چکیده

در این مقاله مسئله انتخاب مسیر حداقل ریسک، در یک شبکه نامطمئن توصیف می‌شود. با فرض اینکه زیان‌های به وقوع پیوسته، متغیرهای نامطمئن هستند، ابتدا سه نوع شاخص ریسک نامطمئن را ارائه می دهیم. پس از آن، برخی از مدل‌های برنامه‌ریزی ریسک نامطمئن، بر اساس شاخص‌های ریسک پیشنهادی ساخته می‌شوند. برای به دست آوردن حداقل مسیر ریسک، این مدل‌های برنامه‌ریزی نامطمئن را به حالت خاص قطعی متغیرهای نامطمئن متناظر آن‌ها تبدیل می‌کنیم. در نهایت یک مثال عددی برای نشان دادن کارایی مدل ها ارائه می شود.

کلمات کلیدی: فضای نامطمئن، شبکه نامطمئن، انتخاب مسیر با کمترین ریسک، برنامه ریزی نامطمئن، تحلیل ریسک.

۱. مقدمه

مسئله انتخاب مسیر یکی از مسائل مهم در بهینه سازی شبکه است. تعداد زیادی از تحقیقات، مسئله انتخاب مسیر را از زوایای مختلف، مانند مشکل کوتاه‌ترین مسیر، مشکل حداکثر جریان و مشکل حمل و نقل مواد خطرناک بررسی کرده‌اند.
در مسئله انتخاب مسیر، عوامل عدم قطعیت و نامعین زیادی وجود دارد که معمولاً منجر به ریسک بالقوه می شود.
نظریه کلاسیکی که برای مقابله با عوامل نامعین استفاده می شود، نظریه احتمال است. بر اساس نظریه احتمال، تعاریف زیادی از ریسک ارائه شده است. آبکوویتز و همکاران از احتمال وقوع حادثه به عنوان معیار ریسک پیشنهادی معیارهای انتخاب مسیر استفاده کردند[1]. ارکوت و ورتر، احتمال تصادف را با پیامدهای آن مرتبط کردند و یک رویکرد ارزیابی ریسک برای انتخاب مسیر حمل و نقل پیشنهاد کردند[2]. علاوه بر این، ارکوت و ورتر اشاره کردند که مدل‌های ریسک مختلف ممکن است به مسیرهای بهینه متفاوتی منجر شوند[3]. دیاز بانز و همکاران، کوتاهترین مسیرها را برای حمل و نقل کالاهای خطرناک با حداقل کردن خطرات و هزینه مسیر تعیین کردند[4]. ناظمی و همکاران، بر روش های حل مسائل کوتاهترین مسیر و حداکثر جریان با کمک شبکه های عصبی مصنوعی پژوهش هایی انجام دادند[5,6].

در این مسئله انتخاب مسیر، برای به دست آوردن تابع احتمال وقوع یا توزیع تلفات، به داده های تاریخی زیادی نیاز داریم. با این حال، در واقعیت، اغلب به دلایل اقتصادی، تکنیک یا دلایل دیگر دست یابی به داده های تاریخی دشوار است و یا این داده ها در دسترس نیستند. در چنین شرایطی، استفاده از نظریه احتمال برای مدل‌سازی عوامل نامعین نادرست است. در

* **Corresponding author:** فرحناز امیدی
Email: omidi@semnanac.ir

این مقاله، نظریه نامطئن را برای مقابله با این نوع عامل عدم قطعیت انتخاب می کنیم و مسئله انتخاب مسیر را مورد بحث قرار می دهیم. نظریه نامطمئن شاخه ای از ریاضیات است که توسط لیو پایه گذاری شد [7] و به عنوان ابزاری برای مطالعه پدیده های نامطمئن در سیستم های انسانی، به ویژه در شرایط کمبود داده های تاریخی، توسط بسیاری از محققان از جنبه نظری مورد مطالعه قرار گرفته است و همچنین جنبه عملی این تحقیقات نظری شامل فرآیند نامطمئن [8]، مجموعه نامطمئن[9,10,11] ، نمودار نامطمئن[12,13,14] ؛ متغیر نامطمئن [15] و غیره، همچنین تحقیقات عملی شامل امور مالی نامطمئن [16,17]، بیمه نامطمئن[18,19] ، برنامه ریزی با هدف تصادفی نامطمئن [20] و غیره مورد بحث قرار گرفته اند.

تئوری نامطمئن برای اولین بار توسط لیو در سال ۲۰۰۹ بر روی شبکه و گراف اعمال شد که رویکرد جدیدی برای مطالعه شبکه در محیط نامطمئن ارائه کرد. پس از آن، گائو مسئله کوتاه ترین مسیر را با طول کمان نامشخص مورد بحث قرار داد [21]. ژانگ و پنگ، از برنامه ریزی نامطمئن برای مقابله با مشکل پستچی چینی با وزن نامعین استفاده کردند[22]. علاوه بر این، دینگ، مسئله جریان حداقل هزینه کلاسیک را به مسئله جریان حداقل هزینه نامشخص گسترش داد [22]. هان و همکاران، حداکثر جریان را در یک شبکه نامطمئن در نظر گرفت[23].

در مسئله انتخاب مسیر نامطمئن، توابع هدف عبارتند از طول [21]، زمان [12,13]، هزینه [22]، ظرفیت [23] و غیره. آنها ریسک را در نظر نمی گیرند و این موضوع انگیزه ای برای مطالعه روی مسئله انتخاب مسیر از نقطه نظر ریسک بر اساس نظریه نامطمئن فراهم می کند. این مقاله با با مسئله انتخاب مسیر با حداقل ریسک، با این فرض که ریسک توسط متغیر نامطمئن توصیف می‌شود، سروکار دارد. با الهام از شاخص های ریسک برای سیستم نامطمئن از لیو [9,10,11]، پنگ [24] و لیو و رالسکو [25]، ما چند شاخص ریسک نامطمئن را برای اندازه گیری ریسک یک مسیر پیشنهاد می کنیم. سپس مدل‌های برنامه‌ریزی ریسک نامطمئن را جهت جستجوی مسیر با حداقل ریسک در شبکه نامطمئن معرفی می کنیم. در مدل‌های ارائه شده، توابع هدف، شاخص‌های ریسک نامطمئن هستند. علاوه بر این، یک تکنیک برای حل راحت مدل‌ها ارائه می‌کنیم.

ادامه این مقاله به شرح زیر سازماندهی شده است. در بخش ۲، برخی از مفاهیم اساسی نظریه نامطمئن یادآوری می شود. در بخش ۳، به بیان مسئله و شاخص های ریسک در یک مسیر در شبکه نامطمئن پرداخته شده است. در بخش ۴، مدل‌هایی برای انتخاب مسیر با حداقل ریسک نامطمئن ساخته و مدل شبکه عصبی جهت حل مسائل برنامه ریزی به دست آمده پیشنهاد شده‌اند. در بخش ۵، یک مثال عددی برای نشان دادن کارایی مدل ها آورده شده است. بخش آخر شامل خلاصه ای کوتاه و نتیجه گیری است.

۲. مقدمات

تعریف: فرض کنید Γ یک مجموعه ناتهی و $\mathcal{L}$ یک σ- جبر روی Γ و $\mathcal{M}$ یک اندازه نامطمئن باشد؛ سه تایی $(\Gamma, \mathcal{L}, \mathcal{M})$یک فضای نامطمئن نامیده می‌شود و هرعضو $\Lambda \in \mathcal{L}$ یک پیشامد روی $(\Gamma, \mathcal{L}, \mathcal{M})$ نامیده می‌شود .

تعریف: متغیر نامطمئن: یک تابع اندازه‌پذیر مثل ξ از فضای نامطمئن $(\Gamma, \mathcal{L}, \mathcal{M})$ به مجموعه اعداد حقیقی است، به‌طوری‌که برای هر مجموعه بورل $\mathcal{B}$ مجموعه $\{\xi \in \mathcal{B}\}$ یک پیشامد باشد.

تعریف: تابع مجموعه‌ای $\mathcal{M}$ یک اندازه نامطمئن نامیده می‌شود اگر در اصول موضوعه نرمال بودن، خود دوگانی، زیرجمعی شمارا و اصل حاصلضرب که در زیر بیان می‌شوند صدق کند .

اصول موضوعه فضای نامطمئن: به منظور ارائه یک تعریف از اصول موضوعی فضای نامطمئن ضروری است که به هر پیشامد Λ یک عدد $\mathcal{M}\{\Lambda\}$ نسبت داده شود که میزان اعتقاد بر رخ دادن Λ را نشان می‌دهد. لیو اصول موضوعه زیر را برای این تابع ارائه داده است :

اصل۱: (نرمال بودن) $\mathcal{M}(\Gamma) = 1$،

اصل ۲: (خود دوگانی) برای هر پیشامدΛ ، $\mathcal{M}(\Lambda) + \mathcal{M}(\Lambda^c) = 1$،

اصل ۳: (زیر جمعی شمارا) برای هر دنباله شمارا از پیشامدهای$\{\Lambda_i\}$ داریم :

$$\mathcal{M}\left(\bigcup_{i=1}^{\infty} \Lambda_i\right) \leq \sum_{i=1}^{\infty} \mathcal{M}(\Lambda_i).$$

اصل۴: (اصل یکنوایی) اگر $\Lambda_1 \subseteq \Lambda_2$ آنگاه $\mathcal{M}(\Lambda_1) \leq \mathcal{M}(\Lambda_2)$

اصل۵: (اصل حاصلضرب) فرض کنید $(\Gamma_k, \mathcal{L}_k, \mathcal{M}_k)$ برای $k = 1,2,\ldots$ فضاهای نامطمئن باشند. اندازه نامطمئن ضربی $\mathcal{M}$ یک اندازه نامطمئن است که در رابطه زیر صدق می‌کند :

$$\mathcal{M}\left(\prod_{k=1}^{\infty} \Lambda_k\right) = \bigwedge_{i=1}^{\infty} \mathcal{M}_k(\Lambda_k).$$

که در آن $\wedge$ نماد اینفیمم و Λ_k پیشامد دلخواه از $\mathcal{L}_k$ است .

تعریف: فرض کنید $\xi_1, \xi_2, \ldots, \xi_n$ متغیرهای نامطمئن باشند و f یک تابع اندازه پذیر با مقادیر حقیقی باشد. در این صورت $f(\xi_1, \xi_2, \ldots, \xi_n)$ یک متغیر نامطمئن است .

تعریف: توزیع نامطمئن $\Phi: \mathbb{R} \to [0,1]$ برای متغیر نامطمئن ξ به‌صورت $\Phi(x) = \mathcal{M}\{\gamma \in \Gamma | \xi(\gamma) \leq x\}$ تعریف می‌شود .

تعریف: *فرض کنید ξ یک متغیر نامطمئن با توزیع نامطمئن Φ باشد در این صورت برای هر عدد حقیقی x داریم:*

$$\mathcal{M}\{\xi \leq x\} = \Phi(x), \quad \mathcal{M}\{\xi > x\} = 1 - \Phi(x)$$

قضیه : تابع Φ^{-1} را معکوس توزیع نامطمئن متغیر نامطمئن ξ گوییم اگر و تنها اگر به ازای هر $\alpha \in [0,1]$ داشته باشیم:

$$\mathcal{M}\{\xi \leq \Phi^{-1}(\alpha)\} = \alpha$$

اثبات فرض تابع Φ^{-1} معکوس توزیع نامطمئن متغیر ξ باشد. در این صورت برای هر α داریم :

$$\mathcal{M}\{\xi \leq \Phi^{-1}(\alpha)\} = \Phi(\Phi^{-1}(\alpha)) = \alpha$$

عکس قضیه، فرض کنید $\mathcal{M}\{\xi \leq \Phi^{-1}(\alpha)\} = \alpha$. قرار می‌دهیم $x = \Phi^{-1}(\alpha)$ آنگاه $\alpha = \Phi(x)$ و در نتیجه $\mathcal{M}\{\xi \leq x\} = \alpha = \Phi(x)$ بنابراین تابع Φ توزیع نامطمئن متغیر ξ و Φ^{-1} معکوس آن است .

قضیه: فرض $\xi_1, \xi_2, \ldots, \xi_n$ متغیرهای نامطمئن مستقل باشند و $\Phi_1, \Phi_2, \ldots, \Phi_n$ به ترتیب توابع توزیع نامطمئن این متغیرها باشد. اگر تابع $f(x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_n)$ نسبت به $x_1, x_2, \ldots, x_m$ اکیداً صعودی و نسبت

به $x_{m+1}, x_{m+2}, \dots, x_n$ اکیداً نزولی باشد. آنگاه فرایند نامطمئن $\xi = f(\xi_1, \xi_2, \dots, \xi_m, \dots, \xi_n)$ دارای تابع توزیع معکوس نامطمئنی به صورت زیر است .

$$\Phi^{-1}(\alpha) = f(\Phi_1^{-1}(\alpha), \dots, \Phi_m^{-1}(\alpha), \Phi_{m+1}^{-1}(1-\alpha), \dots, \Phi_n^{-1}(1-\alpha))$$

تعریف: اگر ξ یک متغیر نامطمئن باشد، تابع توزیع نامطمئن زیر را نرمال می‌نامند . که در آن $\sigma > 0$ و e اعداد حقیقی هستند و با $N(e, \sigma)$ نشان داده می‌شود .

$$\Phi(x) = (1 + exp\left(\frac{\pi(e-x)}{\sqrt{3}\sigma}\right))^{-1}, \quad x \in \mathbb{R} \tag{1}$$

تابع توزیع نامطمئن فوق را استاندارد گوییم اگر در آن $e = 0$ و $\sigma = 1$ باشد. معکوس تابع توزیع نامطمئن متغیر نامطمئن ξ با $\Phi^{-1}(\alpha), \alpha \in (0,1)$ نشان داده می‌شود و امید ریاضی آن را به صورت زیر تعریف می‌شود .

$$E[\xi] = \int_0^1 \Phi^{-1}(\alpha) d\alpha, \tag{2}$$

تعریف: فرض کنید ξ یک متغیر نامطمئن باشد؛ امید ξ به‌صورت زیر تعریف می‌شود .

$$E[\xi] = \int_0^{\infty} M\{\xi \geq x\} dx - \int_{-\infty}^0 M\{\xi \leq x\} dx,$$

به شرط آنکه حداقل یکی از دو انتگرال فوق متناهی باشند .

تعریف: فرض کنید ξ یک متغیر نامطمئن با امید متناهی e باشد؛ واریانس ξ به‌صورت زیر تعریف می‌شود .

$$V[\xi] = E[(\xi - e)^2]$$

تعریف: سیستمی با عوامل نامطمئن $\xi_1, \xi_2, \dots, \xi_n$ را در نظر بگیرید. تابع f یک تابع ضرر نامیده می شود، اگر مقدار از دست دادن مشخص شده باشد اگر و فقط اگر $f(\xi_1, \xi_2, \dots, \xi_n) > 0$ باشد.

تعریف: سیستمی با عوامل نامطمئن $\xi_1, \xi_2, \dots, \xi_n$ و تابع ضرر f را در نظر بگیرید. شاخص ریسک، یک اندازه نامطمئن است که دستگاه دارای ضرر مثبت است، یعنی

$$\text{ریسک} = M\{f(\xi_1, \xi_2, \dots, \xi_n) > 0\}$$

تعریف: سیستمی با عوامل نامطمئن $\xi_1, \xi_2, \dots, \xi_n$ و تابع ضرر f را در نظر بگیرید. ارزش در معرض ریسک به صورت زیر تعریف می شود.

$$VaR = sup\{x | M\{f(\xi_1, \xi_2, \dots, \xi_n) \geq x\} \geq \alpha\}.$$

تعریف: سیستمی با عوامل نامطمئن $\xi_1, \xi_2, \dots, \xi_n$ و تابع ضرر f را در نظر بگیرید. زیان مورد انتظار به صورت زیر تعریف می شود.

$$L = \int_0^{+\infty} M\{f(\xi_1, \xi_2, \dots, \xi_n) \geq x\} dx.$$

لم: فرض کنید $\xi_1, \xi_2, \ldots, \xi_n$ متغیرهای نامطمئن مستقل با توزیع نامطمئن $\Phi_1, \Phi_2, \ldots, \Phi_n$ باشند. اگر تابع ضرر $f(\xi_1, \xi_2, \ldots, \xi_n)$ نسبت به $\xi_1, \xi_2, \ldots, \xi_m$ اکیداً صعودی و نسبت به $\xi_{m+1}, \xi_{m+2}, \ldots, \xi_n$ اکیداً نزولی باشد، آنگاه شاخص ریشه معادله زیر خواهد بود.

$$f\left(\Phi_1^{-1}(1-\alpha), \ldots, \Phi_m^{-1}(1-\alpha), \Phi_{m+1}^{-1}(\alpha), \ldots, \Phi_n^{-1}(\alpha)\right) = 0$$

لم: فرض کنید $\xi_1, \xi_2, \ldots, \xi_n$ متغیرهای نامطمئن مستقل با توزیع نامطمئن $\Phi_1, \Phi_2, \ldots, \Phi_n$ باشند. اگر تابع ضرر $f(\xi_1, \xi_2, \ldots, \xi_n)$ نسبت به $\xi_1, \xi_2, \ldots, \xi_m$ اکیداً صعودی و نسبت به $\xi_{m+1}, \xi_{m+2}, \ldots, \xi_n$ اکیداً نزولی باشد، ارزش در معرض ریسک به صورت زیر خواهد بود.

$$VaR(\alpha) = f\left(\Phi_1^{-1}(1-\alpha), \ldots, \Phi_m^{-1}(1-\alpha), \Phi_{m+1}^{-1}(\alpha), \ldots, \Phi_n^{-1}(\alpha)\right)$$

لم: فرض کنید $\xi_1, \xi_2, \ldots, \xi_n$ متغیرهای نامطمئن مستقل با توزیع نامطمئن $\Phi_1, \Phi_2, \ldots, \Phi_n$ باشند. اگر تابع ضرر $f(\xi_1, \xi_2, \ldots, \xi_n)$ نسبت به $\xi_1, \xi_2, \ldots, \xi_m$ اکیداً صعودی و نسبت به $\xi_{m+1}, \xi_{m+2}, \ldots, \xi_n$ اکیداً نزولی باشد، آنگاه زیان مورد انتظار به صورت زیر خواهد بود.

$$L = \int_0^1 f\left(\Phi_1^{-1}(\alpha), \ldots, \Phi_m^{-1}(\alpha), \Phi_{m+1}^{-1}(\alpha 1-), \ldots, \Phi_n^{-1}(1-\alpha)\right) d\alpha.$$

۳. بیان مسئله

فرض کنید $N = (V, E)$ نشان دهنده یک شبکه باشد که در آن $V = \{v_1, v_2, \ldots, v_n\}$ مجموعه متناهی از راس ها و $E = \{(v_i, v_j) | v_i, v_j \in V\}$ مجموعه یالها باشد. زیان به وقوع پیوسته که توسط عوامل معینی بر یال (v_i, v_j) ایجاد شده است به صورت r_{ij} است. اگر زیان به وقوع پیوسته r_{ij} مقدار قطعی و دقیق باشد، مسیر حداقل ریسک به مسئله کلاسیک کوتاهترین مسیر تبدیل می شود.

برای مثال اگر $N = (V, E)$ یک شبکه ریسک قطعی باشد که در آن زیان r_{ij} بر یال v_{ij} در جدول ۱ نشان داده شده است. مسیر با حداقل ریسک P از راس v_1 به راس v_2 به صورت $v_1 \to v_4 \to v_5 \to\to v_2 \to v_3 \to v_6$ خواهد بود. و حداقل زیان ۶ است.

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	–	۵	۷	۱	۳	۱۰
v_2	۵	–	۲	۴	۱	۳
v_3	۷	۲	–	۸	۵	۱
v_4	۱	۴	۸	–	۱	۸
v_5	۳	۱	۵	۱	–	۶
v_6	۱۰	۳	۱	۸	۶	–

جدول ۱

برای کاهش ریسک، باید زیان تصادفی را پیش بینی کنیم. با این حال، در واقع، ما معمولاً ارزش دقیق از دست دادن تصادفی قبل از رسیدن به مقصد و پایان را نمی دانیم. هنگامی که داده های کافی در مورد تلفات تصادفی وجود دارد، می

توانیم توزیع احتمال را در مورد از دست دادن تصادفی به دست آوریم و با برخی از روش های تصادفی و مدل های برنامه نویسی مسئله انتخاب مسیر را حل کنیم. [1,26]

متأسفانه، در بسیاری از موارد، ما فقط داده های کمی داریم، یا حتی داده ای برای تخمین توزیع احتمال به دلایل مختلفی در دسترس نداریم. در چنین مواردی، تنها انتخاب دعوت از کارشناسان حوزه برای ارزیابی درجه اعتقاد به وقوع خسارت تصادفی است. تعداد زیادی از بررسی‌ها نشان می‌دهند که از دست دادن تصادفی محاسبه شده توسط کارشناسان، اضافه وزن خواهند داشت و دامنه بسیار وسیع تری از کاهش تصادفی را نسبت به کاهش واقعی ارائه می دهند.

بنابراین، مدل‌سازی درجات باور با نظریه احتمال نامناسب است. لذا نظریه نامطمئن را به عنوان ابزاری برای مقابله با درجه اعتقاد و بحث در مورد مسئله انتخاب مسیر انتخاب می‌کنیم.

فرض کنید $\xi = \{\xi_{ij}|(v_i, v_j) \in \mathrm{E}\}$ یک مجموعه از متغیرهای نامطمئن مستقل باشند و از ξ_{ij} برای بیان زیان از دست رفته استفاده کنیم، آنگاه شبکه ریسک نامطمئن به صورت $N = (V, E, \xi)$ نمایش داده می شود. در مثال قبل اگر مقادیر دقیق را با متغیرهای نامطمئن ξ_{ij} جایگزین کنیم، شبکه ریسک نامطمئن به صورت جدول ۲ به دست می آید که در آن $\xi_{ij} = \xi_{ji}$.

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	-	ξ_{12}	ξ_{13}	ξ_{13}	ξ_{14}	ξ_{15}
v_2	ξ_{21}	-	ξ_{23}	ξ_{24}	ξ_{25}	ξ_{26}
v_3	ξ_{31}	ξ_{32}	-	ξ_{34}	ξ_{35}	ξ_{36}
v_4	ξ_{41}	ξ_{42}	ξ_{43}	-	ξ_{45}	ξ_{46}
v_5	ξ_{51}	ξ_{52}	ξ_{53}	ξ_{54}	-	ξ_{56}
v_6	ξ_{61}	ξ_{62}	ξ_{63}	ξ_{64}	ξ_{65}	-

جدول 2

هدف، یافتن مسیری از گره مبدا به گره مقصد است که دارای حداقل تلفات باشد، یعنی مسیر با حداقل ریسک در شبکه ریسک نامطمئن $\mathrm{N} = (\mathrm{V}, \mathrm{A}, \xi)$.

ابتدا، یک نمایش رایج و مفید از یک مسیر P را معرفی می کنیم. فرض کنید $\mathrm{P} = \{x_{ij}|(v_i, v_j) \in \mathrm{E}\}$، که در آن x_{ij} متغیر تصمیم است و مقادیر 0 و 1 را می پذیرد. اگر مسیر P یال (v_i, v_j) را شامل شود، آنگاه $x_{ij} = 1$؛ در غیر این صورت $x_{ij} = 0$.

بدون از دست دادن کلیت، فرض کنیم راس مبدا v_1 و راس مقصد v_n باشد، بنابراین P مسیری از از راس v_1 به v_n خواهد بود اگر و تنها اگر

$$\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_i,v_j)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases}$$

$$x_{ij} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_j) \in \mathrm{E}.$$

زیان به وقوع پیوسته از طریق مسیر P به صورت زیر خواهد بود

$$l(P) = \sum_{(v_i,v_j)\in E} x_{ij}\xi_{ij}.$$

تعریف: فرض کنید $N = (V, A, \xi)$ یک شبکه ریسک نامطمئن و P یک مسیر باشد؛ اولین شاخص ریسک به صورت زیر تعریف می‌شود .

$$R_{l(P)} = M\{l(P) \geq x_0\},$$

که در آن $x_0 > 0$ زیان از قبل تعیین شده است.

تعریف: فرض کنید $N = (V, A, \xi)$ یک شبکه ریسک نامطمئن و P یک مسیر باشد؛ برای سطح اطمینان ریسک داده شده $\alpha \in (0,1)$ ، دومین شاخص ریسک به صورت زیر تعریف می‌شود .

$$l(P)_{VaR}(\alpha) = sup\{x | M\{l(P) \geq x\} \geq \alpha\},$$

که شاخص ارزش در معرض ریسک نامیده می شود.

تعریف: فرض کنید $N = (V, A, \xi)$ یک شبکه ریسک نامطمئن و P یک مسیر باشد؛ سومین شاخص ریسک به صورت زیر تعریف می‌شود .

$$E[l(P)] = \int_0^{+\infty} M\{l(P) \geq x\}dx,$$

که شاخص ریسک مورد انتظار نامیده می شود.

شاخص ریسک اندازه نامطمئن تنها اندازه نامعینی را مشخص می کند که زیان در آن رخ می دهد. شاخص ریسک VaR نامطمئن، هم درجه احتمال وقوع زیان و هم مقدار ارزش وقوع زیان را در نظر می‌گیرد که می‌تواند به عنوان مکمل اولین شاخص ریسک در نظر گرفته شود. شاخص ریسک مورد انتظار نامطمئن به معنای مقدار متوسط زیان به وقوع پیوسته $l(P)$ است. این شاخص ها ریسک یک مسیر در شبکه نامطمئن را از زوایای مختلف اندازه گیری می کنند.

تعریف: فرض کنید $N = (V, A, \xi)$ یک شبکه ریسک نامطمئن و P^* یک مسیر باشد؛ مسیر P^*، مسیر با اندازه حداقل ریسک نامیده می شود، اگر

$$M\{l(P^*) \geq x_0\} \leq M\{l(P) \geq x_0\},$$

برای همه مسیر های P ، که در آن $x_0 > 0$ زیان از قبل تعیین شده است.

تعریف: فرض کنید $N = (V, A, \xi)$ یک شبکه ریسک نامطمئن و P^* یک مسیر باشد؛ برای سطح اطمینان ریسک داده شده $\alpha \in (0,1)$ ، مسیر P^*، مسیر با اندازه حداقل ارزش در معرض ریسک نامیده می شود، اگر

$$sup\{x | M\{l(P^*) \geq x\} \geq \alpha\} \leq sup\{x | M\{l(P) \geq x\} \geq \alpha\}$$

برای همه مسیر های P.

تعریف: فرض کنید $N = (V, A, \xi)$ یک شبکه ریسک نامطمئن و P^* یک مسیر باشد؛ مسیر P^*، مسیر با حداقل ریسک مورد انتظار نامیده می شود، اگر

$$\int_0^{+\infty} M\{l(P^*) \geq x\}dx \leq \int_0^{+\infty} M\{l(P) \geq x\}dx$$

برای همه مسیر های P.

۴. مدل های مسیر حداقل ریسک

در این قسمت مدل هایی را بر اساس تعاریف مسیر حداقل ریسک مطرح کرده و روش هایی برای به دست آوردن حداقل مسیر ریسک ارائه می دهیم.

قضیه: فرض کنید ξ_{ij} ها متغیرهای نامطمئن مستقل با توزیع عدم قطعیت منظم Φ_{ij} برای هر $(v_i, v_j) \in E$ باشند. آنگاه مسیر با اندازه حداقل ریسک را می توان از مدل برنامه ریزی نامطمئن زیر بدست آورد

$$\begin{aligned} &Min \quad M\{l(P) \geq x_0\} \\ &\text{subject to} \\ &\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_j,v_i)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases} \\ &x_{ij} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_j) \in E. \end{aligned} \tag{۱}$$

که معادل قطعی آن به صورت مسئله برنامه ریزی زیر خواهد بود:

$$\begin{aligned} &Min \quad \alpha \\ &\text{subject to} \\ &\sum_{(v_i,v_j)\in E} x_{ij}\Phi_{ij}^{-1}(1-\alpha) = x_0, \\ &\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_j,v_i)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases} \\ &x_{ij} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_j) \in E. \end{aligned} \tag{۲}$$

قضیه: فرض کنید ξ_{ij} ها متغیرهای نامطمئن مستقل با توزیع عدم قطعیت منظم Φ_{ij} برای هر $(v_i, v_j) \in E$ باشند. آنگاه برای سطح اطمینان ریسک $\alpha \in (0,1)$، مسیر با اندازه حداقل ارزش در معرض ریسک را می توان از مدل برنامه ریزی نامطمئن زیر بدست آورد

$$\begin{aligned} &Min \quad l(P)_{VaR}(\alpha) \\ &\text{subject to} \\ &\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_j,v_i)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases} \\ &x_{ij} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_j) \in E. \end{aligned} \tag{۳}$$

که معادل قطعی آن به صورت مسئله برنامه ریزی خطی زیر خواهد بود:

$$Min \sum_{(v_i,v_j)\in E} x_{ij}\Phi_{ij}^{-1}(1-\alpha)$$

subject to

$$\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_j,v_i)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases} \quad (۴)$$

$$x_{ij} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_j) \in \mathrm{E}.$$

قضیه: فرض کنید ξ_{ij} ها متغیرهای نامطمئن مستقل با توزیع عدم قطعیت منظم Φ_{ij} برای هر $(v_i, v_j) \in \mathrm{E}$ باشند. آنگاه مسیر با اندازه حداقل ریسک مورد انتظار را می توان از مدل برنامه ریزی نامطمئن زیر بدست آورد

$$Min \quad E[l(P)] = \int_0^{+\infty} M\{l(P) \geq x\}dx$$

subject to

$$\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_j,v_i)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases} \quad (۵)$$

$$x_{ii} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_i) \in \mathrm{E}.$$

که معادل قطعی آن به صورت مسئله برنامه ریزی خطی زیر خواهد بود:

$$Min \sum_{(v_i,v_j)\in E} x_{ij}E[\xi_{ij}]$$

subject to

$$\sum_{v_j:(v_i,v_j)\in E} x_{ij} - \sum_{v_j:(v_j,v_i)\in E} x_{ji} = \begin{cases} 1, & v_i = v_1, \\ 0, & v_i \in V\backslash\{v_1, v_n\}, \\ -1, & v_i = v_n. \end{cases} \quad (۶)$$

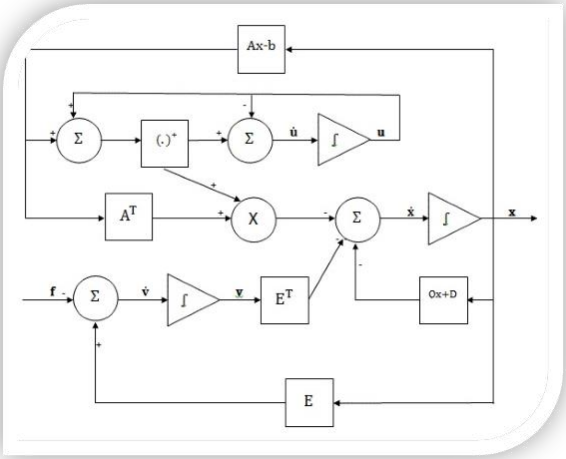
$$x_{ij} = \{\mathbf{0}, \mathbf{1}\} \qquad \forall\ (v_i, v_j) \in \mathrm{E}.$$

در هر سه قضیه فوق با تبدیل مسئله به معادل قطعی آن در حالات خاص ماغیرهای نامطمئن، به مدلهای برنامه ریزی خطی می رسیم که برای حل آم مدل شبکه عصبی زیر پیشنهاد می شود، این مدل در حل مسائل کوتاهترین مسیر و حداکثر جریان در [6] و همچنین در فضای نامطمئن برای حل مسائل انتخاب پرتفوی بهینه در [27] مورد استفاده قرار گرفته و همگرایی و پایداری آن اثبات و همچنین کارایی آن مورد بررسی قرار گرفته است.

۴.۱. مدل شبکه عصبی

مسئله کلی زیر را در نظر بگیرید:

$$\begin{aligned} \text{Min} \quad & C^T x \\ \text{s.t.} \quad & \\ & Ax - b \le 0 \\ & Ex - g = 0 \end{aligned}$$



که در آن $b \in \mathbb{R}^m$ و $g \in \mathbb{R}^l$ و $x \in \mathbb{R}^n$ و $E \in \mathbb{R}^{l\times n}$ و $A \in \mathbb{R}^{m\times n}$.

مدل زیر را می توان برای بدست آوردن جواب بهینه این مسائل و دوگان آن بکار برد:

$$\begin{cases} \dfrac{dx}{dt} = -(C + A^T(u + Ax - b)^+ + E^T v), \\ \dfrac{du}{dt} = (u + Ax - b)^+ - u, \\ \dfrac{dv}{dt} = (Ex - g), \end{cases}$$

که در آن $(u + Ax - b)^+ = ([(u + Ax - b)_1]^+, [(u + Ax - b)_2]^+, \dots, [(u + Ax - b)_m]^+)$ و $[(u + Ax - b)_k]^+ = \max\{(u + Ax - b)_k, 0\}, \quad k = 1,2, \dots, m$ می باشند.

۵. مثال عددی

در این بخش، یک مثال عینی برای توضیح روش‌هایی که در بالا توضیح داده شد، ارائه می‌شود

یک متغیر نامطمئن ξ خطی نامیده می شود و با نماد $L(a,b)$ نشان داده می شود، اگر دارای توزیع نامطمئن خطی به فرم زیر باشد:

$$\Phi(x) = \begin{cases} 0 & x \le a, \\ \dfrac{x-a}{b-a} & a < x \le b, \\ 1 & x > b. \end{cases}$$

که در آن a و b اعداد حقیقی با شرط $a < b$ هستند. و توزیع وارون نامطمئن آن به صورت $\Phi^{-1}(\alpha) = (1-\alpha)a + \alpha b$ است.

فرض کنید $\xi_1, \xi_2, \ldots, \xi_n$ متغیرهای خطی نامطمئن مستقل با $L(a_1, b_1), L(a_2, b_2), \ldots, L(a_n, b_n)$ باشند. از آنجایی که تابع $f(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n$ نسبت به $x_1, x_2, \ldots, x_n$ اکیدا صعودی است، لذا $\sum_{i=1}^{n} x_i$ نیز یک متغیر خطی نامطمئن $L(\sum_{i=1}^{n} a_i \ , \sum_{i=1}^{n} b_i)$ است.

برای راحتی، فرض می کنیم که همه متغیرهای نامطمئن در جدول ۲، متغیرهای خطی نامطمئن مستقل هستند که در جدول ۳ فهرست شده است.

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	-	$L(2,4)$	$L(5,10)$	$L(2,3)$	$L(6,12)$	$L(10,20)$
v_2	$L(2,4)$	-	$L(1,3)$	$L(4,8)$	$L(1,4)$	$L(5,10)$
v_3	$L(5,10)$	$L(1,3)$	-	$L(7,12)$	$L(2,5)$	$L(2,4)$
v_4	$L(2,3)$	$L(4,8)$	$L(7,12)$	-	$L(3,4)$	$L(6,12)$
v_5	$L(6,12)$	$L(1,4)$	$L(2,5)$	$L(3,4)$	-	$L(1,4)$
v_6	$L(10,20)$	$L(5,10)$	$L(2,4)$	$L(6,12)$	$L(1,4)$	-

جدول ۳. فهرست ξ_{ij} ها

ابتدا مسیر با اندازه حداقل ریسک را برای $x_0 = 10$ می یابیم. برای هر ξ_{ij} توزیع وارون نامطمئن $\Phi_{ij}^{-1}(1-\alpha)$ که در جدول ۴ آمده است را محاسبه می کنیم.

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	-	$4-2\alpha$	$10-5\alpha$	$3-\alpha$	$12-6\alpha$	$20-10\alpha$
v_2	$4-2\alpha$	-	$3-2\alpha$	$8-4\alpha$	$4-3\alpha$	$10-5\alpha$
v_3	$10-5\alpha$	$3-2\alpha$	-	$12-7\alpha$	$5-3\alpha$	$4-2\alpha$
v_4	$3-\alpha$	$8-4\alpha$	$12-7\alpha$	-	$4-\alpha$	$12-6\alpha$
v_5	$12-6\alpha$	$4-3\alpha$	$5-3\alpha$	$4-\alpha$	-	$4-3\alpha$
v_6	$20-10\alpha$	$10-5\alpha$	$4-2\alpha$	$12-6\alpha$	$4-3\alpha$	-

جدول ۴. فهرست $\Phi_{ij}^{-1}(1-\alpha)$ ها

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	-	3.8	9.5	2.9	11.4	19
v_2	3.8	-	2.8	7.6	3.7	9.5
v_3	9.5	2.8	-	11.5	4.7	3.8
v_4	2.9	7.6	11.5	-	3.9	11.4
v_5	11.4	3.7	4.7	3.9	-	3.7
v_6	19	9.5	3.8	11.4	3.7	-

جدول ۵. فهرست $\Phi_{ij}^{-1}(0.9)$ ها

حال با حل مدل ۲ برای مسئله فوق طبق داده های به دست آمده در جداول، و با استفاده از مدل شبکه عصبی بیان شده برای حل این مسئله برنامه ریزی خطی، مسیر دارای حداقل اندازه ریسک به صورت $v_1 \to v_2 \to v_3 \to v_6$ به دست می آید و اندازه نامطمئن برای وقوع زیان بیش از ۱۰ برابر با $\frac{1}{6}$ به دست می آید.

حال با حل مدل ۴ برای $\alpha = 0.1$ با کمک شبکه عصبی مطرح شده، مسیر با حداقل ارزش در معرض ریسک به صورت $v_1 \to v_2 \to v_3 \to v_6$ به دست می آید که در آن $l(P)_{VaR}(0.1) = 10.4$. و با تغییر از ۰.۱ تا ۰.۹ مسیرهای با حداقل ارزش درمعرض ریسک مطابق جدول ۶ به دست می آیند.

همچنین با حل مدل ۶ با توجه به ارزش مورد انتظار $E[\xi_{ij}]$ محاسبه شده در جدول ۷ و به کمک شبکه عصبی پیشنهادی، مسیر با ریسک مورد انتظار حداقل به دو صورت $v_1 \to v_2 \to v_3 \to v_6$ و $v_1 \to v_2 \to v_5 \to v_6$ به دست می آید، که زیان مورد انتظار به وقوع پیوسته $\mathrm{E}[l(\mathrm{P})] = 8$ است

α	مسیر با حداقل ارزش در معرض ریسک	$l(P)_{VaR}(\alpha)$
0.1	$v_1 \to v_2 \to v_3 \to v_6$	**10.4**
0.2	$v_1 \to v_2 \to v_3 \to v_6$	**9.8**
0.3	$v_1 \to v_2 \to v_3 \to v_6$	**9.2**
0.4	$v_1 \to v_2 \to v_3 \to v_6$	**8.6**
0.5	$v_1 \to v_2 \to v_5 \to v_6$	**8**
0.6	$v_1 \to v_2 \to v_5 \to v_6$	**7.2**
0.7	$v_1 \to v_2 \to v_5 \to v_6$	**6.4**
0.8	$v_1 \to v_2 \to v_5 \to v_6$	**5.6**
0.9	$v_1 \to v_2 \to v_5 \to v_6$	**4.8**

جدول ۶. فهرست $l(P)_{VaR}(\alpha)$ ها

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	-	**3**	**7.5**	**2.5**	**9**	**15**
v_2	**3**	-	**2**	**6**	**2.5**	**7.5**
v_3	**7.5**	**2**	-	**9.5**	**3.5**	**3**
v_4	**2.5**	**6**	**9.5**	-	**3.5**	**9**
v_5	**9**	**2.5**	**3.5**	**3.5**	-	**2.5**
v_6	**15**	**7.5**	**3**	**9**	**2.5**	-

جدول ۷. فهرست $\mathrm{E}[\xi_{ij}]$ ها

۶. نتیجه‌گیری

در این مقاله مسئله انتخاب مسیر حداقل ریسک، در یک شبکه نامطمئن توصیف شده و با فرض اینکه زیان‌های به وقوع پیوسته، متغیرهای نامطمئن هستند، ابتدا سه نوع شاخص ریسک نامطمئن را ارائه داده و پس از آن، برخی از مدل‌های

برنامه‌ریزی ریسک نامطمئن، بر اساس شاخص‌های ریسک پیشنهادی ایجاد گردید. برای به دست آوردن حداقل مسیر ریسک، این مدل‌های برنامه‌ریزی نامطمئن را به حالت خاص قطعی متغیرهای نامطمئن متناظر آن‌ها تبدیل می‌کنیم که مسائل برنامه ریزی خطی حاصل می شود و با کمک یک مدل شبکه عصبی کارا به حل مسائل به دست آمده پرداختیم. در نهایت با ارائه یک مثال عددی، کارایی مدل ها نشان داده شده است.

۷. مراجع

[1] M. Abkowitz, M. Lepofsky, P. Cheng, "Selecting criteria for designating hazardous materials highway routes". *Transp Res Rec* 1333, pp. 30–35, 1992.
[2] E. Erkut, V. Verter, "A framework for hazardous materials transport risk assessment". *Risk Anal* 15(5):589–601, 1995.
[3] E. Erkut, V. Verter, "Modeling of transport risk for hazardous materials". *Oper Res* 46(5):625–642, 1998.
[4] J. Díaz-Báñez, F. Gómez, G. Toussaint, "Computing shortest paths for transportation of hazardous materials incontinuous spaces". *J Food Eng* 70(3): pp. 293–298, 2005.
[5] A. R. Nazemi, F. Omidi, "An efficient dynamic model for solving the shortest path problem", *Transportation Research Part C*, 26:1-19.۲۰۱۳ ,
[6] A. R. Nazemi, F. Omidi, "A capable neural network model for solving the maximum flow problem", *Journal of Computational and Applied Mathematics*, 236:3498-3513, 2012.
[7] B. Liu, Uncertain Theory, 2nd edn. Springer, Berlin, 2007.
[8] B. Liu, "Fuzzy process, hybrid process and uncertain process". *J Uncertain Syst* 2:3–16, 2008
[9] B. Liu, "Uncertain set theory and uncertain inference rule with application to uncertain control". *J Uncertain Syst* 4(2):83–98, 2010a.
[10] B. Liu, "Uncertain risk analysis and uncertain reliability analysis". J Uncertain Syst 4(3):163–170, 2010b.
[11] B. Liu, Uncertainty theory: a branch of mathematics for modeling human uncertainty. Springer, Berlin, 2010c.
[12] B. Zhang, J. Peng, "Euler index in uncertain graph". *Appl Math Comput* 218(20):10279–10288, 2012a.
[13] **B.** Zhang, J. Peng, "Uncertain programming model for Chinese postman problem with uncertain weights". *Ind Eng Manag Syst* 11(1):18–25, 2012b.
[14] X. Gao, Y. Gao, "Connectedness index of uncertain graphs". *Int J Uncertain Fuzziness Knowl Based Syst* 21(1):127–137, 2013.
[15] X. Gao, L. Jia, S. Kar, "A new definition of cross-entropy for uncertain variables". *Soft Comput* 22(17):5617–5623, 2018.
[16] B. Liu B, "Some research problems in uncertainty theory". *J Uncertain Syst* 3(1):3–10, 2009a.
[17] B. Liu, Theory and practice of uncertain programming, 2nd edn. Springer, Berlin, 2009b.
[18] B. Liu, "Extreme value theorems of uncertain process with application to insurance risk model". *Soft Comput*, 17(4):549–556, 2013b.
[19] S. Li, J. Peng, B. Zhang, "The uncertain premium principle based on the distortion function". *Insur Math Econ* 53(2):317–324, 2013.

[20] Z. Qin, "Uncertain random goal programming". *Fuzzy Optim Decis Mak* 17(4):375–386, 2018.
[21] Y. Gao, "Shortest path problem with uncertain arc lengths". *Comput Math Appl* 62(6):2591–2600, 2011.
[22] S. Ding, "Uncertain minimum cost ow problem". *Soft Comput*, 18 (11):2201–2207, 2014.
[23] S. Han, Z. Peng, S. Wang, "The maximum flow problem of uncertain network". *Inf Sci* 265:167–175, 2014.
[24] J. Peng, "Risk metrics of loss function for uncertain system". *Fuzzy Optim Decis Mak* 12(1):53–64, 2013.
[25] Y. Liu, DA. Ralescu, "Expected loss of uncertain random system". *Soft Comput* 22(17):5573–5578, 2018.
[26] V. Verter, B. Kara, "A path-based approach for hazmat transport network design". *Manag Sci* 54(1):29–40, 2008.
[27] F. Omidi, B. Abbasi, AR. Nazemi, "An efficient dynamic model for solving a portfolio selection with uncertain chance constraint models", *Journal of Computational and Applied Mathematics*, 319: 43–55, 2017.

I4CPAPERS-064
9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Extremal Sombor Index of Cactus Graphs with Pendant Edges: Starburst, Sparkle, Sun, and Broken Sun Graphs

Maryam Mohammadi, Hasan Barzegar
Department of Mathematics, Tafresh University, Tafresh 39518−79611, Iran
mohamadi.math01@gmail.com; barzegar@tafreshu.ac.ir

ABSTRACT

In this paper, we study a group of cactus graphs with specific pendant edge structures, including starburst, sparkle, sun, and broken sun graphs. Our primary focus is on deriving the extremal Sombor index of these graphs, motivated by their relevance in various scientific fields such as chemical science. The Sombor index, introduced by Ivan Gutman, serves as a powerful topological descriptor for predicting physicochemical properties of molecules. This work extends prior research by offering novel insights into the Sombor index calculations by analyzing chemical structures. We state the utility of these indices in studying the physicochemical behavior of molecular compounds, emphasizing their predictive power in chemical contexts.

KEYWORDS: Extermal Sombor Index, Cactus Graphs, Starburst, Sparkle, and Sun Graphs

1 INTRODUCTION

Topological indices are mathematical tools that have been extensively used to predict the physicochemical properties of molecular structures. Among these, the Sombor index has gained significant attention due to its affect in correlating molecular graphs with chemical properties. The Sombor index has been studied in numerous contexts such as the references [1], [2] and [3], including trees and specific types of cactus chain graphs.
Cactus graphs represent a particular class of graphs for studying topological indices. Within this class, graphs with pendant edges, such as starburst, sparkle, sun, and broken sun graphs, have particular importance. These graphs are not only significant in theoretical studies but also have practical applications in chemical science, data science, optimization, and programming. Understanding the extremal properties of the Sombor index in these graphs can lead to better predictions and insights into molecular behavior and other complex systems.

This study distinguishes itself by introducing and examining a comprehensive set of cactus graphs in the context of their extremal Sombor indices. Unlike prior works that primarily focused on trees and simple molecular graphs, this research highlights how pendant edge structures in cactus graphs impact the Sombor index. Specifically, we derive explicit formulas and present comparative analyses for this index, providing a deeper understanding of its behavior across various graph families. Additionally, the innovative application of this index to aromatic hydrocarbons and molecular property predictions sets this work apart, offering a new framework for analyzing molecular stability and boiling points using topological indices.

This is to inform you that this paper and its applications in aromatics been made in the preprint at the following internet address (URL):
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5014969.

Let G be a graph with n vertices and m edges, then the Sombor index is defined as

$$SO(G) = \sum_{uv \in E(G)} \sqrt{d^2(u) + d^2(v)}. \quad (1)$$

2 THE SOMBOR INDEX OF STARBURST CHAIN GRAPHS

In [4], a *cactus graph* has been defined as a connected graph such that no two cycles of G have any common edge. A *starburst chain graph* is a cactus graph consisting of C cycles, where all cycles are of type C_P with $p \geq 3$. In this graph, each cycle is adjacent to at most two other cycles, and every other vertex has two pendant edges (see for example Figures 1).

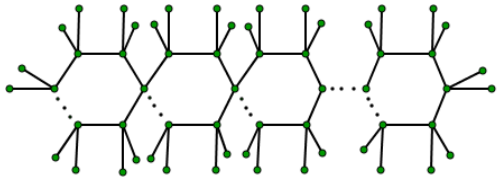


Figure 1**:** Cactus chain graph G for $P > 3$ and $C \geq 1$

Theorem 1 *Let G be a starburst chain graph with C cycles, where all cycles are C_P. Then,*

$$SO(G) = (4\sqrt{2}P + 2\sqrt{17}P - 4\sqrt{17})C + 4\sqrt{17} \quad \forall\, C \geq 1, \forall\, P \geq 3, \quad (2)$$

Proof. By mathematical induction on P.

Remark *As you notice, $\frac{\partial SO(G)}{\partial C} > 0$ for each $C \geq 1$ and $\frac{\partial SO(G)}{\partial P} > 0$ for each $P \geq 3$ so with arising C and P the Sombor index is increasing.*

3 THE SOMBOR INDEX OF THE SPARKLE GRAPHS

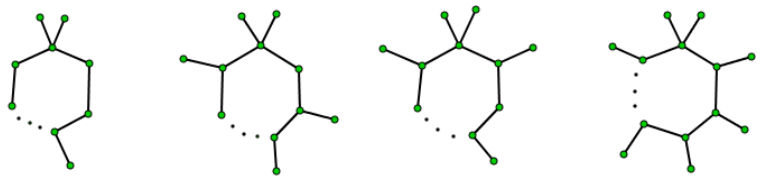


Figure 2**:** Some sparkle graphs with p sides

A unicyclic graph is a connected graph containing exactly one cycle. Some authors have studied the Sombor index and other indices in some articles such as [1], [3] and [5] for specific unicyclic graphs. Here, we name a group of these unicyclic graphs as *sparkle graphs* and define it as a graph containing a cycle where one of its vertices has two pendent vertices and its other vertices could have one pendant vertex or not which we put the number of such vertices equal with r (see Figure 2). Sparkle graphs are denoted by $H_{1,r}$ and the set of all $H_{1,r}$s with n vertices is denoted by CY_n. For an sparkle graph $H_{1,r}$, let n_d indicates the vertices number of degree $d \leq 4$ in the graph and $m_{d,d'}$ indicates the number of edges with ends vertices degree d and d'. Then $n_1 + n_2 + n_3 + n_4 = n$, $\Sigma m_{d,d'} = 2m$ and

$$SO(H_{1,r}) = 5m_{4,3} + 2\sqrt{5}m_{4,2} + 3\sqrt{2}m_{3,3} + \sqrt{13}m_{2,3} \quad (3)$$

in which $m_{4,1} = 2$ and $m_{3,1} = r$.

It is easy to verify that for every $r \in \mathbb{N}_0$, the table of the vertex degree distribution for the graph $H_{1,r}$ corresponds to Table ١.

Table ١ Vertex degree distribution for graphs $H_{1,r}$

	n_4	n_3	n_2	n_1
$H_{1,r}$	1	$\forall\, r\ 0 \le r \le p-1$	$p-(1+r)$	$2+r$

In the following lemma, we show that the table of the edges distribution for the sparkle graphs is as Table ٢.

Table ٢ Edge distribution in graph $H_{1,r} \in CY_n$ for each $r \in \mathbb{N}_0$ and $0 \le m_{3,3} \le r-1$.

	$m_{4,3}$	$m_{4,2}$	$m_{4,1}$	$m_{3,3}$	$m_{3,2}$	$m_{3,1}$	$m_{2,2}$
$H_{1,r}$	0	2	2	$m_{3,3}$	$2(r-m_{3,3})-0$	r	$n-(3r-m_{3,3}+4)$
	1	1	2	$m_{3,3}$	$2(r-m_{3,3})-1$	r	$n-(3r-m_{3,3}+3)$
	2	0	2	$m_{3,3}$	$2(r-m_{3,3})-2$	r	$n-(3r-m_{3,3}+2)$

Lemma 2 *The table of the edge distribution for the sparkle graphs is shown in Table* (4).

Proof. It is easily seen that $m_{4,3}$ can only take the values of 0, 1 or 2 and by having different values of $m_{4,3}$, one can easily obtain different values of $m_{4,1}$ and $m_{4,2}$. Now we show that for each $r \in \mathbb{N}_0$ and for values p with a fixed $m_{3,3}$ always $m_{3,2} = 2(r-m_{3,3})-0$ or $m_{3,2} = 2(r-m_{3,3})-1$ or $m_{3,2} = 2(r-m_{3,3})-2$. Indeed, at first, the problem is proved directly for $r=0$ and $r=1$:

If $r=0$, then $m_{4,3}=0$ and hence $m_{2,3}=0=2(0-0)-0$.

If $r=1$ then $m_{4,3}=0$ or $m_{4,3}=0$ and hence $m_{2,3}=2=2(1-0)-0$ or $m_{2,3}=1=2(1-0)-1$, respectivily.

Now the mathematical induction is applied on $r \ge 2$ and we leave it to the reader.

Equalities and inequalities make a good prediction of molecular physicochemical properties can be seen in [2] and [6]. Here by applying equation (3) and Lemma 2, we have

Theorem 3 *For every* $r \in \mathbb{N}_0$, $p \ge 3$ *and each* $0 \le m_{3,3} \le r-1$,

$$SO(H_{1,r}) = \begin{cases} 2\sqrt{2}n + (2\sqrt{13}+\sqrt{10}-6\sqrt{2})r + (5\sqrt{2}-2\sqrt{13})m_{3,3} + 4\sqrt{5} + 2\sqrt{17} - 8\sqrt{2} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad m_{4,3}=0 \\ 2\sqrt{2}n + (2\sqrt{13}+\sqrt{10}-6\sqrt{2})r + (5\sqrt{2}-2\sqrt{13})m_{3,3} + 5 + 2\sqrt{5} + 2\sqrt{17} - 6\sqrt{2} - \sqrt{13} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad m_{4,3}=1 \\ 2\sqrt{2}n + (2\sqrt{13}+\sqrt{10}-6\sqrt{2})r + (5\sqrt{2}-2\sqrt{13})m_{3,3} + 10 + 2\sqrt{17} - 2\sqrt{13} - 4\sqrt{2} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad m_{4,3}=2, \end{cases} \quad (4)$$

Theorem 4 *Let* $H_{1,r}$ *be a sparkle graph with* $r \ge 2$ *and* A_p *be the set of all sparkle graphs with* p *vertices in the cycle. In the following cases* $H_{1,r} \in A_p$ *has the maximum* (*minimum*) *Sombor index if and only if* $m_{3,3}=0$ ($m_{3,3}=r-1$).

(i) $p \ge 2r+2$ and $m_{4,3}=0$.

(ii) $p \ge 2r+1$ and $m_{4,3}=1$.

(iii) $p \geq 2r$ and $m_{4,3} = 2$.

Proof. Based on the equation (4), since $5\sqrt{2} - 2\sqrt{13} < 0$, $H_{1,r} \in A_p$ has the maximum (minimum) Sombor index if and only if $m_{3,3} = 0$ ($m_{3,3} = r - 1$).

Theorem 5 *Let $H_{1,r}$ be a sparkle graph with $r \geq 2$ and A_p be the set of all sparkle graphs with p vertices in the cycle.*

(i) If $r + 3 \leq p < 2r + 2$ and $m_{4,3} = 0$, then $H_{1,r} \in A_p$ has the maximum (minimum) Sombor index if and only if $m_{3,3} = 2r + 2 - p$ ($m_{3,3} = r - 1$).

(ii) If $r + 2 \leq p < 2r + 1$ and $m_{4,3} = 1$, then $H_{1,r} \in A_p$ has the maximum (minimum) Sombor index if and only if $m_{3,3} = 2r + 1 - p$ ($m_{3,3} = r - 1$).

(iii) $r + 2 \leq p < 2r$ and $m_{4,3} = 2$, then $H_{1,r} \in A_p$ has the maximum (minimum) Sombor index if and only if $m_{3,3} = 2r - p$ ($m_{3,3} = r - 1$).

Proof. (i) Let $A \subseteq CY_{\mathrm{n}}$ be the set of sparkle graphs with $p = 2r + 1$ and $m_{4,3} = 0$. It is not difficult to check that for each graph in A, $m_{3,3} \neq 0$. Now replace one edge $m_{3,3}$ of the cycle of each graph in A with a path of length two, the new set of sparkle graphs is denoted by A_1 with $p_0 = 2r + 2$. Then by Theorem 4(i), the sparkle graph $G \in A_1$ has the maximum Sombor index if and only if $m_{3,3} = 0$. Now, we replace the same path of length 2 again with an edge so that the set A is obtained again. So the maximum (minimum) Sombor index occurs in A if and only if $m_{3,3} = 1 = p_0 - p$ ($m_{3,3} = r - 1$). Now let $A \subseteq CY_{\mathrm{n}}$ be the set of sparkle graphs with $p = 2r$ and $m_{4,3} = 0$. By replacing two edges $m_{3,3}$ of the cycle of each graph in A with a path of length two, the new set of sparkle graphs is denoted by A_2 with $p_0 = 2r + 2$. Then by Theorem 4(i), the sparkle graph $G \in A_2$ has the maximum Sombor index if and only if $m_{3,3} = 0$. Now, we replace each of the same paths of length 2 again with an edge so that the set A is obtained again such that for each graph in A, $m_{3,3} \geq 2$. So the maximum (minimum) Sombor index occurs in A if and only if $m_{3,3} = 2 = p_0 - p$ ($m_{3,3} = r - 1$). Continuing this process and after a finite number, let $A \subseteq CY_{\mathrm{n}}$ be the set of sparkle graphs with $p = r + 3$ and $m_{4,3} = 0$. Now replace $r - 1$ edges $m_{3,3}$ of the cycle of each graph in A with a path of length two, the new set of sparkle graphs is shown by A_{r-1} with $p_0 = 2r + 2$. Then by Theorem 4(i), the sparkle graph $G \in A_{r-1}$ has the maximum Sombor index if and only if $m_{3,3} = 0$. Now, by replacing each of the same paths of length 2 with an edge again, we obtain the set A such that for each graph in A, $m_{3,3} \geq r - 1$. Thus the maximum (minimum) Sombor index occurs in A if and only if $m_{3,3} = r - 1 = p_0 - p$ ($m_{3,3} = r - 1$).

Similarly, using Theorems 4(ii) and 4(iii), parts (ii) and (iii) can be proven.

To better understand Theorems 3 and 4, see Table 3.

Table 3: Induction steps on r in graph $H_{1,r} \in CY_n$ ($n = p + r + 2$) and edge distribution.

$H_{1,r}$	p	$n = p + r + 2$	$m_{4,3}$	$m_{4,2}$	$m_{4,1}$	$m_{3,3}$	$m_{3,2}$	$m_{3,1}$	$m_{2,2}$
$H_{1,0}$	$3, 4, 5, \ldots$	$p + 2$	0	2	2	0	0	0	n-4
$H_{1,1}$	$4, 5, 6, \ldots$	$p + 3$	0	2	2	0	2	1	n-7
$H_{1,1}$	$3, 4, 5, \ldots$	$p + 3$	1	1	2	0	1	1	n-6
$H_{1,2}$	$6, 7, 8, \ldots$	$p + 4$	0	2	2	0	4	2	n-10
$H_{1,2}$	$5, 6, 7, \ldots$	$p + 4$	1	1	2	0	3	2	n-9
$H_{1,2}$	$4, 5, 6, \ldots$	$p + 4$	2	0	2	0	2	2	n-8
$H_{1,2}$	$5, 6, 7, \ldots$	$p + 4$	0	2	2	1	2	2	n-9
$H_{1,2}$	$4, 5, 6, \ldots$	$p + 4$	1	1	2	1	1	2	n-8
$H_{1,2}$	3	$p + 4$	2	0	2	1	0	2	n-7
$H_{1,3}$	$8, 9, 10, \ldots$	$p + 5$	0	2	2	0	6	3	n-13
$H_{1,3}$	$7, 8, 9, \ldots$	$p + 5$	1	1	2	0	5	3	n-12

$H_{1,3}$	$6,7,8,\ldots$	$p+5$	2	0	2	0	4	3	n-11
$H_{1,3}$	$7,8,9,\ldots$	$p+5$	0	2	2	1	4	3	n-12
$H_{1,3}$	$6,7,8,\ldots$	$p+5$	1	1	2	1	3	3	n-11
$H_{1,3}$	$5,6,7,\ldots$	$p+5$	2	0	2	1	2	3	n-10
$H_{1,3}$	$6,7,8,\ldots$	$p+5$	0	2	2	2	2	3	n-11
$H_{1,3}$	$5,6,7,\ldots$	$p+5$	1	1	2	2	1	3	n-10
$H_{1,3}$	4	$p+5$	2	0	2	2	0	3	n-9
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$H_{1,s-1}$	$2s, 2s+1,..$	$p+s+1$	0	2	2	0	$2(s-1)-0$	$s-1$	n-(3s+1)
$H_{1,s-1}$	$2-1,2s,\ldots$	$p+s+1$	1	1	2	0	$2(s-1)-1$	$s-1$	n-3s
$H_{1,s-1}$	$2-2,2s-1,\ldots$	$p+s+1$	2	0	2	0	$2(s-1)-2$	$s-1$	n-(3s-1)
$H_{1,s-1}$	$2s-1,2s,\ldots$	$p+s+1$	0	2	2	1	$2(s-1-1)-0$	$s-1$	n-3s
$H_{1,s-1}$	$2s-2,2s-1,\ldots$	$p+s+1$	1	1	2	1	$2(s-1-1)-1$	$s-1$	n-(3s-1)
$H_{1,s-1}$	$2s-3,2s-2,\ldots$	$p+s+1$	2	0	2	1	$2(s-1-1)-2$	$s-1$	$n-(3s-2)$
$H_{1,s-1}$	$2s-2,2s-1,\ldots$	$p+s+1$	0	2	2	2	$2(s-1-2)-0$	$s-1$	$n-(3s-1)$
$H_{1,s-1}$	$2s-3,2s-2,\ldots$	$p+s+1$	1	1	2	2	$2(s-1-2)-1$	$s-1$	$n-(3s-2)$
$H_{1,s-1}$	$2s-4,2s-3,\ldots$	$p+s+1$	2	0	2	2	$2(s-1-2)-2$	$s-1$	$n-(3s-3)$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$H_{1,s-1}$	$s+3,s+4,\ldots$	$p+s+1$	0	2	2	$s-1-2$	4	$s-1$	$n-(2s+4)$
$H_{1,s-1}$	$s+2,s+3,\ldots$	$p+s+1$	1	1	2	$s-1-2$	3	$s-1$	$n-(2s+3)$
$H_{1,s-1}$	$s+1,s+2,\ldots$	$p+s+1$	2	0	2	$s-1-2$	2	$s-1$	$n-(2s+2)$
$H_{1,s-1}$	$s+2,s+3,\ldots$	$p+s+1$	0	2	2	$s-1-1$	2	$s-1$	$n-(2s+3)$
$H_{1,s-1}$	$s+1,s+2,\ldots$	$p+s+1$	1	1	2	$s-1-1$	1	$s-1$	$n-(2s+2)$
$H_{1,s-1}$	s	$p+s+1$	2	0	2	$s-1-1$	0	$s-1$	$n-(2s+1)$

4 THE SOMBOR INDEX OF SUN GRAPHS AND BROKEN SUN GRAPHS

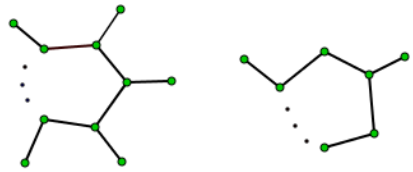


Figure ٣: Sun graph and broken sun graph

The graph G is called a *sun graph* with $n = 2p$ vertices ($p \in \mathbb{N}$) when it is formed by adding one pendant vertex to each of the vertices of a p-cyclic graph. Also, it is named a *broken sun* graph when it is a unicyclic subgraph of a sun graph (see Figure ٣). Here these graphs are shown by H_r such that r is the number of the pendant edges (if $r = p$, then H_r is a sun graph). The set of all broken sun graphs H_r with n vertices and r pendant edges ($r \in \mathbb{N}_0$) is denoted by CU_n. In this case, the vertex degree distribution table for these graphs is given in Table 4 and the edge distribution table is given in Table 5. So the Sombor index is as the following:

$$SO(H_r) = 3\sqrt{2}m_{3,3} + \sqrt{13}m_{2,3} + \sqrt{10}m_{1,3} + 2\sqrt{2}m_{2,2}, \quad (5)$$

in which $m_{3,1} = r$.

Table 4: Vertex degree distribution in graphs $H_r \in CU_n$.

n_d	n_1	n_2	n_3
H_r	r	$n-2r$	r

Table 5: Table of edge distribution in graphs $H_r \in CU_n$ for each $r \in \mathbb{N}_0$ and $0 \leq m_{3,3} \leq r$.

$m_{d,d'}$	$m_{3,3}$	$m_{2,3}$	$m_{1,3}$	$m_{2,2}$
H_r	$m_{3,3}$	$2(r-m_{3,3})$	r	$n-(3r-m_{3,3})$

Lemma 3 *For each $H_r \in CU_n$ of broken sun graphs with n vertices, the table of the edge distribution with r -pendant vertices is as Table* 5.

Proof. First, we prove that for each graph $H_r \in CU_n$ with a fixed $m_{3,3}$, $m_{2,3} = 2(r-m_{3,3})$. To do this, note that every pending edge that is not adjacent to an edge of the kind $m_{3,3}$ is adjacent to two $m_{2,3}$ edges. Additionally, each set of edges of the type $m_{3,3}$ that are adjacent and their number is l can be attributed to $l+1$ pending edges and two $m_{2,3}$ edges. Therefore, we can conclude $m_{2,3} = 2(r-m_{3,3})$. Also since $m_{3,3} + m_{1,3} + m_{2,3} + m_{2,2} = n$, then $m_{2,2} = n - m_{3,3} - m_{1,3} - m_{2,3} = n - m_{3,3} - r - 2r + 2m_{3,3} = n - (3r - m_{3,3})$.

Now, we obtain the following theorem by using equation (5) and Lemma 3.

Theorem 6 *For each $r \in \mathbb{N}_0$, $p \geq 3$ and $0 \leq m_{3,3} \leq r$, we have*

$$SO(H_r) = 2\sqrt{2}n + (5\sqrt{2} - 2\sqrt{13})m_{3,3} + (2\sqrt{13} + \sqrt{10} - 6\sqrt{2})r, \quad (6)$$

To better understand Theorem 7, one could see Table 6.

Theorem 7 *Let H_r be a broken sun graph with $r \in \mathbb{N}_0$ and A_p be the set of all broken sun graphs with p vertices in the cycle.*

(i) For $0 \leq r \leq 1$ and $p \geq 3$, $H_r \in A_P$ has maximum (minimum) Sombor index if and only if $m_{3,3} = 0$ ($m_{3,3} = 0$).

(ii) For $r \geq 2$,

a) If $p \geq 2r$, then $H_r \in A_p$ has maximum (minimum) Sombor index if and only if $m_{3,3} = 0$ ($m_{3,3} = r-1$).

b) If $r < p < 2r$, then $H_r \in A_p$ has maximum (minimum) Sombor index if and only if $m_{3,3} = 2r - p$ ($m_{3,3} = r-1$).

c) If $p = r$, then $H_r \in A_p$ has maximum (minimum) Sombor index if and only if $m_{3,3} = r$ ($m_{3,3} = r$).

Proof. (i) If H_r be a broken sun graph with $r = 0$ or $r = 1$ then for $p \geq 3$ the graph $H_r \in A_P$ has both maximum and minimum Sombor index if and only if $m_{3,3} = 0$ ($m_{3,3} = 0$).

(ii) For $r \geq 2$,

a) Since $p \geq 2r$, so $0 \leq m_{3,3} \leq r-1$. Now with attention to the equation (6) whereas the coefficient of $m_{3,3}$, $5\sqrt{2}-2\sqrt{13}$, is a negative number, so $SO(G)$ is maximum (minimum) if and only if $m_{3,3}=0$ ($m_{3,3}=r-1$).

b) With attention to the part (i) if G is a broken sun graph with $p_0=2r$ and with maximum $SO(G)$, so $m_{3,3}=0$, now if remove one vertex of the cycle, then the number of the cycle's vertices is $p=p_0-1=2r-1$. So in a new graph G' two pendant edges would be adjacent and based on the relation (6) G' has the maximum (minimum) Sombor index if and only if $m_{3,3}=1=p_0-p=2r-(2r-1)$ ($m_{3,3}=r-1$). By keeping on this process and for other graphs, after a finite number, removing $r-1$ vertices and considering the new graph G' with $p=p_0-(r-1)=2r-(r-1)=r-1$, $r-1$ pendant edges also would be adjacent and necessarily the graph G' would have the maximum (minimum) Sombor index if and only if $m_{3,3}=r-1=p_0-p=2r-(2r-(r-1))=r-1$ ($m_{3,3}=r-1$).

c) In this case, H_r is a sun graph and as a result $m_{3,3}=r$.

To better understand Theorem 7, see the following table.

Table 6: Induction table on number of pendant edges r for $H_r \in CU_n$.

H_r	$m_{3,3}$	p	$n=p+r$	$m_{2,3}$	$m_{1,3}$	$m_{2,2}$
H_0	0	$3,4,5,\ldots$	p	0	0	n
H_1	0	$3,4,5,\ldots$	$p+1$	2	1	$n-3$
H_2	0	$4,5,6,\ldots$	$p+2$	4	2	$n-6$
H_2	1	$3,4,5,\ldots$	$p+2$	2	2	$n-5$
H_3	0	$6,7,8,\ldots$	$p+3$	6	3	$n-9$
H_3	1	$5,6,7,\ldots$	$p+3$	4	3	$n-8$
H_3	2	$4,5,6,\ldots$	$p+3$	2	3	$n-7$
H_3	3	3	$p+3$	0	3	$n-6$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
H_{r-1}	0	$2(r-1),2(r-1)+1,\ldots$	$p+r$	$2(r-1)$	$r-1$	$n-(3r-3)$
H_{r-1}	1	$[2(r-1)-1],[2(r-1)],\ldots$	$p+r$	$2(r-1)-2$	$r-1$	$n-(3r-4)$
H_{r-1}	2	$[2(r-1)-2],[2(r-1)-1],\ldots$	$p+r$	$2(r-1)-4$	$r-1$	$n-(3r-5)$
H_{r-1}	3	$[2(r-1)-3],[2(r-1)-2],\ldots$	$p+r$	$2(r-1)-6$	$r-1$	$n-(3r-6)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
H_{r-1}	$r-1$	$[r-1]$	$p+r$	0	$r-1$	$n-(2r-2)$
H_r	0	$2(r-1)+2,2(r-1)+2+1,\ldots$	$p+r$	$2(r-1)+2$	r	$n-3r$
H_r	1	$[2(r-1)-1]+2,[2(r-1)-1]+2+1,\ldots$	$p+r$	$2(r-1)$	r	$n-(3r-1)$
H_r	2	$[2(r-1)-2]+2,[2(r-1)-2]+2+1,\ldots$	$p+r$	$2(r-1)-2$	r	$n-(3r-2)$
H_r	3	$[2(r-1)-3]+2,[2(r-1)-3]+2+1,\ldots$	$p+r$	$2(r-1)-4$	r	$n-(3r-3)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
H_r	$r-1$	$[r-1]+2,[r-1]+2+1,\ldots$	$p+r$	$2(r-1)-2r$	r	$n-(2r-1)$
H_r	r	$[r-1]+1$	$p+r$	0	r	$n-2r$

5 CONCLUSION

The obtained results provide valuable insights into the behavior of the Sombor index in these specialized graph structures, demonstrating its effectiveness as a predictive tool.

Due to some limitations, we only present main results related to aromatic compounds:

Cycloalkanes serve as examples of the starburst graphs with only one cycle. Analyzing these compounds reveals that the Sombor index values provide a good approximation of the molecular mass (M. Mass) such that $\frac{M.Mass}{SO(G)} = 1.009$.

Our findings on a class of sparkle graphs with one cycle including some cyclohexanes and cyclohexanones indicate that as n increases, the Sombor index also increases. Additionally, for a fixed n and constant $m_{4,3}$, the Sombor index decreases with an increase in $m_{3,3}$.

Furthermore, for the sun and broken sun graphs with benzene ring with a fixed number of pendant edges as -CH_3, increasing $m_{3,3}$ results in a decrease in the Sombor index, while the boiling point increases. Moreover, in this group of graphs, a comparison between the molecular mass and the Sombor index reveals a strong correlation.

This work extends the understanding of the Sombor index beyond its previous applications, providing new methodologies and perspectives for future research. By continuing to explore and refine these indices, we can improve our ability to model and predict complex systems, ultimately advancing scientific knowledge and innovation.

Disclosure of interest: We declare that we have no conflicts of interest to disclose related to the subject matter or findings presented in the manuscript. In the event that a conflict of interest arises during the peer review process or after publication, we will promptly disclose this information to the relevant parties.
Declaration of funding: No funding was received.
Data Availability: The data used to support the findings of this study are included within the article

REFERENCES

[1] S. Alikhani, N. Ghanbari, " Sombor Index of Polymers," Match Communications in Mathematical and in Computer Chemistry. Vol. 86 (2021), pp. 715-728.
[2] K. C Das, A. S.Çevik, I. N. Cangul and Y. Shang, "On Sombor Index. Symmetry," vol. 13 (2021) 140.
[3] N. Ghanbari, S. Alikhani. "Sombor Index of Certain Graphs," Journal of Mathematical Chemistry," vol. 12 (1) (2021), pp. 27-37.
[4] H. Ahmeda, A. A. Bhattia, A. Ali. "Zeroth-order general Randi´c index of cactus graphs," Akce international journal of Graphs and Combinatorics. vol. 16 (2019), pp. 182-189 .
[5] H. Liu, L. You, Y. Huang, "Ordering Chemical Graphs by Sombor Indices and Its Applications," Communications in Mathematical and in Computer Chemistry. Vol. 87 (2022), pp. 5-22.
[6] M. Mohammadi, H. Barzegar, A. R Ashrafi, "Comparisons of the Sombor Index of Alkane, Alkyl, and Annulene Series with Their Molecular Mass," Hindawi: Journal of Chemistry. 2022 (2022).

بهینه سازی الگوریتم KSW در محاسبه دستگاه گربنر

مهدی دهقانی درمیان[1]

گروه ریاضی، دانشگاه ملی مهارت، تهران، ایران

چکیده

در این مقاله الگوریتم KSW را که جزو کارامدترین و موثرترین الگوریتم‌های محاسبه دستگاه گربنر ایده‌آل‌های چندجمله‌ای پارامتری است بهبود می‌دهیم. با حذف سطری از الگوریتم KSW که باعث تولید شاخه‌هایی با پایه‌ی گربنر $\{1\}$ می‌شود و اضافه کردن شاخه‌ی $(\text{other cases}, \{1\})$ به دستگاه گربنر، نه تنها خللی در الگوریتم ایجاد نمی‌شود بلکه با این تغییر تعداد شاخه‌های دستگاه گربنر خروجی کمتر می‌شود و لذا نیازی به بررسی سازگاری شرایط پارامتری آن دسته از شاخه‌هایی که پایه‌ی گربنر $\{1\}$ دارند نیست. با این تغییر ساده و جزیی در الگوریتم KSW، الگوریتمی حاصل می‌شود که از لحاظ تایم مورد نیاز و حافظه‌ی لازم برای محاسبات از الگوریتم اولیه کارامدتر و بهینه‌تر می‌باشد. لازم به ذکر است که این ایده را به‌عنوان نتیجه‌ای فرعی در قالب بخشی از مرجع [۱۴] بیان کرده‌ایم که این مقاله مورد پذیرش قرار گرفته است.

کلمات کلیدی: دستگاه گربنر، الگوریتم KSW، پایه گربنر، الگوریتم $\text{KSW} - \text{Optimized}$، چندجمله‌ای پارامتری.

۱. مقدمه

پای گربنر نوع خاصی از مجموعه مولد یک ایده‌آل چندجمله‌ای و ابزاری قدرتمند در جبر محاسباتی است. پایه های گربنر در سال ۱۹۶۵ همراه با یک الگوریتم (الگوریتم بوخبرگر) برای محاسبه آنها توسط برونو بوخبرگر در رساله دکترایش [۱] معرفی شد. او آنها را به افتخار استاد راهنمایش (ولفگانگ گربنر) پایه گربنر نامگذاری کرد. سپس، در [۲] دو معیار را برای بهبود عملکرد الگوریتم خود پیشنهاد کرد. در سال ۱۹۸۳، لازارد الگوریتمی را برای محاسبه پایه های گربنر با استفاده از تکنیک های جبر خطی [۳] توصیف کرد. بعداً، فوژر دو الگوریتم معروف خود برای محاسبه پایه های گربنر ارائه کرد (مراجع [۴, ۵] را مطالعه کنید). از آنجایی که این مقاله بر پایه‌های گربنر پارامتری، مشهور به دستگاه گربنر، متمرکز است به طور خلاصه، تاریخچه موجود در مورد این موضوع را مرور می‌کنیم. مفهوم دستگاه‌های گربنر و همچنین اولین الگوریتم برای محاسبه آنها برای اولین بار توسط وایزفنینگ در سال ۱۹۹۲ در [۶] معرفی شد. در این سال‌ها، مطالعات موثر و نتایج بسیاری در محاسبات سیستم‌های گربنر به دست آمده است [۸-۱۷] که نشان از اهمیت این مفهوم دارد. در نهایت دهقانی روش کارامد خود را در [۸] معرفی کرد که با استفاده از تکنیک‌های جبرخطی پارامتری به افراز فضای پارامتری می‌پردازد.
سیستم‌های گربنر کاربردهای متعددی در ریاضیات و سایر علوم دارند. به طور خاص، می توان به هندسه جبری [۱۹-۲۳]، جبر خطی پارامتری [۷, ۹, ۱۴]، بیوشیمی و بیولوژی [۲۱, ۲۲]، اثبات خودکار برخی قضایای هندسه [۱۶, ۱۹, ۲۰, ۲۱]،

[1] **Corresponding author**
Email: m.dehghanidarmian@ipm.ir

شبکه‌های الکتریکی [۲۴] و غیره اشاره کرد. برای رسیدن به هدف اصلی این مقاله، ساختار متن به‌صورت زیرتنظیم شده است: در بخش ۱ به بیان مفهوم پایه گربنر و دستگاه گربنر می‌پردازیم. معرفی مختصری از الگوریتم KSW در بخش ۲ انجام می‌شود. در بخش ۳ به اعمال برخی تغییرات در این الگوریتم جهت کارامدتر شدن می‌پردازیم و تاثیر آنرا در قالب دو مثال توضیح می‌دهیم.

۲. پایه‌های گربنر و دستگاه گربنر

مفهوم پایه‌های گربنر و اولین الگوریتم محاسبه‌ی آن‌ها در رساله‌ی دکترای برونو بوخبرگر تحت راهنمایی ولفگانگ گربنر در سال ۱۹۶۵ معرفی شدند [۱]. در واقع هدف بوخبرگر یافتن نمایش مناسبی برای فضای خارج قسمتی متناظر با یک ایده‌آل چندجمله‌ای از بعد صفر بود. این نمایش مناسب، زمینه ساز معرفی پایه‌ی استانداردی شد که بوخبرگر بعدها به افتخار استاد راهنمایش آن را پایه‌ی گربنر نامید. الگوریتم بوخبرگر از پیچیدگی محاسبات بالایی برخوردار بود. وی توانست در سال ۱۹۷۹ با ارائه‌ی دو محک، الگوریتم خود را قدرتمندتر و سریعتر نماید [۲]. دانیل لازارد در سال ۱۹۸۳ در [۳] با استفاده از جبرخطی توانست محاسبه‌ی پایه‌ی گربنر را بهبود بخشد که این خود نقطه‌ی عطفی در زمینه‌ی بهبود محاسبه‌ی پایه‌ی گربنر است. درنهایت فوژر دو الگوریتم مشهور خود یعنی F_4 و F_5 را ارائه کرد [۴, ۵] که الگوریتم F_5 سریع‌ترین الگوریتم محاسبه‌ی پایه‌ی گربنر تاکنون است. در ادامه این پایه‌ها را مورد مطالعه قرار می‌دهیم. برای این منظور در ابتدا حلقه‌ی چندجمله‌ای‌های چند متغیره را بیان و سپس یک ترتیب تک جمله‌ای را معرفی می‌کنیم. یک تک‌جمله‌ای بر حسب متغیرهای $x_1, \dots, x_n$ حاصل ضربی از متغیرهای تواندار به شکل $x^\alpha = x_1^{\alpha_1} \dots x_n^{a_n}$ است به قسمی که $\alpha = (\alpha_1, \dots, \alpha_n)$ برداری از اعداد صحیح نامنفی باشد. اگر بردار $\alpha = (0, \dots, 0)$ آنگاه $x^\alpha = 1$ ، همچنین درجه‌ی x^α را با نماد $|\alpha|$ نمایش داده و به‌صورت $|\alpha| = \sum_{i=1}^{n} a_i$ تعریف می‌کنیم. فرض کنیم $\mathbb{K}$ یک میدان باشد. هر چندجمله‌ای f بر حسب متغیرهای $x_1, \dots, x_n$ ترکیب خطی تعدادی متناهی از تک جمله‌ای‌ها با ضرایب در $\mathbb{K}$ است که به شکل $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ می‌باشد و در آن $A \subset \mathbb{Z}_{\geq 0}^n$ زیر مجموعه‌ای متناهی است و $a_\alpha \in \mathbb{K}$ ها ضرایب تک‌جمله‌ای‌های x^α در f هستند. همچنین، درجه‌ی چندجمله‌ای f را با نماد $\deg(f)$ نمایش داده و به‌صورت زیر تعریف می‌کنیم:

$$\deg(f) = \max\{|a| \mid a \in A, a_a \neq 0\}$$

مجموعه متشکل از همه‌ی چندجمله‌ای‌ها بر حسب متغیرهای $x_1, \dots, x_n$ با ضرایب در $\mathbb{K}$ به‌همراه دو عمل جمع و ضرب چندجمله‌ای‌ها تشکیل حلقه‌ای می‌دهند که به حلقه‌ی چندجمله‌ای‌های چند متغیره مرسوم است و با نماد $\mathfrak{R} = \mathbb{K}[x_1, \dots, x_n]$ نمایش داده می‌شود. بر خلاف حلقه‌ی چندجمله‌ای‌های یک متغیره که درجه‌ی تک‌جمله‌ای‌ها نقش تعیین کننده‌ای در مقایسه‌ی آن‌ها دارد، در حلقه‌ی چندجمله‌ای‌های چند متغیره نیاز به تعریف نوعی ترتیب داریم: یک ترتیب کلی $\prec$ روی $\mathbb{Z}_{\geq 0}^n$ را یک ترتیب تک‌جمله‌ای گوییم هرگاه به‌ازای هر $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$:

۱. اگر $\alpha \prec \beta$ آنگاه $\alpha + \gamma \prec \beta + \gamma$

۲. ترتیب $\prec$ روی $\mathbb{Z}_{\geq 0}^n$ خوش‌ترتیب باشد.

فرض کنیم $\mathbb{M}(\mathfrak{R})$ مجموعه‌ی تمام تک‌جمله‌ای‌های حلقه‌ی $\mathfrak{R}$ باشد. با استفاده از تناظر یک‌به‌یک زیر یک ترتیب تک‌جمله‌ای روی $\mathbb{Z}_{\geq 0}^n$ به یک ترتیب تک جمله‌ای روی $\mathfrak{R}$ تبدیل می‌شود:

$$\mathbb{M}(\mathfrak{R}) \to \mathbb{Z}_{\geq 0}^n$$
$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \to (\alpha_1, \dots, \alpha_n)$$

بنابر این تناظر، به‌ازای دو تک‌جمله‌ای $x^\alpha, x^\beta \in \mathfrak{R}$ اگر $\alpha \prec \beta$ آنگاه تعریف می‌کنیم $x^\alpha \prec x^\beta$

از مهم‌ترین ترتیب‌های تک جمله‌ای می‌توان به ترتیب الفبایی اشاره کرد که در آن گوییم $\alpha \prec_{lex} \beta$ هرگاه اولین مؤلفه‌ی ناصفر سمت چپ $\alpha - \beta$ مثبت باشد. فرض کنید $\mathfrak{R} = \mathbb{K}[x_1, \dots, x_n]$ و $\prec$ یک ترتیب تک‌جمله‌ای روی $\mathfrak{R}$ باشد.

چندجمله‌ای $f = a_a x^a + \cdots + a_\gamma x^\gamma$ را که در آن $x^\gamma \prec \cdots \prec x^a$ و $a_a \neq 0$ در نظر می‌گیریم. منظور از تک جمله‌ای پیشرو، ضریب پیشرو و جمله‌ی پیشروی f نسبت به $\prec$ به ترتیب a_a, x^γ و $a_a x^a$ است که با نمادهای $\mathrm{LC}_\prec(f), \mathrm{LM}_\prec(f)$ و $\mathrm{LT}_\prec(f)$ نمایش داده می‌شود. همچنین ایده‌آل $I \subset \mathbb{K}[x_1, \dots, x_n]$ را ایده‌آلی تک جمله‌ای نامیم هرگاه توسط یک مجموعه (متناهی یا نامتناهی) از تک جمله‌ای‌ها تولید شود.

فرض کنیم $I \subset \mathfrak{R} = \mathbb{K}[x_1, \dots, x_n]$ ایده‌آلی در حلقه‌ی چندجمله‌ای‌ها و $\prec$ ترتیب تک‌جمله‌ای روی $\mathfrak{R}$ باشد. در این‌صورت ایده‌آل پیشروی I را نسبت به $\prec$ به‌صورت زیر تعریف می‌کنیم:

$$\mathrm{LT}_\prec(I) = \langle \mathrm{LT}_\prec(f) \mid f \in I \rangle$$

همان‌طور که مشخص است $\mathrm{LT}_\prec(I)$ ایده‌آلی تک‌جمله‌ای است. در سال ۱۹۱۳ دیکسون ثابت کرد که هر ایده‌آل تک‌جمله‌ای دارای یک مجموعه مولد متناهی است (لم دیکسون) پس چندجمله‌ای‌های $g_1, \dots, g_k \in I$ موجودند به‌قسمی‌که

$$\mathrm{LT}_\prec(I) = \langle \mathrm{LT}_\prec(g_1), \dots, \mathrm{LT}_\prec(g_k) \rangle.$$

به مجموعه‌ی ذکر شده یعنی $G = \{g_1, \dots, g_k\} \subset I$ یک پایه‌ی گربنر I نسبت به $\prec$ می‌گوییم. باید توجه کنیم که پایه‌ی گربنر یک ایده‌آل یکتا نیست و به ترتیب تک‌جمله‌ای $\prec$ وابسته است. به عنوان مثال اگر $I = \langle y^2 + x, y^3 + 1 \rangle$ ایده‌آلی در $\mathbb{K}[x, y]$ باشد آنگاه با استفاده از دستور Basis در نرم افزار میپل مجموعه‌ی $G_1 = \langle y^2 + x, y^3 + 1 \rangle$ یک پایه‌ی گربنر برای I نسبت به ترتیب $y \prec_{lex} x$ است در حالی‌که مجموعه‌ی $G_2 = \langle y^2 + x, xy - 1, x^2 + y \rangle$ یک پایه‌ی گربنر I نسبت به ترتیب $y \prec_{drl} x$ می‌باشد.

تا کنون پایه‌ی گربنر ایده‌آل I در حلقه‌ی $\mathfrak{R} = \mathbb{K}[x_1, \dots, x_n]$ را نسبت به یک ترتیب تک‌جمله‌ای مطالعه کردیم که در آن ضرایب چندجمله‌ای‌ها در میدان دلخواه $\mathbb{K}$ قرار داشتند. در ادامه قصد داریم به مطالعه‌ی ایده‌آل‌های چندجمله‌ای بپردازیم که در آن ضرایب چندجمله‌ای‌ها خود چندجمله‌ای‌هایی بر حسب تعدادی پارامتر می‌باشند سپس پایه‌ی گربنر این‌گونه ایده‌آل‌ها را معرفی و محاسبه می‌کنیم که به پایه‌ی گربنر پارامتری مشهورند و با توجه به ساختاری که دارند دستگاه گربنر نامیده می‌شوند. انگیزه‌ی اصلی پیدایش مفهوم دستگاه گربنر را می‌توان مسئله‌ی زیر دانست که توسط بایر مطرح شد:

مسئله‌ی بایر: فرض کنیم R و R' دو حلقه‌ی جابجایی نوتری یکدار باشند و $\sigma : R \to R'$ یک همریختی حلقه‌ای باشد. اگر $I \subset R[x_1, \dots, x_n]$ توسیع طبیعی $\sigma : R[x_1, \dots, x_n] \to R'[x_1, \dots, x_n]$ و G یک پایه‌ی گربنر ایده‌آل $\langle \sigma(I) \rangle$ در $R'[x_1, \dots, x_n]$ باشد، آنگاه چه هنگام $\sigma(G)$ یک پایه‌ی گربنر ایده‌آل است؟

حاصل تلاش محققین برای پاسخ به این سوال، منجر به پیدایش مفهومی با عنوان دستگاه گربنر شد. این مفهوم برای اولین بار در سال ۱۹۹۲ توسط وایزفنینگ در [۶] معرفی شد. وی در این مقاله اولین الگوریتم محاسبه‌ی دستگاه گربنر را ارائه کرد. در سال ۱۹۹۷ کالک برنر در [۲۵] پایایی پایه‌های گربنر تحت تاثیر یک همریختی خاص به‌نام تخصیص را مورد مطالعه قرار داد که سال‌ها بعد زمینه‌ی پیدایش الگوریتم‌های سریع‌تر برای محاسبه‌ی این دو مفهوم را فراهم کرد. در سال ۲۰۰۲ مونتس در [۱۶] با استفاده از ایده‌ی طراحی الگوریتم وایزفنینگ در [۶]، اولین الگوریتم سریع و کاربردی محاسبه‌ی دستگاه گربنر را ارائه کرد (همچنین [۱۱]). در سال ۲۰۰۶ سوزوکی و ساتو در [۱۷] با استفاده از نتایج بسیار مهم و مفید کالک برنر در [۲۵] توانستند شیوه‌ای جدید برای محاسبه‌ی دستگاه گربنر و پایه‌ی گربنر فراگیر ارائه کنند. در سال ۲۰۱۰ کاپور و همکارانش در [۱۵] با استفاده از الگوریتم ساتو و سوزوکی و همچنین ایده‌های وایزفنینگ در [۶] توانستند سریع‌ترین الگوریتم محاسبه‌ی دستگاه گربنر را طراحی کنند. در ادامه این مفهوم را معرفی می‌کنیم.

فرض کنیم $S = \mathbb{K}[\mathrm{a}][\mathrm{x}]$ حلقه‌ی چندجمله‌ای‌های پارامتری باشد که در آن $\mathrm{x} = x_1, \dots, x_n$ دنباله‌ای از متغیرها و $\mathrm{a} = a_1, \dots, a_m$ دنباله‌ای از پارامترها است. هر تک‌جمله‌ای در S به شکل $(\prod a_i)^\delta (\prod x_j)^\gamma$ است که در آن $\gamma \in \mathbb{N}^n$ و $\delta \in \mathbb{N}^m$ و برای سادگی به‌صورت $\mathrm{a}^\delta \mathrm{x}^\gamma$ نوشته می‌شود. برای مقایسه‌ی تک‌جمله‌ای‌های موجود در S نیاز به معرفی یک ترتیب تک‌جمله‌ای است: اگر $\prec_\mathrm{x}$ یک ترتیب تک‌جمله‌ای روی متغیرها و $\prec_\mathrm{a}$ یک ترتیب تک‌جمله‌ای روی پارامترها باشد آنگاه ترتیب تک‌جمله‌ای $\prec_{\mathrm{x,a}}$ عبارتست از

$\mathrm{a}^{\delta} \prec_{\mathrm{a}} \mathrm{a}^{\beta}$ و $\mathrm{x}^{\gamma} = \mathrm{x}^{\alpha}$ یا $\mathrm{x}^{\gamma} \prec_{\mathrm{x}} \mathrm{x}^{\alpha}$ اگر $\mathrm{x}^{\gamma}\mathrm{a}^{\delta} \prec_{\mathrm{x,a}} \mathrm{x}^{\alpha}\mathrm{a}^{\beta}$
که در آن $\alpha \in \mathbb{N}^n$ و $\delta, \beta \in \mathbb{N}^m$.

مثال ۲. اگر $\prec_{\mathbf{x}}: y \prec_{lex} x$ ترتیب روی متغیرها و $\prec_{\mathbf{a}}: b \prec_{drl} a$ ترتیب روی پارامترها باشد، آنگاه $a^2bxy \prec_{\mathbf{x,a}} ax^2$ و $a^2x^2y \prec_{\mathbf{x,a}} a^2bx^2y$.

در حلقه‌ی چندجمله‌ای‌ها با ضرایب پارامتری با سه ترتیب تک‌جمله‌ای $\prec_{\mathbf{a}}$, $\prec_{\mathbf{x}}$ و $\prec_{\mathbf{x,a}}$ سروکار داریم. بنابراین برای مشخص شدن مفاهیمی همچون تک‌جمله‌ای پیشرو، ضریب پیشرو و ... از اندیس استفاده می‌کنیم. منظور از یک تخصیص، همریختی $\sigma : \mathbb{K}[\mathrm{a}] \to \overline{\mathbb{K}}$ است که در آن $\overline{\mathbb{K}}$ بستار جبری میدان $\mathbb{K}$ می‌باشد. توسیع طبیعی این همریختی به‌صورت زیر است:

$$\sigma : \mathbb{K}[\mathrm{a}][\mathrm{x}] \to \overline{\mathbb{K}}[\mathrm{x}]$$

که به‌ازای هر $f(\mathrm{a},\mathrm{x}) \in S$ و $\mathrm{a}_\circ = (t_1, \dots, t_m) \in \mathbb{K}^m$ داریم $\sigma(f) = f(\mathrm{a}_\circ, \mathrm{x}) \in \overline{\mathbb{K}}[\mathrm{x}]$.

تعریف ۳. فرض کنیم $F, G_i \subset S$ و $(N_i, W_i) \subset \mathbb{K}[\mathrm{a}] \times \mathbb{K}[\mathrm{a}]$ به‌ازای $i = 1, \dots, l$. مجموعه‌ی متناهی از سه‌تایی‌های $\mathcal{G} = \{(N_i, W_i, G_i)\}_{i=1}^{\ell}$ یک دستگاه گربنر ایده‌آل $\langle f \rangle$ روی $\mathbb{A} \subset \overline{\mathbb{K}}^m$ نسبت به ترتیب تک‌جمله‌ای $\prec_{\mathrm{x,a}}$ نامیده می‌شود هرگاه به‌ازای هر i داشته باشیم:

- مجموعه‌ی $\sigma(G_i) \subset \overline{\mathbb{K}}[\mathrm{x}]$ یک پایه گربنر $\langle \sigma(F) \rangle$ نسبت به $\prec_{\mathrm{x}}$ باشد که $\sigma : \mathbb{K}[\mathrm{a}] \to \overline{\mathbb{K}}$ تخصیص دلخواهی است و در (N_i, W_i) صدق می‌کند.
- $\bigcup_{i=1}^{\ell} \mathbb{V}(N_i) \setminus \mathbb{V}(W_i) = \mathbb{A}$

اگر $\mathbb{A} = \overline{\mathbb{K}}^m$ آنگاه به‌صورت خلاصه $\mathcal{G}$ را یک دستگاه گربنر $\langle F \rangle$ می‌نامیم. به هر یک از سه‌تایی‌های (N_i, W_i, G_i) در $\mathcal{G}$ یک شاخه‌ی دستگاه گربنر می‌گوییم. با توجه به شرط دوم تعریف بالا، N_i را مجموعه‌ی شرایط صفر و W_i را مجموعه‌ی شرایط ناصفر می‌نامیم. همچنین زوج (N_i, W_i) را زوج سازگار گوییم هرگاه $\mathbb{V}(N_i) \setminus \mathbb{V}(W_i) \neq \emptyset$ و در غیر این‌صورت آن را ناسازگار می‌نامیم که از دستگاه گربنر قابل حذف می‌باشند.

در ادامه مثالی از دستگاه گربنر یک ایده‌آل را بیان می‌کنیم که با اجرای میپل الگوریتم KSW محاسبه شده است.

مثال ۴. فرض کنیم $F = \{(a-1)x + y^2, ay + a\} \subset \mathbb{K}[a][x, y]$ که a پارامتر و x, y متغیر هستند. یک دستگاه گربنر $\langle F \rangle$ نسبت به ترتیب تک‌جمله‌ای $a \prec_{lex} y \prec_{lex} x$ عبارتست از:

$$\left\{\begin{array}{lll} (\ \{a\}, & \{\}, & \{-x + y^2\}\ ) \\ (\ \{a-1\}, & \{a\}, & \{1\}\ ) \\ (\ \{\}, & \{a, a-1\}, & \{(a-1)x + y^2, ay + a\}\ ) \end{array}\right.$$

۳. الگوریتم KSW برای محاسبه دستگاه گربنر

الگوریتم KSW برپایه‌ی قضیه‌ی کالک برنر [۳۵] می‌باشد و ساختاری شبیه به ساختار الگوریتم سوزوکی و ساتو [۲۳] دارد. الگوریتم سوزوکی و ساتو نیز بر پایه‌ی قضیه‌ی کالک برنر بنا شده است و ساختار ساده‌تری نسبت به الگوریتم مونتس دارد زیرا بر خلاف مونتس که از الگوریتمی شبیه بوخبرگر استفاده می‌کند، سوزوکی و ساتو به‌طور مستقیم از الگوریتم

محاسبه‌ی پایه‌ی گربنر اجرا شده در نرم‌افزارها بهره می‌برند. اما یکی از معایب الگوریتم سوزوکی و ساتو اینست که در طی محاسبات در هر شاخه‌ی دستگاه گربنر، شرط $\mathbb{V}(G \cap \mathbb{K}[a]) \setminus \mathbb{V}(h) \neq \emptyset$ که معادل سازگار بودن زوج $\mathbb{V}(G \cap \mathbb{K}[a], \{h\})$ است بررسی نمی‌شود و این امر سبب ایجاد شاخه‌های اضافی در دستگاه گربنر می‌شود. برای رفع این مشکل و همچنین بهبود سرعت و قدرت محاسبه‌ی دستگاه گربنر قصد داریم در این بخش سریع‌ترین و مفیدترین الگوریتم محاسبه‌ی دستگاه گربنر را معرفی کنیم. این الگوریتم که به KSW شهرت دارد در سال ۲۰۱۰ در [۱۵] توسط کاپور و همکارانش طراحی گردید. الگوریتم KSW نیز برپایه‌ی قضیه‌ی کالک برنر می‌باشد و ساختاری شبیه به ساختار الگوریتم سوزوکی و ساتو [۱۷] دارد با دو تفاوت که سبب قدرتمندتر شدن KSW می‌شود.

- معرفی مفهوم پایه‌ی دیکسون کمینه و استفاده از آن در محاسبه‌ی دستگاه گربنر که باعث کاهش تعداد شاخه‌های دستگاه گربنر می‌شود.
- بررسی سازگاری زوج‌های پارامتری.

در ادامه پس از بیان مقدمات مورد نیاز، الگوریتم KSW را ارائه می‌دهیم.

تعریف ۵. فرض کنیم $F \subset S = \mathbb{K}[a][x]$ مجموعه‌ای متناهی و $\prec_{x,a}$ ترتیب حاصل‌ضربی معرفی شده باشد. مجموعه $F' \subset S$ را یک پایه‌ی دیکسون کمینه‌ی F نامیم و با نماد $\mathrm{MDBasis}(F)$ نمایش می‌دهیم هرگاه

۱- F' زیرمجموعه‌ی F باشد.

۲- به‌ازای هر $f \in F$ چندجمله‌ای $f' \in F'$ موجود باشد به‌قسمی‌که $\mathrm{LM}_x(f') \mid \mathrm{LM}_x(f)$؛ به عبارت دیگر
$$\langle \mathrm{LM}_x(f) \rangle = \langle \mathrm{LM}_x(f') \rangle$$

۳- برای هر دو چندجمله‌ای $f_1', f_2' \in F'$، شرایط $\mathrm{LM}_x(f_2') \nmid \mathrm{LM}_x(f_1')$ و $\mathrm{LM}_x(f_1') \nmid \mathrm{LM}_x(f_2')$ برقرار باشد. مثال زیر نشان می‌دهد که پایه‌ی دیکسون کمینه‌ی $F \subset \mathbb{K}[a][x]$ یکتا نیست.

مثال ۶. فرض کنیم $F = \{ax^2 - y, ay^2 - 1, ax - 1, (a+1)x - y, (a+1)y - a\} \subset \mathbb{K}[a][x, y]$ و $a \prec_{lex} y \prec_{lex} x$. در این‌صورت مجموعه‌های
$$F_1' = \{ax - 1, (a+1)y - a\}, F_2' = \{(a+1)x - y, (a+1)y - a\}$$
هر دو پایه‌ی دیکسون کمینه برای F هستند.

کاپور و همکارانش با استفاده از این مفهوم توانستند قضیه‌ی مهمی را ثابت کنند که محاسبات دستگاه گربنر را ساده‌تر می‌کند. برای بیان این قضیه‌ی مهم نیاز به ارائه‌ی لم زیر است.

لم ۷. فرض کنیم مجموعه‌ی متناهی $G \subset \mathbb{K}[a][x]$ پایه‌ی گربنر ایده‌آل $\langle G \rangle$ نسبت به ترتیب $\prec_{x,a}$ باشد و $G_1 = \{g_1, \dots, g_s\} \subset G$. همچنین همریختی $\sigma : \mathbb{K}[a] \to \overline{\mathbb{K}}$ وجود دارد که $\sigma(\mathrm{LC}_x(g_i)) \neq 0$ به‌ازای هر $i = 1, \dots, s$.
اگر برای هر چندجمله‌ای $p \in G \setminus G_1$ چندجمله‌ای‌های $p_1, \dots, p_s \in \overline{\mathbb{K}}[x]$ موجود باشند به‌قسمی‌که
$$\sigma(p) = p_1\sigma(g_1) + \cdots + p_s\sigma(g_s)$$
که $\mathrm{LM}_x(p_i\sigma(g_i)) \preccurlyeq \mathrm{LM}_x(p)$ به‌ازای هر $i = 1, \dots, s$، آنگاه $\sigma(G_1)$ یک پایه‌ی گربنر ایده‌آل $\langle \sigma(G) \subset \overline{\mathbb{K}}[x] \rangle$ نسبت به $\prec_x$ است.

برهان. با توجه به فرض مجموعه‌ی $\sigma(G_1)$ یک پایه‌ی $\langle \sigma(G) \rangle$ است. پس کافیست ثابت کنیم $\sigma(G_1)$ یک پایه‌ی گربنر است. به‌ازای هر $g_j, g_k \in G_1$ چون $\mathrm{LC}_x\left(\sigma(g_j)\right) \neq 0$ و $\sigma(\mathrm{LC}_x(g_k)) \neq 0$ پس داریم:

$$\mathrm{Spoly}\left(\sigma(g_j),\sigma(g_k)\right)=c\sigma\mathrm{Spoly}_{\mathrm{x}}(g_j,g_k) \qquad (۳.۴)$$

که $c\in\overline{\mathbb{K}}$ و $\mathrm{Spoly}_{\mathrm{x}}(g_j,g_k)\in\mathbb{K}[\mathrm{a}][\mathrm{x}]$. فرض کنیم $G\backslash G_1=\{g_s+1,\dots,g_\ell\}$. چون G یک پایه‌ی ایده‌آل $S\subset\langle G\rangle$ نسبت به ترتیب $\prec_{\mathrm{x,a}}$ است و $\mathrm{Spoly}_{\mathrm{x}}(g_j,g_k)\in\langle G\rangle$ لذا چندجمله‌ای‌های $h_1,\dots,h_\ell$ وجود دارند به‌قسمی‌که $\mathrm{Spoly}_{\mathrm{x}}(g_j,g_k)=h_1g_1+\cdots+h_\ell g_\ell$ که در آن

$$\mathrm{LM}_{\mathrm{x}}(h_ig_i)\prec\mathrm{lcm}\left(\mathrm{LM}_{\mathrm{x}}(g_j),\mathrm{LM}_{\mathrm{x}}(g_k)\right).$$

با جایگزین کردن این تساوی در برابری 3.4 رابطه‌ی زیر حاصل می‌شود.

$$\mathrm{Spoly}\left(\sigma(g_j),\sigma(g_k)\right)=c\big(\sigma(h_1g_1)+\dots+\sigma(h_\ell g_\ell)\big). \qquad (۳.۵)$$

به‌طوری‌که به‌ازای هر $i=1,\dots,\ell$

$$\mathrm{LM}_{\mathrm{x}}\big(\sigma(h_i)\big)\mathrm{LM}_{\mathrm{x}}(g_i)\preccurlyeq\mathrm{LM}_{\mathrm{x}}(h_ig_i)\prec\mathrm{lcm}\left(\mathrm{LM}_{\mathrm{x}}(g_j),\mathrm{LM}_{\mathrm{x}}(g_k)\right)$$
$$=\mathrm{lcm}\left(\mathrm{LM}_{\mathrm{x}}\left(\sigma(g_j)\right),\mathrm{LM}_{\mathrm{x}}(\sigma(g_k))\right).$$

از طرفی بنا به فرض به‌ازای هر $p\in G\setminus G_1$ چندجمله‌ای‌های $p_1,\dots,p_s\in\overline{\mathbb{K}}[\mathrm{x}]$ موجود باشند به‌قسمی‌که

$$\sigma(p)=p_1\sigma(g_1)+\cdots,p_s\sigma(g_s)$$

که $\mathrm{LM}_{\mathrm{x}}\big(p_i\sigma(g_i)\big)\preccurlyeq\mathrm{LM}_{\mathrm{x}}(p)$ به‌ازای هر $i=1,\dots,s$. با جایگزین کردن این نمایش در برابری 3.5 تساوی زیر به‌دست می‌آید:

$$\mathrm{Spoly}\left(\sigma(g_j),\sigma(g_k)\right)=p_1'\sigma(g_1)+\cdots+p_s'\sigma(g_s),p_1',\dots,p_s'\in\overline{\mathbb{K}}[\mathrm{x}] \qquad (۳.۶)$$

که در آن $\mathrm{LM}_{\mathrm{x}}\big(p_1'\sigma(g_1)\big)\prec\mathrm{lcm}\left(\mathrm{LM}_{\mathrm{x}}\left(\sigma(g_j)\right),\mathrm{LM}_{\mathrm{x}}(\sigma(g_k))\right)$ به‌ازای هر $i=1,\dots,s$. در حقیقت $t\preccurlyeq\mathrm{lcm}\left(\mathrm{LM}_{\mathrm{x}}\left(\sigma(g_j)\right),\mathrm{LM}_{\mathrm{x}}(\sigma(g_k))\right)$ رابطه‌ی 3.6 یک تی-نمایش برای $\mathrm{Spoly}\left(\sigma(g_j),\sigma(g_k)\right)$ است که درنتیجه مجموعه‌ی $\sigma(G_1)$ یک پایه‌ی گربنر است.

اکنون مهم‌ترین قضیه‌ی این بخش را بیان می‌کنیم که در الگوریتم KSW نقش بسیار مهمی ایفا می‌کند.

قضیه ۸. فرض کنیم G یک پایه‌ی گربنر ایده‌آل $\langle F\rangle\subset S=\mathbb{K}[\mathrm{a}][\mathrm{x}]$ نسبت به ترتیب $\prec_{\mathrm{x,a}}$ باشد. دو زیر مجموعه‌ی $G_r=G\cap\mathbb{K}[\mathrm{a}]$ و $G_m=\mathrm{MDBasis}(G\setminus G_r)$ را در نظر می‌گیریم. اگر σ یک تخصیص باشد به‌قسمی‌که

۱- به‌ازای هر $g\in G_r$ داریم $\sigma(g)=0$

۲- اگر $h=\prod_{g\in G_m}\mathrm{LC}_{\mathrm{x}}(g)\in\mathbb{K}[\mathrm{a}]$، آنگاه $\sigma(h)\neq0$

دراین‌صورت مجموعه‌ی $\sigma(G_m)$ یک پایه‌ی گربنر کمینه‌ی ایده‌آل $\langle\sigma(F)\rangle\subset\overline{\mathbb{K}}[\mathrm{x}]$ نسبت به ترتیب $\prec_{\mathrm{x}}$ است.

برهان. فرض کنیم $p\in G\setminus(G_r\cup G_m)$ چندجمله‌ای دلخواهی باشد. بنا به تعریف پایه‌ی دیکسون کمینه، چندجمله‌ای p به پیمانه‌ی G_m نسبت به متغیرها کاهش پذیر است. توجه به این نکته ضروریست که برای تقسیم p بر G_m کافیست ضرایب پیشروی جملات G_m را که متعلق به $\mathbb{K}[\mathrm{a}]$ هستند در p ضرب کنیم و سپس چندجمله‌ای حاصل را بر G_m تقسیم کنیم و این عمل را تا یافتن باقیمانده ادامه دهیم (بنا به فرض چون ضرایب پیشروی جملات G_m مخالف صفر هستند مجاز به انجام این کار هستیم). فرض کنیم r باقیمانده‌ی این تقسیم به شیوه‌ی بیان شده باشد. پس داریم:

$$\big(\mathrm{LC}_{\mathrm{x}}(g_1)\big)^{\alpha_1}\dots\big(\mathrm{LC}_{\mathrm{x}}(g_s)\big)^{\alpha_s}p=q_1g_1+\cdots+q_sg_s+r \qquad (۳.۷)$$

که $g_i \in G_m$ و $q_i \in \mathbb{K}[a][x]$ به‌ازای $i = 1, \dots, s$. همچنین $r \in \mathbb{K}[a][x]$ به‌قسمی‌که هیچ تک‌جمله‌ای موجود در r بر تک‌جمله‌ای‌های پیشروی چندجمله‌ای‌های G_m نسبت به ترتیب $\prec_x$ بخش‌پذیر نیست. در ادامه ثابت می‌کنیم $r \in G_r$. چون $p \in \langle F \rangle$ پس $r \in \langle F \rangle$ و چون G یک پایه‌ی گربنر ایده‌آل $\langle F \rangle$ نسبت به ترتیب $\prec_{x,a}$ است پس $\overline{r}^G = 0$. از طرفی r نسبت به G_m کاهش یافته است پس نسبت به $G \setminus G_r$ کاهش ناپذیر است. با توجه به اینکه r نسبت به $G \setminus G_r$ کاهش ناپذیر است و $\overline{r}^G = 0$ پس $\overline{r}^{G_r} = 0$ و در نتیجه $r \in G_r$. بعلاوه چون r به پیمانه‌ی G_r به صفر کاهش می‌یابد پس در این تقسیم هیچ تک‌جمله‌ای جدیدی برحسب متغیرهای x ظاهر نمی‌شود. همچنین چون $\mathsf{LC}_x(g_i) \in \mathbb{K}[a]$ پس رابطه‌ی $\mathsf{LM}_x(q_i g_i) \preccurlyeq \mathsf{LM}_x(p)$ برقرار است.

حال فرض کنید $c = \left(\mathsf{LC}_x(g_1)\right)^{\alpha_1} \dots \left(\mathsf{LC}_x(g_s)\right)^{\alpha_s}$. با تأثیر تخصیص σ بر دو طرف تساوی 3.7 برابری زیر به‌دست می‌آید:

$$\sigma(c)\sigma(p) = \sigma(q_1)\sigma(g_1) + \cdots + \sigma(q_s)\sigma(g_s) + \sigma(r).$$

طبق فرض $\sigma(h) \neq 0$ پس $\sigma\left(\mathsf{LC}_x(g)\right) \neq 0$ به‌ازای هر $g \in G_m$. همچنین باتوجه به فرض $\sigma(g) = 0$ به‌ازای هر $g \in G_r$. چون $r \in G_r$ پس $\sigma(r) = 0$. چون $\sigma(c) \in \overline{\mathbb{K}}$ و $\sigma(c) \neq 0$ لذا با توجه به لم ۷ نتیجه می‌گیریم که مجموعه‌ی $\sigma(G_m)$ یک پایه‌ی گربنر ایده‌آل $\langle \sigma(G) \rangle = \langle \sigma(F) \rangle$ نسبت به ترتیب $\prec_x$ است که باتوجه به تعریف G_m کمینه می‌باشد.

باتوجه به مقدمات بیان شده الگوریتم KSW را ارائه می دهیم. در الگوریتم زیر برای دو مجموعه‌ی A و B منظور از نماد $A \times B$ یعنی $A \times B = \{ab \mid a \in A, b \in B\}$.

Algorithm 1 KSW

Require: N, W; finite subsets of $\mathbb{K}[\mathbf{a}]$ and F; a finite subset of $\mathbb{K}[\mathbf{a}, \mathbf{x}]$
Ensure: A Gröbner system of F on (N, W) i. e. respecting $\mathbb{V}(N) \setminus \mathbb{V}(W)$

1. If (N, W) is inconsistent then **Return** $(\emptyset)$
2. Otherwise $G :=$ The reduced Gröbner basis$(F \cup N, \prec_{\mathbf{x},\mathbf{a}})$
3. If $1 \in G$, then **Return** $(\{(N, W, \{1\})\})$
4. $G_r := G \cap \mathbb{K}[\mathbf{a}]$
5. If $(N, G_r \times W)$ is inconsistent, then PGB $:= \emptyset$, else PGB: $= \{N, G_r \times W, \{1\}\}$
6. If (G_r, W) is inconsistent, then **Return** (PGB)
7. Otherwise, $G_m :=$ MDBasis$(G \setminus G_r)$
8. If $(G_r, W \times \{h\})$ is consistent then PGB $:=$ PGB$\cup\{G_r, W \times \{h\}, G_m\}$, where $h = \mathrm{lcm}\{h_1, \dots, h_k\}$ with $h_i = \mathrm{LC}_{\prec_{\mathbf{x}}}(g_i)$ for each $g_i \in G_m = \{g_1, \dots, g_k\}$
9. **Return** PGB $\cup \bigcup_{h_i \in \{h_1, \dots, h_k\}}$ KSW $(G_r \cup \{h_i\}, W \times \{h_1 h_2 \dots h_{i-1}\}, G \setminus G_r)$

بنا بر [۱۵] این الگوریتم پس از متناهی مرحله پایان می‌یابد و خروجی آن یک دستگاه گربنر است.

۴. الگوریتم KSW بهینه شده

در این بخش با اعمال تغییری کوچک ولی بسیار تاثیر گذار به بهینه سازی الگوریتم می‌پردازیم. اگر به سطر پنجم الگوریتم KSW دقت کنیم درمی‌یابیم که این سطر شاخه‌هایی را به دستگاه گربنر اضافه می‌کند که دارای پایه‌ی گربنر $\{1\}$ هستند.

با حذف این سطر از الگوریتم کاپور و اضافه کردن شاخه‌ی $(\text{other cases}, \{1\})$ به دستگاه گربنر نه تنها خللی در الگوریتم ایجاد نمی‌شود بلکه الگوریتم حاصل دارای مزیت‌های زیر است:

۱. تعداد شاخه‌های دستگاه گربنر کمتر می‌شود.

۲. نیازی به بررسی سازگاری شرایط پارامتری آن دسته از شاخه‌هایی که پایه‌ی گربنر $\{1\}$ دارند نیست.

الگوریتم بعد همان الگوریتم KSW است که سطر پنجم آن حذف شده است و ما آن‌را الگوریتم $\text{OPTIMIZED} - \text{KSW}$ می‌نامیم. لازم به ذکر است که این ایده را به‌عنوان نتیجه‌ای فرعی در قالب بخشی از مرجع [۱۴] بیان کرده‌ایم که این مقاله مورد پذیرش قرار گرفته است.

Algorithm 15 $\text{OPTIMIZED} - \text{KSW}$

Require: N, W; finite subsets of $\mathbb{K}[\mathbf{a}]$ and F; a finite subset of $\mathbb{K}[\mathbf{a}, \mathbf{x}]$
Ensure: A Gröbner system of F on (N, W) i. e. respecting $\mathbb{V}(N) \setminus \mathbb{V}(W)$

1. If (N, W) is inconsistent then **Return** $(\emptyset)$
2. Otherwise $G :=$ The reduced Gröbner basis$(F \cup N, \prec_{\mathbf{x},\mathbf{a}})$
3. If $1 \in G$, then **Return** $(\{(N, W, \{1\})\})$
4. $G_r := G \cap \mathbb{K}[\mathbf{a}]$
5. If (G_r, W) is inconsistent, then **Return** (PGB)
6. Otherwise, $G_m :=$ MDBasis$(G \backslash G_r)$
7. If $(G_r, W \times \{h\})$ is consistent then PGB $:=$ PGBU$\{G_r, W \times \{h\}, G_m\}$, where $h = \text{lcm}\{h_1, \dots, h_k\}$ with $h_i = \text{LC}_{\prec_{\mathbf{x}}}(g_i)$ for each $g_i \in G_m = \{g_1, \dots, g_k\}$
8. **Return** PGB $\cup \bigcup_{h_i \in \{h_1, \dots, h_k\}} \text{OPTIMIZED} - \text{KSW}\,(G_r \cup \{h_i\}, W \times \{h_1 h_2 \dots h_{i-1}\}, G \backslash G_r)$

قضیه ۹. الگوریتم $\text{OPTIMIZED} - \text{KSW}$ پس از متناهی مرحله پایان می‌یابد و خروجی آن یک دستگاه گربنر F است.

برهان. بنا به الگوریتم KSW خروجی الگوریتم $\text{OPTIMIZED} - \text{KSW}$ نیز یک دستگاه گربنر برای ایده‌آل F است. حال برای اثبات پایان‌پذیری الگوریتم کافیست نشان دهیم که در هر مرحله تعداد متناهی شاخه تولید می‌شود و هر شاخه پس از متناهی مرحله پایان می‌یابد. مجموعه‌ی G_m تعداد متناهی عضو دارد و لذا در هر مرحله تعداد متناهی شاخه تولید می‌شود. از طرفی می‌دانیم G پایه‌ی گربنر کاهش‌یافته‌ی $\langle F \cup N \rangle \subset \mathbb{K}[\mathrm{a}][\mathrm{x}]$ است. چون $h_i = \text{LC}_{\mathrm{x}}(g) \in \mathbb{K}[\mathrm{a}]$ به‌ازای هر $g \in G$ و $G_r = G \cap \mathbb{K}[\mathrm{a}]$ نتیجه می‌گیریم که $h_i \notin G_r$. بنابراین در هر مرحله از فراخوانی الگوریتم $\text{OPTIMIZED} - \text{KSW}$ مجموعه‌ی N زیرمجموعه‌ی سره‌ی $N \cup \{h_i\}$ است و لذا از نوتری بودن حلقه‌ی $\mathbb{K}[\mathrm{a}]$ نتیجه می‌گیریم هر شاخه پس از متناهی مرحله پایان می‌یابد.

مثال ۱۰. مجموعه‌ی زیر را بعنوان ورودی الگوریتم‌های $\text{OPTIMIZED} - \text{KSW}$ و KSW در نظر می‌گیریم:

$$F = \{ax + b - 1, by + a - 1, cz + a - b, du + m - n\} \subset \mathbb{K}[a, b, c, d, m, n, x, y, z, u]$$

را که در آن x, y, z, u متغیر و a, b, c, d, m, n پارامتر هستند. همچنین ترتیب‌های زیر را روی پارامترها و متغیرها قرار می‌دهیم.

$$m \prec_{drl} n \prec_{drl} d \prec_{drl} c \prec_{drl} b \prec_{drl} a, \quad u \prec_{drl} z \prec_{drl} y \prec_{drl} x$$

جدول زیر دستگاه گربنر ایده‌آل F محاسبه شده توسط الگوریتم KSW است. همان‌طور که مشاهده می‌شود این دستگاه دارای هفده شاخه است که نه شاخه از آن‌ها پایه‌ی گربنر $\{1\}$ دارند.

Null set	Non − null set	Gröbner Basis
[ ]	$[abcd]$	$[du+m-n, cz+a-b, by+a-1, ax+b-1]$
$[b-1, a]$	$[c, d]$	$[du+m-n, -1+cz, -1+y]$
$[m-n, d, b-1, a]$	$[c]$	$[-1+cz, -1+y]$
$[b, a-1]$	$[c, d]$	$[du+m-n, 1+cz, x-1]$
$[m-n, d, b, a-1]$	$[c]$	$[1+cz, x-1]$
$[c, a-b]$	$[b, d]$	$[du+m-n, -1+b+by, x-y]$
$[m-n, d, c, a-b]$	$[b]$	$[-1+b+by, x-y]$
$[m-n, d]$	$[a, b, c]$	$[cz+a-b, by+a-1, ax+b-1]$
$[d]$	$[m-n]$	$[1]$
$[m-n, d, c]$	$[a-b]$	$[1]$
$[m-n, a, b, c, d]$	[ ]	$[1]$
$[m-n, b, d]$	$[ac-c]$	$[1]$
$[m-n, a, d]$	$[b^2c-bc]$	$[1]$
$[c]$	$[ad-bd]$	$[1]$
$[a, b, c]$	$[d]$	$[1]$
$[b]$	$[acd-cd]$	$[1]$
$[a]$	$[b^2cd-bcd]$	$[1]$

جدول زیر دستگاه گربنر F را که با استفاده از الگوریتم $\text{KSW}-\text{OPTIMIZED}$ محاسبه شده است نشان می‌دهد.

Null set	Non − null set	Gröbner Basis
[ ]	$[abcd]$	$[du+m-n, cz+a-b, by+a-1, ax+b-1]$
$[b-1, a]$	$[c, d]$	$[du+m-n, -1+cz, -1+y]$
$[m-n, d, b-1, a]$	$[c]$	$[-1+cz, -1+y]$
$[b, a-1]$	$[c, d]$	$[du+m-n, 1+cz, x-1]$
$[m-n, d, b, a-1]$	$[c]$	$[1+cz, x-1]$
$[c, a-b]$	$[b, d]$	$[du+m-n, -1+b+by, x-y]$
$[m-n, d, c, a-b]$	$[b]$	$[-1+b+by, x-y]$
$[m-n, d]$	$[a, b, c]$	$[cz+a-b, by+a-1, ax+b-1]$
other caces	other caces	$[1]$

تأثیر حذف سطر پنجم الگوریتم KSW در مثال بعد قابل توجه است.

مثال ۱۱. ایده‌آل تولید شده توسط مجموعه‌ای از چندجمله‌ای‌های خطی پارامتری زیر را در نظر می‌گیریم که در آن a_iها پارامتر و x_iها متغیر هستند:

$$F = \{a_i x_i + x_{i+1} - a_{i+1}\}_{i=1}^{19} = \{a_1x_1 + x_2 - a_2, a_2x_2 + x_3 - a_3, \dots, a_{19}x_{19} + x_{20} - a_{20}\}$$

ترتیب روی پارامترها ومتغیرها را به‌صورت $x_{i+1} \prec_{drl} x_i$, $a_{i+1} \prec_{drl} a_i$ در نظر می‌گیریم. نتایج قابل توجه اجرای این مثال در جدول زیر آمده است.

Algorithm	Time (Sec)	Used Memory (GB)	Branch
KSW	> 600	$-$	$-$
$\text{OPTIMIZED} - \text{KSW}$	$32/98$	$2/64$	101

همانطورکه در جدول دیده می‌شود الگوریتم KSW قادر به محاسبه‌ی دستگاه گربنر ایده‌آل F در مدت ۶۰۰ ثانیه نمی‌باشد در حالی‌که در کمتر از ۳۳ ثانیه با استفاده از الگوریتم $\text{OPTIMIZED} - \text{KSW}$ محاسبه شده است.

نتیجه‌گیری

قدرت تحلیل دستگاه‌های گربنر آنها را به ابزاری ارزشمند در رشته‌های مختلف علوم و مهندسی تبدیل کرده است. بسیاری از مسایل پیرامون ما را می‌توان با استفاده از دستگاه‌های گربنر با نتایج کاملا رضایت بخش و محاسبات کاملا خودکار و اتومات بررسی کرد. به عنوان مثال، دستگاه‌های گربنر را می توان در پردازش تصویر، رمزنگاری، بیوشیمی و بسیاری از زمینه‌های دیگر که در آن مسائل پیچیده جبری نیاز به تحلیل حالات مختلف شرایط دارند، استفاده نمود. با بکارگیری تکنیک‌های جبر محاسباتی، محققان، متخصصان و مهندسان می‌توانند محاسبات پیچیده مدلسازی‌های خود را به‌راحتی آنالیز کرده و راه حل‌هایی برای مسائل کاربردی بیابند. با توجه به همه‌ی این کاربردها، هر تغییر الگوریتمی که باعث کارامدتر شدن الگوریتم محاسبه‌ی دستگاه گربنر بشود می‌تواند مهم و تاثیرگزار باشد.

فهرست منابع

[۱] Buchberger, B. (2006). "Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, *J.Symb. Comput.*, *41* (3-4), 475-511.

[۲] Buchberger, B. (1979). A criterion for detecting unnecessary reductions in constructing Gröbner bases, in *International Symposium on Symbolic and Algebraic Manipulation*, 3-21.

[۳] Lazard, D. (1983). Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, in *European Conference on Computer Algebra*, 146-156.

[٤] Faugere, J.-C. (1999). A new efficient algorithm for computing Gröbner bases (F4), *Journal of Pure and Applied Algebra*, *139* (1-3), 61-88.

[٥] Faugere, J.-C. (2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 75-83.

[٦] Weispfenning, V. (1992). Comprehensive gröbner bases, *Journal of symbolic computation*, *14*, (1), 1-29.

[٧] Dehghani Darmian, M. (2024). Efficient Algorithm for Computing Inverse of Parametric Matrices, *Scientific Annals of Computer Science*, *1*, 1-22.

[۸] Dehghani Darmian, M. (2024). Improvement of an incremental signature-based comprehensive Gröbner system algorithm., *Math. Comput. Sci, 18* (12).

[۹] Dehghani Darmian, M., & Hashemi, A. (2017). Parametric FGLM algorithm, *Journal of Symbolic Computation, 82*, 38-56.

[۱۰] Dehghani Darmian, M., & Hashemi, A. (2024). Parametric F_4 Algorithm, *Iranian Journal of Mathematical Sciences and Informatics, 19* (4), 117-133.

[۱۱] Dehghani Darmian, M., Hashemi, A., & Montes, A. (2011). Erratum to "A new algorithm for discussing Gröbner bases with parameters" J. Symb. Comput. *33* (1-2)(2002) 183-208, *J. Symb. Comput.," 46* (10), 1187-1188.

[۱۲] Hashemi, A., Dehghani Darmian, M., & Barkhordar, M. (2018, July 24-27). Universal Gröbner basis for parametric polynomial ideals, in *Mathematical Software–ICMS 2018: 6th International Conference, South Bend, IN, USA, Proceedings* Springer, 191-199.

[۱۳] Hashemi, A., Dehghani Darmian, M., & Barkhordar, M. (2017). Gröbner systems conversion, *Mathematics in Computer Science, 11*, 61-77.

[۱٤] Hashemi, A., M.-Alizadeh, B., & Dehghani Darmian, M. (2013). Minimal polynomial systems for parametric matrices, *Linear and Multilinear Algebra, 61* (2), 265-272.

[۱٥] Kapur, D., Sun, Y., & Wang, D. (2010). A new algorithm for computing comprehensive Gröbner systems, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 29-35.

[۱٦] Montes, A. (2002). A new algorithm for discussing Gröbner bases with parameters, *J. Symb. Comput., 33* (2), 183-208.

[۱۷] Suzuki, A., & Sato, Y. (2006). A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 326-331.

[۱۸] Cox, D. A., Little, J., & O'Shea, D. (2005). *Using algebraic geometry*. Springer Science & Business Media.

[۱۹] Dehghani Darmian, M., Hashemi, A. (2010, November 10-11). Classification of cubic curves by Gröbner systems, presented at the 21st Algebra seminar of Iran, Tabriz, Iran.

[۲۰] Montes, A., & Recio, T. (2006, August 31-September 2). Automatic discovery of geometry theorems using minimal canonical comprehensive Gröbner systems, in *Automated Deduction in Geometry: 6th International Workshop, Pontevedra, Spain,*113-138.

[۲۱] Dimitrova, E. S., Jarrah, A. S., Laubenbacher, R., & Stigler. B. (2007). A Gröbner fan method for biochemical network modeling, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 122-126.

[۲۲] Laubenbacher, R., & Stigler. B. (2004). A computational algebra approach to the reverse engineering of gene regulatory networks, *Journal of Theoretical Biology, 229* (4), 523-537.

[۲۳] Cox, D. A., Little, J., & O'Shea, D. (2015). *Ideals, varieties, and algorithms*. Springer.

[۲٤] Montes, A. (1998). Algebraic solution of the load-flow problem for a 4-node electrical network, *Mathematics and computers in simulation, 45* (1-2), 163-174.

[۲٥] Kalkbrener, M. (1997). On the stability of Gröbner bases under specializations, *Journal of Symbolic Computation, 24* (1), 51-58.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December 25-26, 2024

Leveraging Reinforcement Learning with Greedy Path Mining for Target Group Influence Maximization in Social Networks

Neda Binesh, Mahdieh Haddadi

Faculty of Mathematics, Statistics and Computer Science
Semnan University, Semnan, Iran
neda_binesh@semnan.ac.ir; m.haddadi@semnan.ac.ir

ABSTRACT

Social networks are characterized by the formation of groups, where decisions are often influenced by majority consensus. This paper deals with the issue of Target Group Influence Maximization (TGIM). The objective of TGIM is to select a set of *k* influential nodes to maximize the activation of target group members through the dissemination of specific content or information.

We propose a novel algorithm, Target Group Influence Maximization using Reinforcement Learning with Greedy Path mining (TGRLGP), to address the TGIM problem. TGRLGP leverages reinforcement learning techniques to identify optimal paths from target nodes to potential influencers. Experimental results demonstrate the superior performance of our proposed TGRLGP algorithm compared to existing methods.

KEYWORDS: Target Group Influence Maximization; Social Network; Reinforcement Learning; Greedy Path mining.

1 INTRODUCTION

Social networks constitute online platforms designed to facilitate the creation, sharing, and dissemination of information and ideas among individuals and groups. These networks function as interconnected nodes, enabling the rapid propagation of information. A salient characteristic of social networks is their capacity to influence individuals and groups through the dissemination of opinions and perspectives. This influence can be strategically targeted to specific demographics. Furthermore, social networks have become essential tools for commercial purposes, allowing businesses to persuade consumers, raise awareness, and stimulate sales on a broader scale. In recent times, online social networks have emerged as effective channels for promoting new products and cultivating relationships between businesses and consumers. By leveraging these platforms, companies can reach a vast audience while minimizing advertising expenditures, thereby maximizing their impact.

Companies can utilize social networks like Instagram to identify influential nodes with a substantial follower base to promote their products. By distributing product samples and encouraging these influencers to endorse the product, companies can trigger a cascading effect, leading to widespread adoption and increased sales. This targeted approach allows companies to optimize their marketing efforts.

Consequently, determining the significance of nodes and identifying influential nodes within a social network is a crucial challenge in the field of Influence Maximization (IM). The goal of IM is to select a set of "seed nodes" that can maximize the spread of influence across the network. The IM problem is computationally challenging, classified as NP-hard. Researchers have extensively investigated this problem, employing various techniques to address it, as detailed in [1, 2, 3].

Group Influence Maximization (GIM) is a specialized area within the broader domain of influence maximization. The primary objective in GIM is to strategically select an initial set of k active nodes (individuals) within a network. These chosen nodes serve as influencers, with the overarching goal of maximizing the expected number of influenced groups. Unlike traditional influence maximization, which focuses on maximizing individual impact by targeting specific individuals, GIM adopts a broader approach, emphasizing the activation of entire groups rather than isolated individuals [4].

In certain contexts, organizations may prioritize a specific subset within a social network, often referred to as the "target group." This subset could represent users of a particular product, residents of a specific geographic region, individuals with particular political inclinations, or similar categories. Such scenarios introduce a novel challenge in the influence maximization domain: identifying influential nodes to activate the target group. This concept is known as Target Group Influence Maximization (TGIM). In this study, we focus on TGIM, aiming to activate an entire group rather than targeting individuals in isolation.

2 PRELIMINARIES

Table 1 includes the necessary notations and symbols in this paper.

Table 1 Frequent notations used across the paper

Notations	Meaning
k	Number of spreaders
G/V/E	a social network/ set of nodes/ set of links
n/m	number of nodes/ number of links/ number of candidate nodes
bn(i)	number of neighbours of node i whose degrees are greater than or equal to deg(i)
ND	neighborhood-degree index
V'	Set of destination nodes include candidate nodes
l	$=\|V'\|$: number of candidate nodes
H / h	Set of Target Group / number of target group
$Q \in \mathbb{R}^{n\times n}$	Q-value matrix in reinforcement learning approach
$R \in \mathbb{R}^{n\times n}$	Reward matrix in reinforcement learning approach
γ	the learning rate in Q-learning
$P \in \mathbb{R}^{h\times l}$	Path matrix include the scaled path length from each target to each candidate nodes
M	Diffusion model
$A_0 / A_t / A_T$	initial spreaders set/active nodes set in time t/ final active nodes set
R	number of iterations in Monte Carlo simulation
IS	Influence Spread (average number of final active nodes in R iterations)
$\beta(u,v)$	probability of information transfer from node u to node v in the IC model

2.1 Social Networks

A social network is typically modeled as a graph $G = (V, E)$, where the set V represents individuals (nodes), and the set E denotes the edges, signifying social connections or relationships. The neighbors of a node u in this network are the nodes directly connected to u by an edge. The degree of u, denoted by $\deg(u)$, represents the number of edges incident to u. The Neighborhood-degree of u is defined as follows [5]:

$$ND(u) = \frac{deg(u)}{bn(u)+1}, \quad (1)$$

where $bn(u)$ indicates the number of neighbours of the node u whose degrees are greater than or equal to $\deg(u)$. A higher value of $ND(u)$ indicates that the node u is a more effective spreader. If $bn(u) = 0$, it means that node u is better than its neighbors, and in this case, $ND(u) = deg(u)$. Consequently, nodes with the highest degrees will be selected as anchor nodes. When two nodes have equal degrees, the one with the least $bn(u)$ value is considered better. It is worth noting that bn is a vector similar to the vector LI used in the LIR algorithm [6].

2.2 Independent Cascade Diffusion model

In this framework, the method of information dissemination in networks is crucial and has been studied under the title of "dissemination models." In the general framework of all dissemination models, each user has one of two statuses: passive or active. By starting to publish news, only the primary broadcasting nodes are active, and other nodes are inactive. Throughout the propagation process, active nodes attempt to activate other nodes using various methods.

A random diffusion model (with discrete time steps) for a social network $G = (V, E)$ is the random process of generating the active set A_t per broadcast set of primary influencers A.

Dissemination models classify users as either inactive or active, with information released in time steps $t = 0,1,2, ...,$T. In the context of influence maximization, effective nodes (often referred to as influencers) become active at time $t = 0$ and attempt to activate other previously inactive nodes. The nodes that eventually become active at step t are denoted as A_t.

Diffusion models can be categorized into two main types: progressive and non-progressive [7]. In progressive models, an active node remains active in the next steps. Conversely, non-progressive models allow activated nodes to return to an inactive state. Progressive models are commonly employed to simulate the acceptance of new technologies or products, such as the adoption of smartphones or the viewership of a new movie. On the other hand, non-progressive models typically capture the spread of ideas and opinions related to events, where nodes may change their state and opinion based on new information from the network. It's noteworthy that many algorithms designed to maximize the impact of these models tend to utilize forward (progressive) models.

Two of the most common diffusion models are independent cascade diffusion models (IC) [6, 8, 9] and linear threshold (LT) [1], which differ in the way of activating other inactive nodes. Different branches of the influence maximization problem have emerged, with the common goal of determining effective nodes for various purposes. One of the most used model is the Independent Cascade Model (IC).

In IC model, each user v is independently activated by each of their outgoing neighbours (friends) with a probability of influence $\beta(u, v)$ for the edge (u, v). To determine the probability of propagation and weight the edges of the network, the folowing equation

$$\beta(u, v) = 1 - (1 - \alpha)^{W(u,v)} \quad (2)$$

is utilized. In this equation, α holds significance as it represents a parameter governing the speed of node activation, akin to the news that influences the model.

2.3 Problem definition

Here we explain the IM and TGIM problems and what should be known about them.

The influence expansion function: in the social network $G = (V, E)$ for a set of users $S \in V$ and the set of network parameters P is represented by $(\sigma_G, P)(S)$. Its value is equal to the mathematical

expectation of the number of users who are affected by the set S under the parameters of the problem P.

The influence maximization (IM) problem: For a social network G, diffusion model M, and a positive number k, the problem of maximizing the influence involves finding the set A_0 containing k initial nodes such that the spread of the influence $(\sigma_G, M)(A_0)$ is maximized. Here P is the diffusion model M.

The Target Group influence maximization (TGIM) problem: For a social network G, diffusion model M, a positive number k, and a target group H, the problem of maximizing the influence involves finding the set A_0 containing k initial nodes such that the spread of the influence $(\sigma_G, M, H)(A_0)$ is maximized.

The problem revolves around maximizing local influence within a network while targeting a specific number of individuals, target group H, rather than the entire network. The goal is to determine a set of broadcasting nodes, keeping their number within a specified limit k, that will optimize the activation percentage of the predefined target group. This problem formulation encapsulates the challenge of strategically selecting nodes to efficiently influence a specific subset of individuals in the network. The proposed approach tries to use reinforcement learning to solve this TGIM problem.

2.4 Reinforcement Learning

Reinforcement Learning (RL) is a learning paradigm wherein an agent acquires the skill of making sequential decisions by engaging with an environment. Through its actions, the agent obtains feedback in the form of rewards or penalties. The primary objective of RL is to learn an optimal policy that maximizes cumulative rewards over time. The agent explores the environment through trial and error, takes actions based on its current state, and receives feedback. Utilizing this feedback, the agent updates its policy to enhance decision-making for future actions. RL algorithms commonly employ functions or value functions to estimate rewards or expected values associated with different states and actions. These estimations empower the agent to learn and refine its decision-making abilities. Through repeated interactions and learning, the agent's policy gradually converges towards an optimal solution, fostering intelligent and adaptive behavior in complex and dynamic environments.

Q-learning is an algorithm employed in reinforcement learning. It operates in a model-free, value-based, and off-policy manner. The primary objective of Q-learning is to identify the optimal sequence of actions based on the current state of an agent. The letter “Q” signifies quality, representing the value of an action in terms of maximizing future rewards. Unlike model-based approaches that rely on transition and reward functions, Q-learning learns from experience without explicitly using such functions. Instead, it trains a value function to assess the relative importance of different states and guide action selection [10].

Through successive iterations, Q-learning updates its estimate of the value of each action in each state, known as the Q-value, based on the observed rewards and the transition probabilities. By iteratively refining its Q-values, Q-learning converges towards an optimal policy that dictates the best action to take in each state to maximize long-term rewards.

3 RELATED WORK

In Influence Maximization, one typically begins by specifying a predetermined quantity k to represent the number of influencers or spreaders to be chosen. These spreaders can be identified using either local or global methods. Local methods involve selecting each influencer independently, without regard for interactions with other influencers, whereas global methods consider the interplay among all influencers

[5]. Noteworthy local approaches include the degree centrality index (Degree) [1, 11, 12], k-shell decomposition [13-15], semi-local centrality (LC) [16], and the Local Index Rank algorithm (LIR) [6]. Successful global methods encompass the betweenness centrality (BC) index [17], closeness centrality (CC) index [18, 19], eigenvector centrality [20], spreaders inside communities [21-26], IM based on overlapping community detection algorithms [27, 28], the CR method [29], the generalized closeness centrality index (GCC) [26], and HIPA [30]. These methods offer diverse strategies for pinpointing influential nodes in complex networks, thereby optimizing influence spread across various contexts.

Kempe et al. pioneered the exploration of social influence maximization as a combinatorial optimization problem, delving into its computational intricacies under the LT and IC diffusion models [31]. In their investigations, they assumed the social influence function, denoted as σ, to be both submodular and monotone. The proposed greedy strategy is a key aspect of their approach.

To address scalability challenges, Leskovec et al. introduced a Cost-Effective Lazy Forward (CELF) scheme, leveraging the submodularity property of the social influence function. Their key insight was grounded in the observation that the marginal gain in influence spread for any node in the current iteration is constrained by its marginal gain in previous iterations. Exploiting this idea allowed them to significantly reduce the number of evaluations of the influence estimation function (σ), leading to a notable improvement in running time [32]. In CELF, each node u in the network keeps track of some information in a table, including its marginal gain in influence for the current seed set, the node with the highest gain encountered so far, and other details.

Chen, Wei, et al. proposed enhancements to the basic greedy algorithm, including techniques to accelerate influence simulations and enhance the accuracy of influence estimates. Their contributions aimed to make influence maximization more scalable and efficient for large-scale social networks [33].

Wu, Yang, et al. focused on maximizing influence in social networks based on group information (GIM). They applied the greedy algorithm in this context, considering group dynamics and information to optimize influence spread. This work expanded the applicability of influence maximization techniques to scenarios involving group behavior [34]. Cordasco and the team put forward a quick and effective method to choose target sets in undirected social networks. While this method gives the best solutions for trees, cycles, and complete graphs, it particularly stands out for its performance in real-life social networks compared to other existing methods [35].

There are other extensions to the influence maximization, for example, an extension to the traditional Influence Maximization (IM) problem was proposed introducing the concept of a supplementary Independent Cascade (IC) model. This model accounts for scenarios where the diffusion probability of one item increases as users adopt supplementary products in advance [36].

One of the approaches that recently been used in this area is reinforcement learning. For example, in [37] the authors proposed the Q-learning-based DOM (QDOM) framework to address Dynamic Opinion Maximization (DOM) in signed social networks. This framework includes an activated dynamic opinion model based on stateless Q-learning theory for opinion propagation and a Q-learning-based seeding algorithm to identify seed nodes efficiently.

4 PROPOSED METHOD

In this study, the approach involves leveraging reinforcement learning to determine the optimal path from a source node to some destination nodes within a social network. The destinations are some candidate nodes, typically those with high degrees or influential positions. We want to excerpt some of these destinations as influencers (seed nodes). So the final influencers will select from these destination nodes which are capable of effectively reaching and activating a predetermined target group of individuals. In this context, each node in the graph serves as a state, and the objective is to identify the most effective route from the source to the best destination.

Here we use ND index from equation (1) as the local score. V' is the set of destination nodes which are selected based on the local score (ND). We show the size of V' as l.

In Q-learning approach, we should construct a reward matrix which is shown with R. This matrix contains reward values representing the agent's experience when transitioning from one state to another. A value of 0 signifies the presence of an edge between two nodes, while a value of -1 indicates the absence of edges between states. Notably, a value of 100 denotes an edge connected to the goal node, emphasizing its significance in the learning process.

Utilizing the reward matrix R, a corresponding matrix Q can be constructed, and its values are updated iteratively using following equation

$$Q(s,a) = R(s,a) + \gamma \times max(Q(ns,aa) \quad (3)$$

In (2), matrix Q contains Q-values, such that Q(s, a) is the value of state s and action a. R is the reward matrix, γ is the learning rate which is set to 0.9 in our experiments. Also, Q (s, a) is the Q matrix value at state (s) and action (a). R (s, a) is the R matrix value at state (s) and action (a). Q (ns, aa) is the Q matrix values at the next state (ns) and all actions (aa). The formula basically says the value of matrix Q at state (s) and action (a) is equal to the sum of the corresponding value in matrix R and the learning parameter, multiplied by the maximum value of matrix Q for all possible actions in the next state.

After producing Q, for each target node, we can compute the best path to the closest destination. We used a greedy approach for this aim. In this approach, we trace matrix Q for each target node u to find the next node with the highest value in the row corresponding to u. We can continue this process to reach one goal. The founded nodes from the target node to the closest candidate node, construct the path. For some nodes with equal weights, there are more than one closest destination. If matrix P contains target group nodes as rows, and candidate destinations as columns, P(i, j) represents the scaled path length from i-th target to j-th destination. Table 2 shows the Greedy Path Selection pseudocode of the computing path between target node u and the closest goal.

Table 2 Greedy Path Selection

Algorithm: GPS: Greedy Path Selection
Inputs: target group H, matrix Q from reinforcement learning approach
Output: path matrix P
1. for each $u \ in \ H$: path= an array of size n i=0 path[i]=u while path[i] is not in V': i=i+1 path[i]=where(Q[path[i-1],])==max(Q[path[i-1],])) P(destination)=scaled(sum(path))

Then we sum each column of matrix P in vector S. So, vector S contains of score of each goal node. In the last we select k seeds as nodes with the highest value in S. Table 3 states our algorithm steps.

Figure 1 show the graphic abstract of the proposed method on a sample network with 8 nodes. The goals are selected based on ND index and are shown in green color. After running TGRLGP, the score of node 3 is more than 1 to activate the yellow target nodes. Finally, node 3 with red color is selected as the seed node.

Table 3 The Proposed Algorithm TGRLGP

Algorithm: TGRLGP
Inputs: network G, target group H, number of seeds k
Output: Seed nodes
• Phase 1: compute the neighborhood-degree (ND) of each network node based on equation (1). • Phase 2: select goals between the nodes with the highest ND. For example, 0.1 of the network's nodes. • Phase 3: Construct reward matrix R and run Q-learning approach based on (2) to compute matrix Q. • Phase 4: compute P matrix contains the scaled length of the best path between each target node and each destination by GPS approach. • Phase 5: compute vector S contains the sum of each column of P. • Phase 6: select k seed with the highest values in S as seed nodes.

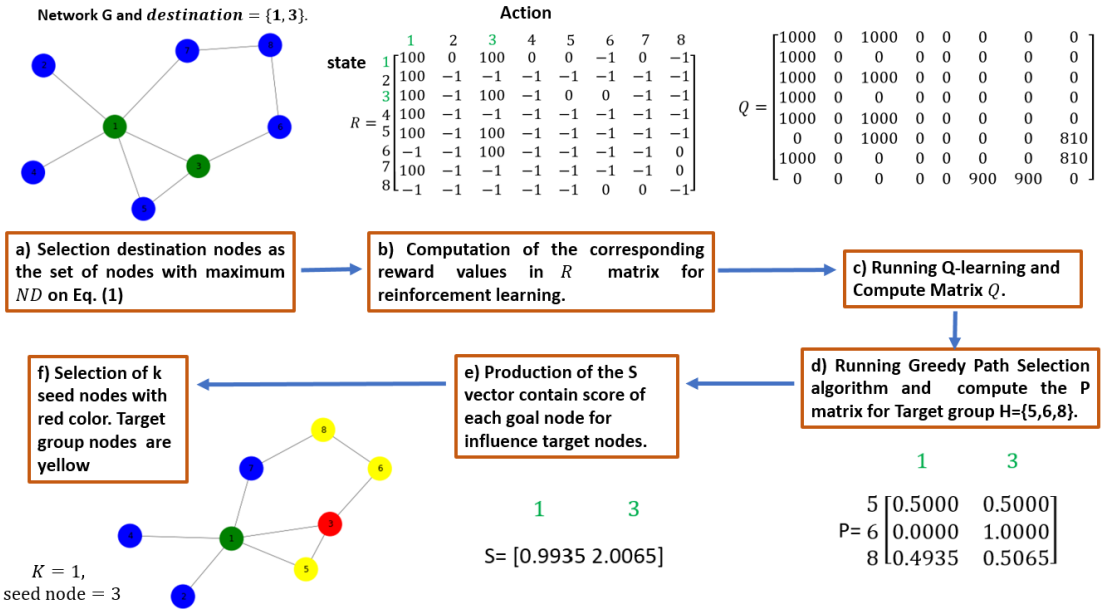


Figure 1: The graphic abstract of the proposed method for a sample network with 8 nodes and 2 destination and k=1.

5 EXPERIMENTS AND RESULT

In this section we compare TGRLGP with some other algorithms on some popular datasets as described in Table 4.

Table 4 The properties of the used datasets

Network's name	Number of nodes (n)	Number of edges (m)
Zachary	34	78
Dolphin	62	159
Jazz	198	2742
Football	115	613

First, we use Zachary karate club network and |goal|=0.15*n, and goal = {34, 1, 33, 3, 2}. Figure 2 shows this network. In this figure, the target group is shown with yellow color, and the red node is the seed from TGRLGP. Green is the seed node for the Degree measure. We can see matrix P corresponds to TGRLGP in Table 5. These values show the ideal probabilities of influencing each target with each destination. The corresponding S vector is as:

S= [0.332, 6.186, 0.344 ,1.36, 0.778]

and the maximum value in S is 6.18 which belongs to node 1. We can see this node is close to the target group, while the node with the highest degree is not an ideal choice.

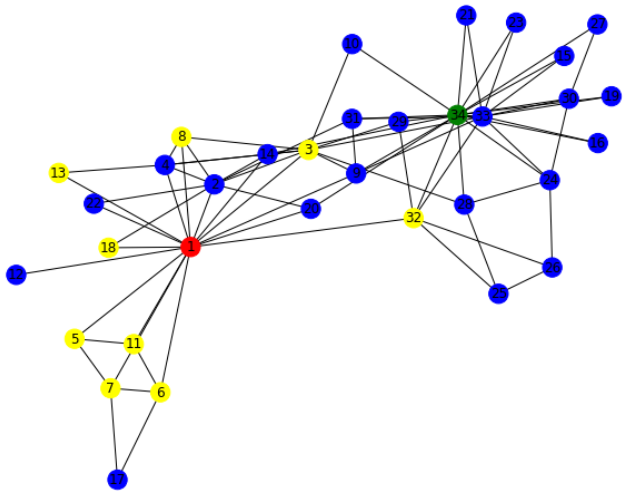


Figure 2: Zachary karate club network.

Table 5 The P matrix for Figure 2

Network's name	Number of nodes (n)	Number of edges (m)
Zachary	34	78
Dolphin	62	159
Jazz	198	2742
Football	115	613

Figure 3 shows the jazz musician network. In this network, we first do clustering and then select some nodes randomly from one cluster as the target group and show them with yellow color.

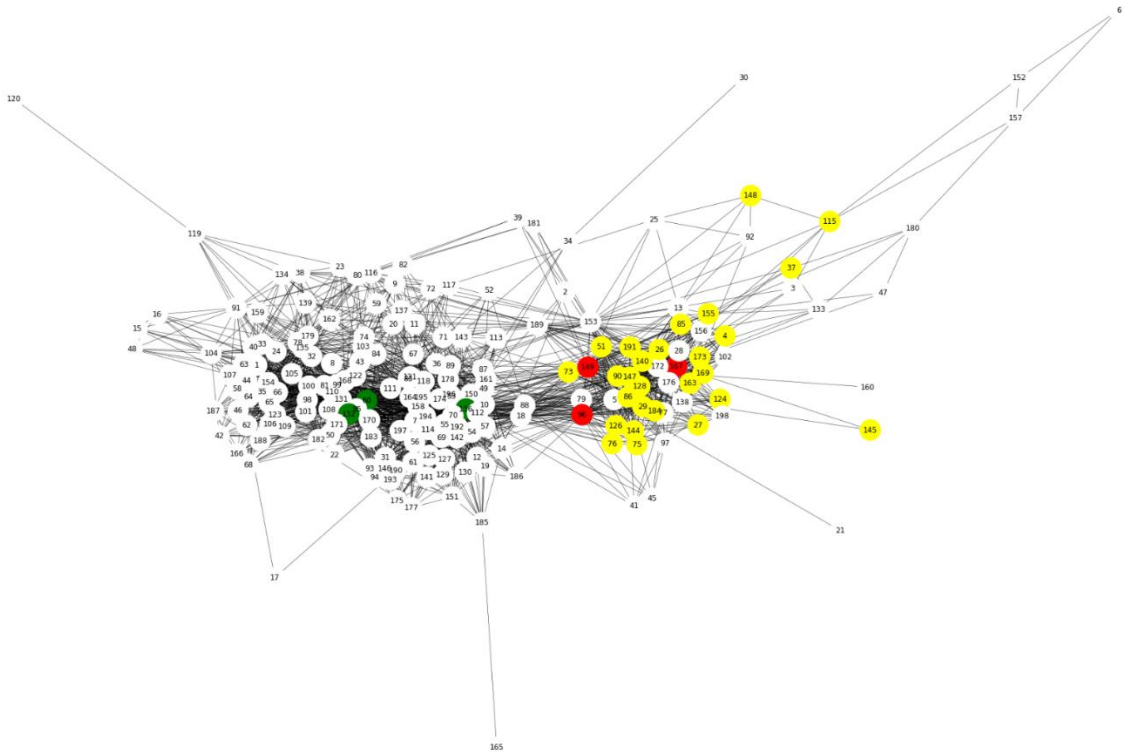


Figure 3: Jazz musician network. Target group nodes are yellow and the spreaders of RLTG are red and Degree influencers are green.

In this figure, the seed nodes from TGRLGP are colored with red which shows that they are located appropriately between target group nodes. Green nodes are high-degree nodes that are selected by the Degree algorithm. They do not correspond to target group nodes and cannot influence them well. The seeds of other algorithms are listed in Table 6.

Besides these ideal graphical results, we compare the algorithms with the Influence Spread (IS) measure. Influence Spread (IS) is one of the popular measures, which counts the final active nodes after a diffusion process. If $A_T(i)$ is the set of final active nodes in the *i-th* experiment (i $\in$ 1,2,3, … , R), under a certain diffusion model, then

$$\mathrm{IS} = \frac{(\sum_{i=1}^{R} A_T(i))}{R} \qquad (4)$$

The larger this measure, the better the result of the algorithm. Table VI shows the values of influence spread (IS) for various algorithms such as Degree, LIR, Local Centrality (LC), GCC, HIPA, and Greedy approach (for TGIM problem) with our Algorithm (TGRLGP). We use IC diffusion model with fixed α which is mentioned in the first column of this table. Also k is number of seeds. In this table, target groups are shown in second column which for Zachary and Jazz networks they correspond to Fig.3 and Fig.4. Seeds columns show the selected seeds by each algorithm. These results show that for various target group nodes, the TGRLGP has the best IS score.

Table 6 Comparison of the proposed method (TGRLGP) with other algorithms based on IS measure.

Network	Target Group	Alg.	Seeds	IS (%)
Zachary network , $\alpha = 0.1 , k = 1$	3, 5, 6, 7, 11, 13, 18, 8, 32	Degree	34	40.15
		LIR	34	38.57
		LC	1	**56.26**
		GCC	6	21.45
		HIPA	34	38.22
		TGRLGP	1	**56.9**
		Greedy (TGIM)	6	21.42
Dolphin network , $\alpha = 0.1 , k = 3$	All nodes	Degree	15, 46, 38	69.49
		LIR	15, 18, 46	81.71
		LC	15, 38, 46	68.59
		GCC	15, 35, 55	74.09
		HIPA	15, 38, 46	69.35
		TGRLGP	15, 18, 21	**85.6**
		Greedy (TGIM)	1, 11, 15	57.96
Football network, $\alpha = 0.09 , k = 2$	95, 20, 56, 21, 32, 97, 18, 80, 30, 36, 19, 114, 81, 35, 77, 55, 28, 88, 98, 43, 59, 96, 83, 72, 31	Degree	68,4	84.69
		LIR	1,2	84,87
		LC	3,16	83.65
		GCC	4,18	84.4
		HIPA	68,2	85.3
		TGRLGP	16,2	**89.12**
		Greedy (TGIM)	36, 28	85.78
Jazz musician network, $\alpha = 0.07, k = 3$	163,173, 76, 145, 86, 184, 37, 149, 148, 51, 167, 85, 4, 124, 90, 144, 26, 75, 128, 29, 115, 191,147, 126,169, 27, 155, 73, 96, 140	Degree	60,132,136	97.2
		LIR	1,2,136	97.32
		LC	60.132,136	97.16
		GCC	54,132,136	97.23
		HIPA	136,60,132	97.14
		TGRLGP	167,149,96	**98.54**
		Greedy (TGIM)	115, 4, 167	97.77

6 CONCLUSION

In this paper, we introduce the Reinforcement Learning Approach for the Target Group influence maximization problem. The proposed algorithm (TGRLGP) is designed to identify influential nodes within a target group by leveraging Q-learning methodology, augmented with the optimal path from each target node to the candidate nodes (destinations) which is computed using Greed Path Mining algorithm. Through this innovative approach, TGRLGP aims to maximize the local coverage of target group nodes, thereby enhancing the potential impact of influence propagation within the network.

To evaluate the effectiveness of TGRLGP, we conducted extensive experiments across four benchmark networks. Additionally, we compared the performance of TGRLGP against six state-of-the-art algorithms commonly used for influence maximization tasks. Our findings consistently demonstrate that TGRLGP achieves superior influence spread in the majority of experimental

scenarios. The success of TGRLGP underscores its efficacy in identifying influential nodes within target groups, offering promising prospects for various applications in network analysis and influence maximization strategies.

REFERENCES

[1] D. K. J. a. T. É. Kempe, "Maximizing the spread of influence through a social network," in Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, 2003.

[2] W. L. L. V. a. C. C. Chen, "Information and influence propagation in social networks," Synthesis Lectures on Data Management, vol. 5, no. 4, pp. 1-177, 2013.

[3] Y. Z. a. D.-Z. D. Wenguo Yang, "Influence maximization problem: properties and algorithms,," Journal of Combinatorial Optimization, vol. 40, pp. 907-928, 2020.

[4] J. S. G. a. W. W. Zhu, "Group influence maximization problem in social networks.," IEEE Transactions on Computational Social Systems , vol. 6.6, pp. 1156-1164, 2019.

[5] N. Binesh and. M. Ghatee., " "Distance-aware optimization model for influential nodes identification in social networks with independent cascade diffusion."," Information Sciences , vol. 581, pp. 88-105 , 2021.

[6] D. J. Y. Z. J. W. W. a. S. G. Liu, "A fast and efficient algorithm for mining top-k nodes in complex networks.," Scientific Reports, vol. 7, p. 43330, 2017.

[7] Y. Z. D. a. T. K.-L. Li, "Real-time targeted influence maximization for online advertisements.," 2015.

[8] J. L. B. a. M. E. Goldenberg, "Using complex systems analysis to advance marketing theory development: Modeling heterogeneity effects on new product growth through stochastic cellular automata," Academy of Marketing Science Review, 2001.

[9] J. L. B. a. M. E. Goldenberg, "Talk of the network: A complex systems look at the underlying process of word-of-mouth.," Marketing letters, 2001.

[10] P. D. Christopher J. C. H. Watkins, "Q-learning,," Machin Learning, vol. 8, pp. 279-292, 1992.

[11] M. F. Z. S. A. M. S. a. H. S. Alshahrani, "Efficient algorithms based on centrality measures for identification of top-k influential users in social networks," Information Sciences, 2020.

[12] N. Arazkhani, M. R. Meybodi and A. Rezvanian , "Influence Blocking Maximization in Social Network Using Centrality Measures," in 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), 2019.

[13] A. S. F. a. H. S. Garas, "A k-shell decomposition method for weighted networks.," New Journal of Physics, vol. 14, no. 8, p. 083030, 2012.

[14] G. Maji, "Influential spreaders identification in complex networks with potential edge weight based k-shell degree neighborhood method.," Journal of Computational Science, vol. 39, p. 101055, 2020.

[15] G. M. S. a. S. S. Maji, "A systematic survey on influential spreaders identification in complex networks with a focus on k-shell based techniques.," Expert Systems with Applications, p. 113681, 2020.

[16] D. L. ̈ L. S. M.-S. Z. Y.-C. a. Z. T. Chen, "Identifying influential nodes in complex networks," Physica A: Statistical Mechanics and its Applications, vol. 391, no. 4, pp. 1777-1787, 2012.

[17] L. C. Freeman, "A set of measures of centrality based on betweenness.," Sociometry, pp. 35-41.

[18] Z. W. X. Z. W. a. Z. Z. Zhao, "A community-based approach to identifying influential spreaders," Entropy, vol. 17, no. 4, pp. 2228-2252, 2015.

[19] N. Arazkhani, M. R. Meybodi and A. Rezvanian, "An Efficient Algorithm for Influence Blocking Maximization based on Community Detection," in 2019 5th International Conference on Web Research (ICWR), 2019.

[20] P. C. A. a. R. S. Dey, "Influence maximization in online social network using different centrality measures as seed node of information propagation," Sa ̄dhana ̄, vol. 44, no. 9, p. 205, 2019.

[21] E. D. G. a. H. A. Bagheri, "Fsim: A fast and scalable influence maximization algorithm based on community de- tection," International Journal of Uncertainty, Fuzziness and Knowledge- Based Systems, vol. 26, no. 03, pp. 379-396, 2018.

[22] M. S. C. D. C. M. L. a. S. B. Gong, "An efficient memetic algorithm for influence maximization in social networks," IEEE Computational Intelligence Magazine, vol. 11, no. 3, pp. 22-33, 2016.

[23] W.-X. Z. C. a. W. J. Lu, "Big social network influence maximization via recursively estimating influence spread," Knowledge- Based Systems, vol. 113, pp. 143-154, 2016.

[24] M. A. M. a. K. M. A. M. A. Jalayer, "A hybrid algorithm based on community detection and multi attribute decision making for influence maximization.," Computers & Industrial Engineering, vol. 120, pp. 234-250, 2018.

[25] W. Z. H. L. S. W. H. D. H. W. C. a. J. Q. Li, "Evolutionary community discovery in dynamic social networks via resistance distance," Expert Systems with Applications, vol. 171, p. 114536, 2021.

[26] H.-L. M. C. X. B.-B. T. M. a. Z. H.-F. Liu, "Identifying multiple influential spreaders based on generalized closeness centrality," Physica A:Statistical Mechanics and its Applications, vol. 492, pp. 2237 -2248, 2018.

[27] H. G. M. F. M. a. S. K. Kalantari, "A new multi-objective optimization model in one-layer weighted network through key nodes identification in overlapping communities," Computers & Industrial Engineering, p. 106413, 2020.

[28] W. Z. K. W. J. a. C. D. Li, "A dynamic algorithm based on cohesive entropy for influence maximization in social networks," Expert Systems with Applications, vol. 169, p. 114207, 2021.

[29] D. W. Y. a. Z. Z. Zhang, "Identifying and quantifying potential super-spreaders in social networks," Scientific reports, vol. 9, no. 1, pp. 1-11, 2019.

[30] S. a. R. M. Kianian, "An efficient path-based approach for influence maximization in social networks," Expert Systems with Applications, p. 114168, 2020.

[31] D. K. J. a. T. É. Kempe, "Maximizing the spread of influence through a social network.," in In Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining,, 2003.

[32] J. K. A. G. C. F. C. V. J. a. G. N. Leskovec, "Cost-effective outbreak detection in networks," in Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining, 2007.

[33] W. C. a. Y. Y. a. L. Zhang, "Scalable Influence Maximization in Social Networks under the Linear Threshold Model," 2010 IEEE International Conference on Data Mining, pp. 88-97, 2010.

[34] Y. e. a. Wu, "Maximizing influence in social networks based on group information," ACM Transactions on Knowledge Discovery from Data (TKDD), 2010.

[35] U. V. Gennaro Cordasco and Luisa Gargano and Marco Mecchia and Adele A. Rescigno, "Discovering Small Target Sets in Social Networks: A Fast and Effective Algorithm," Algorithmica, vol. 80, pp. 1804-1833, 2016.

[36] J. G. W. Y. a. W. W. Y. Zhang, "Supplementary Influence Maximization Problem in Social Networks," IEEE Transactions on Computational Social Systems, vol. 11, pp. 986-996, 2024.

[37] He, "Reinforcement-Learning-Based Dynamic Opinion Maximization Framework in Signed Social Networks," IEEE Transactions on Cognitive and Developmental Systems, vol. 15, pp. 54-64, 2023.

تحلیل و ارزیابی رویکردها و الگوهای ارزیابی قدرت سایبری

حسین باقری [*۱]، محمد رضا کریمی قهرودی [۲]، محمد رضا ولوی [۳]

۱-۲-۳ مجتمع دانشگاهی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، تهران، ایران.

چکیده

قدرت سایبری کشورها از مهم ترین عوامل نشان دهنده توان آن هاست و میزان آن قدرت ملی را تعیین خواهد کرد. از طرفی هرچه قدرت سایبری کشوری بالاتر باشد لزوما امنیت سایبری آن بالاتر بوده و هم چنین اقتصاد، سیاست و عوامل دیگر را هم تحت تاثیر خود قرار خواهد داد. با توجه به اهمیت شناسایی قدرت سایبری کشور ها برای تعیین اهداف، راهبردها، نقشه راه سیاست خارجی بسیار مهم و حیاتی است که الگوی مناسبی برای ارزیابی و تعیین میزان آن داشته باشیم. بههمین خاطر در این مقاله به بررسی و تشریح مفاهیم قدرت سایبری و رویکردهای ارزیابی آن در کشورها پرداخته ایم.

کلمات کلیدی: امنیت سایبری، قدرت سایبری، قدرت ملی، ارزیابی قدرت سایبری.

۱. مقدمه

قدرت سایبری دارای چنان توانمندی است که هم می‌تواند برای حصول نتایج مطلوب در داخل فضای سایبر استفاده شود و هم می‌توان از ابزارهای سایبری آن برای کسب نتایج مطلوب در حوزه‌های دیگر خارج از فضای سایبر استفاده نمود و این خصوصیتی است که دیگر انواع قدرت نیز از آن برخوردار هستند؛ به‌عنوان‌مثال قدرت دریایی به استفاده از منابع در حوزه دریا برای پیروزی در نبردهای دریایی، کنترل نقاط بازرسی کشتیرانی نظیر تنگه‌ها و نمایش حضور در دریاها اطلاق می‌شود اما همچنین توانایی استفاده از دریاها برای تأثیر گذاشتن بر نبردها، تجارت و افکار در خشکی را نیز شامل می‌شود. قدرت سایبری می‌تواند بسیاری از حوزه‌های دیگر - از جنگ تا تجارت - را تحت تأثیر قرار دهد[۱].

سلطه شبکه‌های مدرن، برخی کشورها را قادر خواهد ساخت تا قدرت بیشتر نظامی را به‌وسیله تجهیز نیروهایشان با ابزارهایی برای دکترین و عملیات مدرن حتی بدون امکانات زمینی، هوایی و دریایی گران‌قیمت مورداستفاده ایالات‌متحده کسب نمایند. بزرگنمایی راهبردی فزاینده این کشورها ممکن است آن‌ها را برانگیزد تا به دنبال نفوذ بیشتر در منافع ملی‌شان باشند .برخی کشورها همچنین ممکن است قدرت سایبر را به‌عنوان یک ابزار مؤثر ارعاب و تحمیل علیه همسایگان و رقبا دنبال کنند. قدرت سایبر به‌عنوان ابزار راهبردی، جذاب و برتر ساز است زیرا می‌تواند به‌طور ارزان کسب شود و می‌تواند در هماهنگی با سایر ابزارها یا به‌تنهایی مورداستفاده قرار گیرد. دولت‌ها قبل از شروع هرگونه درگیری بانفوذ در محیط‌های سایبری یکدیگر، فضای نبرد آینده را فراهم می‌کنند، آنچه از طرف قدرت‌هایی چون آمریکا و چین مورداستفاده قرار می‌گیرد؛ اما هیچ‌گاه این دو کشور به وجود دکترین تهاجم سایبری خود آشکارا اعتراف نکرده‌اند. قدرت سایبری با توجه به عوامل متعدد شکل‌گرفته است. درحالی‌که فضای سایبر فقط به‌عنوان یک محیط وجود دارد، همیشه قدرت سایبری به خاطر اندازه‌گیری توانایی استفاده از آن محیط است .فناوری یکی از عوامل است، چراکه توانایی ورود به فضای سایبر چیزی است که با آن می‌شود استفاده از فضای سایبر را امکان‌پذیر نماید[۲, ۳, ۴]. این فناوری به‌طور مداوم درحالی‌که تغییر است و برخی از کاربران کشورها، جوامع و عوامل غیردولتی مشترکین این فضا هستند .قادر به جهش در

[*] **Corresponding author:** دانشجوی دکترای مهندسی کامپیوتر
Email: h-b-۲۰۰۶@gmail.com

فناوری‌های قدیمی برای استقرار و استفاده از امکانات جدید مزیت چشمگیری برای آنان به همراه دارد؛ اما عنصر اطلاعات نزدیک‌ترین ارتباط را به قدرت سایبری داشته و با آن گره‌خورده است.

فضای سایبر و قدرت سایبری ابعاد دستگاه اطلاعاتی از قدرت هستند و راه‌های بی‌شماری برای قدرت سایبری و ایجاد پیوندها و پشتیبانی وجود دارد. در اقتصاد جهانی قرن۲۱، فضای مجازی، مهم‌ترین عامل ایجاد ارتباط بین همه نقش‌آفرینان باهم و افزایش بهره‌وری است. همین امر برای توسعه و بکار گیری فن‌آوری‌های جدید که تأثیر قدرت سایبری در بهره‌برداری، اندازه‌گیری و موفقیت در امور سیاسی و به‌ویژه دیپلماتیک هست را راحت ترکرده است. در حال حاضر بیشتر از همیشه اغلب دولت‌ها و افراد در تعامل با یکدیگر در سراسر مرزهای ملی هستند. عناصر اصلی قدرت سایبری اعم از امواج الکترومغناطیسی، فناوری الکترونیک و زیرساخت یکپارچه ساخته دست انسان هستند. قدرت سایبری وابسته به سخت‌افزار و نرم‌افزار است. سخت‌افزار شامل دستگاه‌های مکانیکی، مغناطیسی، الکترونیکی و الکتریکی و یا شامل یک سیستم کامپیوتری، ازجمله واحد پردازش مرکزی هست. نرم‌افزار شامل برنامه‌های مورداستفاده برای توانایی تولید یک نیروی سایبری ماهر، باکیفیت، یکپارچه، عملیات سایبری است[۵, ۶, ۷].

بااین‌وجود، چنین اثری بستگی به این دارد که چگونه این نیروها مورداستفاده قرار گیرند. ابزارهایی که کشورها با توسعه فنی، استفاده تاکتیکی، زمینه عملیاتی و فرماندهی استراتژیک به‌عنوان متغیرهای اصلی مداخله‌گر در سراسر چارچوب ارزیابی، رویکردشان را با آن سازمان‌دهی می‌کنند. این درنهایت یک دولت را در وضعیت ایجاد قدرت سایبری قرار می‌دهد. قدرت سایبری ممکن است به‌عنوان توانایی تغییر رفتار یک هدف از طریق فضای سایبری درزمینهٔ امنیت ملی تعریف شود[۸, ۹]. این قدرت توسط بازیگران دولتی یا غیردولتی از طریق کمپین‌های سایبری که شامل یک هدف خاص (مجموعه‌ای از رویدادها است با استفاده از اجبار، قانع کردن یا وسایل فنی به‌منظور دستیابی به یک هدف راهبردی به کار گرفته می‌شود. این توانایی را می‌توان به قابلیت‌های متمایز زیر تقسیم کرد:

- مشارکت فعال و نفوذ به‌منظور درک و شکل‌گیری دیدگاه باهدف مدیریت سیاست و گفتمان
- در حوزه سایبری است با استفاده از پروژه قدرت نرم
- اقدامات پدافندی هدفمند و احتمالی برای انکار، تخریب، نابود کردن، اختلال یا انتقال خدمات یا داده‌ها به دستگاه‌ها یا تجهیزات خاص برای دستیابی به اهداف خاص
- تاب‌آوری زیرساخت‌های سایبری از طریق پیش‌بینی مؤثر، جذب، انطباق‌پذیری و بازیابی از طریق یک کمپین سایبر. (که کمپین سایبری می‌تواند شامل تکنیک‌های قدرت سخت، نرم و هوشمند و قابل‌دسترس یک بازیگر دولتی یا غیردولتی است)که از طریق ترکیبی از مکانیسم‌های فنی و سیاستی برای تقویت، انطباق و دفاع از زیرساخت‌ها تحقق یابد. این امر به‌وسیله شناسایی و اطلاعات به‌منظور حفظ آگاهی وضعیتی جامع از دارایی‌های واقع‌شده در فضای نزدیک به دست می‌آید.

در این مقاله، در بخش دوم مروری بر کارهای انجام شده داریم. بخش سوم ارکان و مولفه های قدرت سایبری را بیان نمودیم. در بخش چهارم، رویکردهای ارزیابی قدرت سایبری و در بخش پنجم نیز به تحلیل و ارزیابی قدرت سایبری چین و اروپا پرداختیم.

۲. مروری بر کارهای انجام‌شده

در این بخش مروری بر مهم ترین مقالات منتشر شده داخلی و خارجی در حوزه قدرت سایبری خواهیم داشت. بشارت (۱۳۹۹) به مقاله‌ای به بررسی جنگ سرد نوین و رقابت بین قدرت‌های جهانی در فضای سایبری پرداخته، جنگ سرد نوعی درگیری میان ملت‌هاست که موجب فعالیت نظامی مستقیم نمی‌شود، اما در درجه اول فعالیت‌های اقتصادی، سیاسی، تبلیغاتی، اعمال جاسوسی یا جنگ نیابتی را به همراه دارد که توسط جایگزین‌ها انجام می‌شود که امروزه در سایه فضای

سایبر، رقابت و همکاری دولت‌ها شکل جدیدی یافته است، این پژوهش به دنبال بررسی، نقش فضای سایبر بر رقابت بین قدرت‌های جهانی در دوره جنگ سرد نوین است. به این منظور با بررسی اسناد انجام‌شده، ضمن بررسی جایگاه و کارکرد سیاسی فضای سایبر، به نقش تعاملی سایبر در تعاملات و قدرت‌نمایی پرداخته است و مرور اسناد نشان می‌دهد که فضای سایبر درعین‌حال که شکل قدرت و روابط را تغییر داده و قدرت عمل دولت را محدود کرده است و گروه‌های غیردولتی را قدرتمند ساخته است و روابط بین قدرت‌های جهانی از دوسویه به چند سویه تبدیل کرده است. تمامی جوامع برای بقا و پایداری و توسعه نظام خویش و اصلاح و کسب جایگاه در بین آحاد مردم و جهانیان نیازمند فعالیت و نمایش در این عرصه و بهره‌مندی از قدرت نرم یا به تعبیری بهتر قدرت هوشمند است و کشوری در این رقابت پیروزمند است که از منابع و امکانات و فضای سایبر جهت تأثیرگذاری بر رویدادهای بین‌المللی به نفع خود استفاده کند[۲].

بشارت و ذاکریان (۱۳۹۹) در پژوهشی به بررسی تأثیر قدرت سایبری بر منطقه‌گرایی اعضای شورای همکاری خلیج‌فارس پرداختند، فضای سایبر و قدرت هوشمند در عصر جدید، تأثیر به سزایی در همکاری، رقابت، دشمنی، جنگ و قدرت‌نمایی دارد. فضای سایبر عرصه‌ای برای قدرت‌نمایی گروه‌های مختلف و دولت‌ها است. آن‌ها در این پژوهش به این نتیجه رسیدند که گسترش فناوری‌های اطلاعات و ارتباطات و کاربست آن در تمامی قلمرو حیات بشری، جایگاه فناوری را در حوزه‌های سیاسی، اقتصادی و اجتماعی برجسته ساخته است، به‌گونه‌ای که بافت فناوری‌های را پدیدآورنده که روندها و پویش‌های عرصه داخلی و بین‌المللی از آن تأثیر چشمگیری می‌پذیرند. فضای مجازی اهمیتی همپای جهان واقعی یافته است؛ بنابراین امنیت را دیگر نمی‌توان با ویژگی‌های سنتی که بیشتر مبتنی بر ویژگی‌های جهان فیزیکی است، تعریف کرد. چراکه فناوری اطلاعات و ارتباطات، قوام‌بخش بافت فناورانه هستند که پویش‌های امنیتی در آن متفاوت با ویژگی‌های جهان فیزیکی است. در این بافت فناورانه، مرزهای متصل عرصه داخلی و عرصه بین‌المللی بسیار کم‌رنگ می‌شود، به‌طوری‌که کنترل دولت‌ها بر جریان اطلاعات، ارز و کالا در طول مرزهای سرزمینی از بین می‌رود، چراکه بخش قابل‌توجهی از فعالیت‌های نظامی، اقتصادی و فرهنگی کنشگران غیردولتی در فضای مجازی و با بهره‌گیری از امکانات فناوری‌های اطلاعات و ارتباطات انجام می‌گیرد. توسعه فضای سایبر از اهمیت زیادی در منطقه خلیج‌فارس برخوردار است.

شرایط جدید نظام بین‌الملل باعث شده است که مؤلفه‌های جدیدی در ساختار رسمی بین‌المللی نقش‌آفرینی کنند و کشورها برای تأمین منافع ملی خود ابزارهای جدیدی را به‌کارگیرند که مهم‌ترین آن‌ها را می‌توان بهره‌گیری از قدرت نرم دانست؛ اما در دوران جدید هم قدرت نرم نیز موردانتقاد قرار گرفت و امروزه قدرت هوشمند مطرح است. چنانچه امروزه دولت‌های قدرتمند دریافتند که برای ماندگاری درصحنه بین‌الملل و دستیابی به اهداف خود باید ورای استفاده از قدرت سخت به‌عنوان یک ابزار مهم بازدارندگی، ابزارها و منابع خود، قدرت نرم و هوشمند را ارتقا داده و از طریق اغواگری و تولید جذابیت و با استفاده از قدرت اقناع دیگران را به سمت برآورده سازی اهداف خود ترغیب و جلب نمایند. برای این منظور شناسایی منابع بالقوه قدرت و تبدیل آن‌ها به منابع بالفعل بسیار مفید و ضروری است تا از قدرت سایبری برای همگرایی و توسعه منافع اعضای شورای خلیج‌فارس در سطح داخلی و سطح بین‌المللی استفاده کرد. فضای سایبر تبدیل به محملی برای اطلاع‌رسانی، فراخوانی برای تظاهرات و گردش اطلاعات شده‌اند[۲].

ربیعی و همکاران (۱۳۹۹) به بررسی معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران پرداخته‌اند، امروزه قدرت سایبری دفاعی برای سازمان نظامی در کشور اهمیت ویژه‌ای دارد. با توجه به اینکه چهار حوزهٔ زمین دریا، هوا و فضا از فضای سایبری برای انجام بهتر و کاراتر عملیات خود بهره می‌برند؛ یک الگوی ارزیابی قدرت سایبری برای سازمان دفاعی می‌تواند بینش صحیحی از متغیرهای اثرگذار بر قدرت سایبری دفاعی را در اختیار مدیران و تصمیم گیران این حوزه قرارداد. هدف از این مقاله، شناسایی و الگوسازی مؤلفه‌های ارزیابی قدرت سایبری، برای یک سازمان دفاعی است که درنهایت ۵ مؤلفه ۲۶ شاخص و ۷۸ سنجه برای اندازه‌گیری معرفی گردیده است. الگوی معرفی‌شده بامطالعهٔ الگوهای ارزیابی سایبری و برنامه‌های راهبردی ملی سایبری، مؤلفه‌های قدرت سایبری دفاعی استخراج گردیده، و با استفاده از روش الگوسازی معادلات ساختاری با رویکرد کمترین مربعات جزئی با سنجه‌های

تکوینی، کشف و تعیین اعتبارشده است. فن (تکنیک) نامبرده شده از داده‌های تجربی (قضاوت خبرگان) برای الگوسازی استفاده می‌نماید. روش تحلیل در این نوع الگوسازی تحلیل آماری است که ارتباط و اهمیت مؤلفه‌های الگو را با استفاده از آزمونهای مختلف و دقیق آماری موردسنجش قرار می‌دهد. نتایج سطوح معنادار سنجه‌های (سؤال‌های تحقیق) هر سازهٔ اصلی (ابعاد) و فرعی (مؤلفه‌ها) به میزان حداقل ۹۰٪ تا حداکثر بیش از ۹۹٪ (نزدیک به ۱) را نشان می‌دهد. این مقادیر برای معناداری اتصال سازه‌های اصلی به یکدیگر و اتصال سازه‌های فرعی به اصلی نیز برقرار می‌بخشد. همچنین مقادیر R برای سازه‌های اصلی نشان‌دهنده تبیین واریانس توسط متغیرهای پیش‌بینی و حد مطلوب کسب‌شده برای آن‌ها می‌بخشد؛ بنابراین اعتبار متغیرهای انتخاب‌شده و الگوی ترسیم‌شده برای آن‌ها (روابط و چگونگی اثرگذاری متغیرها) مایید گردیده است[۴].

رمضان زاده و همکاران (۱۳۹۹) در پژوهشی به بررسی ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی سایبری پرداخته‌اند، ازجمله روش‌های مقابله با تهدیدات سایبری، فراهم نمودن زمینه ایجاد بازدارندگی سایبری است. هدف از این پژوهش، ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی سایبری است. جامعه آماری، متخصصان حوزه سایبر بوده که با رعایت ملاحظات امنیتی متشکل از ۴۴۰ نفر و حجم نمونه شامل ۳۹۰ نفر است. نوع پژوهش، کاربردی است. روش پژوهش، در مرحله اول به علت شناخت ابعاد و مؤلفه‌های مدل مفهومی، اکتشافی است و در مرحله دوم به علت انجام تحلیل‌های آماری، تحلیلی است. روش گردآوری داده‌ها، میدانی و ابزار گردآوری داده‌ها، پرسش‌نامه است. از روش تحلیل آماری، تی - تک نمونه‌های استفاده‌شده است. نتیجه آنکه مدل مفهومی دارای مؤلفه‌های پنج‌گانه: پشیمان‌کنندهٔ دشمن، استمرار عملیات، پاسخ به تهاجم، استحکام سازی و بازیابی است. همچنین، مؤلفه استمرار عملیات، از اولویت بالاتری نسبت به سایر مؤلفه‌ها برخوردار است. استفاده از نتیجه این تحقیق به‌وسیله معاونت فاوا می‌تواند برای شناسایی و اولویت‌بندی سرمایه‌های سایبری نیروهای مسلح به‌منظور ایجاد زمینه بازدارندگی سایبری در مقابل تهدیدات، مفید باشد[۵].

آریان (۱۳۹۷) در پایان‌نامه‌ای با عنوان شناسایی عوامل قدرت هوشمند در فضای سایبری به بررسی سؤالات زیر پرداخته است: قدرت سایبری چیست؟ چگونه می‌توان قدرت را به‌مثابه پدیده نوظهوری در راستای هم‌اندیشی امنیتی در بازه‌های زمانی مختلف دانست؟ نتایج به‌دست‌آمده حاکی از آن است که عوامل فضای سایبری به‌صورت معنادار در تمامی عوامل قدرت هوشمند، اول بر عامل کنترل دوم بر نوآوری، سوم بر مدیریت زمان هوشمند، چهارم بر مشارکت و پنجم بر راهبرد (استراتژی) دارد. آزمون فریدمن نشان می‌دهد که با توجه به نتایج به‌دست‌آمده اولویت‌بندی عوامل فضای سایبری و قدرت هوشمند ارتباط معناداری با یکدیگر دارند[۶].

زابلی زاده و وهاب پور (۱۳۹۷) در پژوهشی با عنوان: قدرت و بازدارندگی در فضای سایبری به بررسی این سؤالات پرداخته است: آیا کشورها می‌توانند در فضای سایبر دیگران را از آسیب رساندن به امنیت خود بازداشته و منصرف کنند؟ چگونه می‌توان مهاجمان سایبری را از اقدامات مغایر امنیت ملی و بین‌المللی بازداشت؟ نتایج مقاله: سه مؤلفه اساسی درزمینهٔ بازدارندگی در فضای سایبری به دست آمد. همچنین نتیجهٔ دیگر این است که بدون عملیات تلافی‌جویانه، بازدارندگی در فضای سایبری چندان مؤثر نیست[۱۰].

هلیلی و ولوی (۱۳۹۷) پژوهشی با عنوان ارائه الگوی راهبردی ارتقای قدرت سایبری جمهوری اسلامی ایران در تراز جهان انجام داده و به بررسی این سؤالات پرداخته‌اند: الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی چگونه است؟ ماهیت، اجزا، منابع، ویژگی‌ها، پیامدها و دستاوردهای قدرت سایبری چیست؟ ابعاد، مؤلفه‌ها و شاخص‌های مؤثر در ارتقای قدرت سایبری کدام‌اند؟ شاخص‌های کلان سنجش قدرت سایبری در تراز جهانی کدام‌اند؟ نتایج رساله: پس از مروری بر مفاهیم قدرت و قدرت سایبری، ارکان جهت ساز قدرت سایبری احصا و ابعاد قدرت سایبری تدوین و الگوی راهبردی ارائه گردید[۱].

هلیلی و همکاران (۱۳۹۷) به بررسی شناسایی عوامل و مؤلفه‌های اثرگذار بر تدوین رهنامهٔ قدرت سایبری ج.ا.ایران مبتنی بر سیاست‌های ابلاغی و اسناد بالادستی پرداخته‌اند، قدرت سایبری مجموعه‌ای از توانایی‌های مبتنی بر فضای سایبر است که به‌منظور پشتیبانی از قدرت ملی و دستیابی به اهداف راهبردی در فضای سایبر و خارج از آن قابل‌استفاده است. برنامه‌ریزی راهبردی و سیاست‌گذاری کلان در این حوزه، نیازمند تدوین اصول راهنما، به‌منظور هدایت و راهبری فعالیت‌ها و اقدام‌های لازم جهت دستیابی به اهداف و منافع ملی است که در قالب رهنامهٔ قدرت سایبری به دست می‌آید. در این مقاله، هدف اصلی، شناسایی عوامل و مؤلفه‌های اثرگذار بر تدوین رهنامهٔ قدرت سایبری در سیاست‌های ابلاغی و اسناد بالادستی ج.ا.ایران است. این تحقیق، ازنظر هدف، بنیادی و ازنظر ماهیت و چگونگی گردآوری داده‌ها، توصیفی-موردی است. رویکرد مورداستفاده برای تجزیه‌وتحلیل داده‌ها نیز، کیفی و مبتنی بر روش تحلیل مضمون و فرا ترکیب است. اطلاعات گردآوری‌شده پس از فیش‌برداری توسط نرم‌افزار مکس کیودا موردبررسی قرارگرفته است. یافته‌های تحقیق نشان می‌دهد که مقابله با سلطهٔ جهانی، مواجههٔ هوشمندانه و اثرگذار در تعاملات جهانی، از اصول اساسی در تدوین رهنامهٔ قدرت سایبری در سیاست‌های ابلاغی است. همچنین در اسناد بالادستی، بر شکل‌دهی به قواعد و مقررات حقوقی و قضایی سایبر و ترویج فرهنگ و ارزش‌های اسلامی تأکید شده که مبنایی برای سیاست‌ها و هدف‌های راهبردی در رهنامهٔ قدرت سایبری است[۸].

قوچانی خراسانی و حسینی (۱۳۹۶) در پژوهشی با عنوان حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری، به بررسی این سؤال پرداخته است: چگونه می‌توان با استفاده از مفاهیم حاکمیت و حاکمیت شبکه‌ای مدلی برای حاکمیت در فضای سایبری ارائه نمود؟ نتایج رساله: عدم درک اهمیت فرهنگ پژوهشی در حوزه سایبری در بدنهٔ حاکمیتی کشور، نبود یک نقشه راه مدون برای امنیت سایبری کشور، تدوین نظام‌های قراردادی صحیح میان نهادهای حاکمیتی و خصوصی با حفظ حقوق مالکیت معنوی یکی از نیازهای مهم درزمینهٔ حاکمیت در حوزهٔ سایبری است[۱۱].

شهبا (۱۳۹۶) در پژوهشی با عنوان بررسی نقش قدرت سایبری در هندسه قدرت جمهوری اسلامی ایران، به بررسی این سؤالات پرداخته است: قدرت سایبری و تأثیرگذاری آن بر جامعه‌ی ایران به چه میزان است؟ آیا هندسهٔ قدرت سایبری حکومت جمهوری اسلامی ایران مؤثرتر بوده است یا سایر گروه‌ها؟

پژوهشگران مدیریت راهبردی امنیت فضای سایبری، دانشگاه عالی دفاع ملی در سال ۱۳۹۵ در مطالعه گروهی با عنوان: طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن، به بررسی این سؤال پرداخته است: نظام دفاع سایبری کشور چگونه است و الزامات تحقق آن کدام‌اند؟ نتایج مقاله: برای شکل‌گیری دفاع سایبری منسجم و یکپارچه در کشور ضرورت دارد دستگاه‌ها و سازمان‌های مختلفی در سطح کشور با مدیریت واحد تعامل و همکاری نزدیک داشته باشند. ساختار برخی از این نهادها که در دفاع سایبری نقش دارند از قبل ایجادشده است (مانند سازمان صداوسیما). برخی سازمان‌ها نیز اگرچه به‌صورت مستقل در کشور وجود ندارد، ولی وظایف آن‌ها در سازمان‌ها و وزارتخانه‌های مختلف انجام می‌پذیرد مانند تحقیقات، آموزش، استانداردسازی، بومی‌سازی تجهیزات سایبری با همکاری وزارتخانه‌های علوم، تحقیقات و فناوری، صنعت، معدن و تجارت قابل‌دستیابی خواهد بود. بخش سوم نقش‌های جدیدی هستند که نهادی در کشور برای آن پیش‌بینی‌نشده است (مانند متولی هماهنگی امنیت سایبری در قوای سه‌گانه)؛ بنابراین لازم است برای فرآیندهای مشابه نهادهایی ایجاد گردد[۱۱] .

درویشی (۱۳۹۴) در پژوهشی با عنوان ارتش سایبری و پیش‌بینی بعد از حمله سایبری به بررسی این سؤالات پرداخته است: تروریسم سایبری چیست؟ در صورت، بروز حملات سایبری وظیفهٔ ما چیست؟ نتایج رساله: ارتش ضد سایبری با شعار پیشگیری قبل از درمان عنوان می‌شود و ما با قبول حرکت سیل‌آسا و فزاینده فناوری و وابستگی بیش‌ازپیش به اینترنت یک اصل در امنیت اطلاعات و محافظت از کشور و زیرساخت‌ها بیان می‌شود. ابتدا باید تعریف جامعی از تروریسم سایبری و حملات سایبری داشته باشیم و راه‌های مختلف را بررسی نماییم. گام بعدی ما می‌تواند یک‌قدم به جلوتر و دید بدبینانه‌ای باشد و آن اینکه، یک حمله سایبری اتفاق افتاده باشد و بدانیم وظیفهٔ ما چیست[۱۴].

وو و همکارانش (۲۰۲۰) در پژوهشی به بررسی شاخص ملی قدرت سایبری* ۲۰۲۰ پرداخته‌اند، بلفر، شاخص ملی قدرت سایبری را باقابلیت‌های سایبری ۳۰ کشور در چارچوب هفت هدف ملی، با استفاده از ۳۲ شاخص هدف و ۲۷ شاخص قابلیت با شواهد جمع‌آوری‌شده از داده‌های عمومی، اندازه‌گیری می‌کند. برخلاف شاخص‌های موجود مربوط به سایبر، ما معتقدیم هیچ اندازه‌گیری واحدی برای قدرت سایبری وجود ندارد. قدرت سایبری از اجزای متعددی تشکیل‌شده است و باید در چارچوب اهداف ملی یک کشور موردتوجه قرار گیرد. ما برای سنجش قدرت سایبری از رویکرد همه کشورها استفاده می‌کنیم. با درنظرگرفتن "در سراسر کشور"، ما تمام جنبه‌های تحت کنترل یک دولت را تا آنجا که ممکن است شامل می‌کنیم. ارزیابی ما، هم برای اندازه‌گیری قدرت و هم برای اندازه‌گیری پتانسیل سنجش شده است، پس از ارزیابی یک نمره نهایی فرض می‌کند و سپس تعیین می‌کند که دولت آن کشور می‌تواند از این قابلیت‌ها به‌طور مؤثر استفاده کند یا خیر[۵].

۳.ارکان و مولفه های قدرت سایبری

تقسیم فضای سایبری به فضای نزدیک، فضای میانی و فضای دور، فرصتی برای حفظ آگاهی وضعیت سایبری و توانایی مقابله در برابر حملات سایبری ارائه می‌دهد. همچنین از طریق پیش‌بینی، جذب، سازگاری و بازیابی از حملات به تاب‌آوری که یک عامل مهم در ایجاد قدرت سایبری است کمک می‌کند. ترکیب آگاهی وضعیتی با ارزیابی لایه‌های مختلف فضای سایبری می‌تواند فهم فضای سایبری و نحوه برنامه‌ریزی قدرت سایبری را بهبود بخشد. ازآنجاکه از فضای سایبر برای اعمال قدرت سخت از طریق تهدید و اجبار نیز استفاده می‌شود؛ اولویت‌بندی و تخصیص منابع برای بهره‌برداری از این فضا نیز اهمیت زیادی دارد[۱۵, ۱۶, ۱۷, ۱۸].

جدول۱. مؤلفه‌های قدرت سخت و نرم سایبری[۲۳]

	بیرون از فضای سایبر	درون فضای سایبر
ابزارهای اطلاعاتی	**سخت**: حملات ممانعت از خدمات (DoS) با استفاده از بات نتها **نرم**: تعیین هنجارها و استانداردها	**سخت**: حمله به سامانه‌های کنترل نظارت و جمع‌آوری اطلاعات (اسکادا) **نرم**: تبلیغات رسانه‌ای برای تأثیر بر افکار عمومی
ابزارهای فیزیکی	**سخت**: نظارت حکومت‌ها بر شرکت‌ها **نرم**: فراهم‌سازی زیرساخت برای کمک به فعالان حقوق بشر	**سخت**: بمباران تجهیزات مسیریابی و قطع کردن کابل‌ها **نرم**: راه‌اندازی تظاهرات علیه شرکت‌های اینترنتی

مصداق‌های قدرت سایبری در ابعاد چهارگانه عبارت‌اند از[۱۹, ۲۰, ۲۱]:

- اجباری: کنترل ماشین‌ها یا شبکه‌ها، توسعه منبع غیرمادی قدرت
- نهادی: قرار دادن هنجارها و استانداردها، تحت تأثیر قرار دادن مخاطبان خارجی از طریق نهادهای رسانه‌ای
- ساختاری: تغییر ساختارها در فضای سایبر (مثل سلسله مراتبی به شبکه‌ای)
- مولد: تقویت گفتمان‌های موجود، تولید و انتشار گفتمان‌های جدید

*National Cyber Power Index (NCPI)

جدول ۲. سه لایه افقی فضای سایبر[۲۲]

لایه (محیط)	توصیف
فضای نزدیک	شبکه‌های محلی و سامانه‌هایی که برای پشتیبانی زیرساخت ملی حیاتی و خدمات است و فضای نزدیک به‌صورت پیش‌فرض توسط مؤسسات دولتی یا ملی کنترل و محافظت می‌شوند.
فضای میانه	شبکه‌ها و سامانه‌های حیاتی برای دسترسی به فضای سایبر جهانی که کنترل یا محافظت محلی روی آن‌ها وجود ندارد. معمولاً این‌ها ممکن است ازنظر جغرافیای در فاصله دوری قرارگرفته باشند و متعلق به یک شرکت تجاری خارجی یا یک دولت سوم (شخص ثالث) باشند.
فضای دور	شبکه‌ها و سامانه‌هایی که فضای نزدیک رقیب یا دشمن را تشکیل می‌دهند و باید به‌عنوان بخشی از صحنه نبرد به‌منظور طرح‌ریزی قدرت و نفوذ از طریق فضای سایبر کنترل‌شده یا تحت تأثیر قرار گیرند.

شلدون فضای سایبر را در یک مدل سه‌بعدی برحسب سه لایه افقی و پنج لایه مودی مطابق موارد زیر در نظر گرفته است:

۱. لایه زیرساخت: این لایه شامل سخت‌افزار کامپیوتر، سرورها، اجزای شبکه، کابل‌ها، ماهواره و دیگر تجهیزات خصوصی مانند لپ‌تاپ، تبلت و تلفن‌های هوشمند است. در این لایه، پارامترهای قابل‌اندازه‌گیری میزان دسترسی به اینترنت، تعداد تلفن همراه، تعداد آی اس پی ها برحسب جمعیت و تعداد گیت وی ها جهت برقرار اتصال جهانی است.

۲. لایه فیزیکی: این لایه شامل ویژگی‌های قابل‌کنترل و حاکمیت تجهیزاتی ارتباطی است که برای انتقال داده از طریق لایه زیرساخت استفاده می‌شوند؛ مانند مشخصات طیف الکترومغناطیسی، میزان پهنای باند و سرعت انتقال دیتا، روش‌های انتقال دیتا از طریق بلوتوث یا لینک‌های ماهواره‌ای بین‌المللی.

پارامترهای قابل‌اندازه‌گیری در این لایه میزان استفاده از کابل مسی در مقایسه با فیبر نوری پرسرعت، میزان پوشش تلفن همراه، میانگین مصرف دیتا برای کاربران و هزینه دسترسی و ... است.

۳. لایه نحوی: لایه نحوی، شامل دستورالعمل‌هایی است که طراحان و کاربران به ماشین و پروتکل‌ها می‌دهند تا از طریق آن ماشین‌ها با یکدیگر تعامل داشته باشند. در این لایه داده‌ها برای سهولت مخابره از طریق لایه زیرساخت فرمت بندی می‌شوند. این لایه شامل پروتکل‌های مخابراتی، اجزای نرم‌افزاری و الگوریتم‌های مسیریابی است. مقادیر قابل‌اندازه‌گیری در این لایه شامل سطح رمزنگاری بکار گرفته‌شده، تعداد کامپیوترهای محافظت‌شده با آنتی‌ویروس، تعداد ماشین‌های آلوده و تعداد نام‌های دامنه ثبت‌شده است.

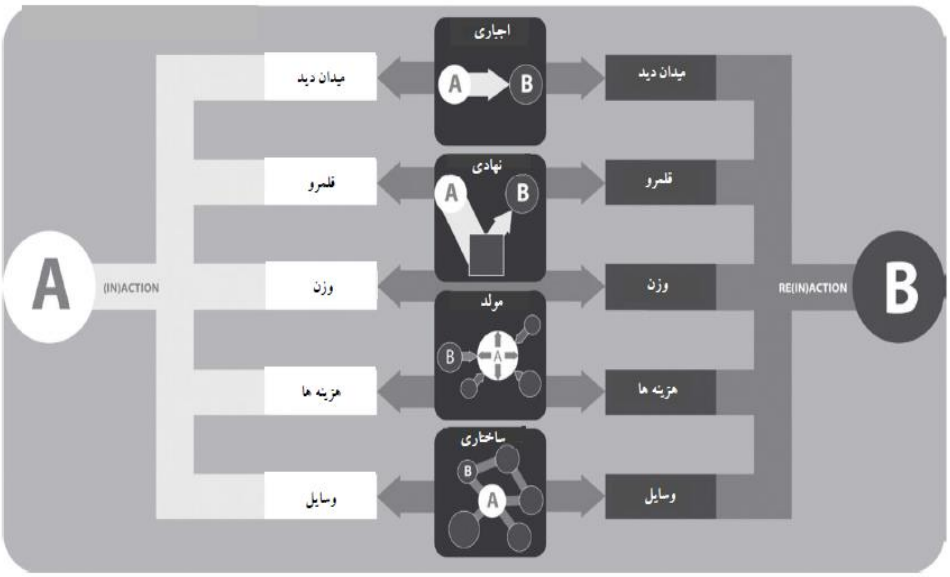
۴. لایه معنایی: در این لایه، اطلاعات به شکل قابل‌استفاده و محسوس توسط کاربران انسانی تبدیل می‌شود. اجزایی مانند نوع و محبوبیت رابط کاربری، ویژگی‌های زبان‌شناختی نرم‌افزار کاربردی، فرهنگ و فاکتورهای انسانی در نظر گرفته‌شده در طراحی آن در این لایه اهمیت دارند. شاخص‌های از تجارت آنلاین، درصد (GDP) قابل‌اندازه‌گیری در این لایه شامل نسبت تولید ناخالص داخلی صفحات وب تولیدشده به زبان محلی (بومی)، درصد افراد فعال و کاربران شبکه‌های اجتماعی، سطوح جرائم سایبری، میزان و اثربخشی قانون و اجبار به این مد چهار لایه‌ای از فضای سایبر است.

۵. لایه انسانی: این لایه مبنای اساس درک فضای سایبر و قدرت سایبری است؛ که نگهداری، بهره‌برداری و تخریب عامل انسانی را دربرمی گیرد. علاوه بر آن تفسیر لایه معنایی که اطلاعات مفید و قابل‌فهم را برای کاربران انسانی فراهم می‌کند به فرهنگ و زبان کاربران بستگی دارد. این مسئله نحوه استفاده مفید یا سوءاستفاده از کامپیوتر را در جوامع مختلف مشخص می‌سازد. علاوه بر سه لایه‌های افقی، پن لایه مودی نیز برای تعریف فضای سایبر در نظر گرفته‌شده است.

جدول ۳. نمونه‌ای از شاخص‌های لایه‌های مختلف فضای سایبر[۲۵, ۲۴]

	فضای دور	فضای میانه	فضای نزدیک
انسانی	گروه‌های جهادی	هکرهای ناشناس	کارکنان دولت
معنایی	برنامه‌های کاربردی رسانه اجتماعی	نرم‌افزار مسیریابی	نرم‌افزار تولید ویدئو
نحوی	فایل‌های ویدئویی	پروتکل TCP/IP	فایلهای ویدئویی
فیزیکی	مخابرات فرکانس رادیویی با شبکه‌های تلفن همراه	نور در کابل فیبر نوری و مخابرات فرکانس رادیویی با ماهواره و لینک‌های مایکروویو	الکترون‌ها در کابل اترنت و نور در کابل‌های فیبر نوری
زیرساختی	شبکه تلفن همراه و تلفن هوشمند	لینک‌های ماکروویو و ماهواره، کابل فیبر نوری در زیردریا، زیرساخت ارائه خدمات اینترنتی	مجموعه تولید ویدئو رایانه رومیزی و شبکه‌های محلی

کنترل فضای نزدیک محلی برای محافظت ملی یا منافع ملی حیاتی است و از طریق سرزمین بدون انسان (لایه میانی) قدرت در فضای دور که فضای نزدیک کشور هدف یا رقیب است نمایش داده می‌شود. تحلیل قوت و ضعف هرکدام از این سه ناحیه اطلاعاتی در مورد بردارهای حمله که ممک است برای کاهش نفوذ و توانایی فعالیت آزادانه در فضای سایبر استفاده شود را فراهم می‌سازد. در ترکیب لایه‌های مودی با لایه‌های افقی فضای نزدیک، میانه و دور، شلدون میزان کنترل این لایه‌ها را قدرت سایبری توصیف می‌کند. بخش‌های زیادی از فضای سایبر، مانند زیرساخت سخت‌افزاری و ارتباطی، شبکه‌ها و برنامه‌های نرم‌افزاری در خارج از مرزهای جغرافیایی کشورها قرار دارد و تسلط کامل بر آن‌ها عملاً غیرممکن است[۲۶, ۲۷, ۲۹].



شکل ۱. چارچوب مفهومی تحلیل قدرت سایبری

۴. رویکردها و مدل های ارزیابی قدرت سایبری

ارزیابی راهبردی قدرت سایبری به معنی سنجش، ارزش‌گذاری و قضاوت در خصوص شاخص‌های کلان قدرت سایبری هست و به‌طورکلی دو رویکرد عمده در ارزیابی قدرت وجود دارد[۳۰].

۱) رویکردهای تک متغیره محاسبه قدرت که بر اساس یک متغیر یا شاخص واحد، قدرت موردمحاسبه قرار می‌گیرد.
۲) رویکردهای چند متغیره ترکیبی سنجش قدرت که چندین متغیر در داخل یک مدل مفهومی یا ریاضی قرارگرفته و سپس بر اساس آن‌ها قدرت موردسنجش قرار می‌گیرد.

۴-۱ رویکرد تک متغیره محاسبه قدرت ملی

برخی اندیشمندان تنها بر روی یک عامل به‌عنوان ملاک و معیار اندازه‌گیری قدرت تأکید کرده و به‌وسیله آن به ارزیابی قدرت پرداخته‌اند. ریچارد مریت و دینا زینز در بررسی رویکردهای سنتی مختلف به‌اندازه گیری قدرت، چند تلاش مشخص برای اندازه‌گیری قدرت را که در آن‌ها برای اجتناب از پیچیدگی مسئله صرفاً به یک متغیر کلی تأکید شده، شرح داده‌اند.

۴-۲ رویکردها و مدل‌های چند متغیره ترکیبی(محاسبه قدرت ملی)

یکی دیگر از روش‌های محاسبه قدرت ملی استفاده از چند متغیر و ترکیب آن‌ها و طراحی یک مدل چند متغیره است. طراحی مدل‌های ترکیبی(چند متغیره)توسط صاحب‌نظران به دو شکلی متفاوت مدل‌های ریاضی و مدل‌های مفهومی صورت گرفته است. در شکل او یعنی سنجش قدرت ملی کشورها بر اساس یک مدل ریاضی، ابتدا متغیرهای موردنظر انتخاب می‌شود و سپس با طراحی یک مدل ریاضی نوع رابطه و ترکیب متغیرها مشخص می‌شود. درنهایت بر اساس این مدل ریاضی قدرت ملی کشورها موردسنجش قرار می‌گیرد. به‌عنوان نمونه می‌توان به مدل‌هایی که توسط کلی فورد جرمن و فوکس طرح‌شده اشاره کرد. در نوع دوم یعنی مدل‌های مفهومی، چند متغیر به‌عنوان مهم‌ترین و عامل مؤثر بر قدرت ملی کشورها توسط طراح مدل انتخاب‌شده و سپس قدرت کشورها بر اساس امتیازات کسب‌شده در آن گروه از متغیرها موردسنجش قرار می‌گیرد. البته در این روش فرمول خاصی که نشان‌دهنده نحوه ترکیب و نوع رابطه متغیرها باشد ارائه نمی‌شود. به‌عنوان نمونه می‌توان به مدل مفهومی ارائه‌شده توسط سینگر اشاره کرد که با توجه به سهم جهانی هر کشور از متغیرهایی مانند تعداد جمعیت، تولید آهن و ...به سنجش قدرت ملی کشورها پرداخته است. درحالی‌که مدل‌های گوناگون را می‌توان برحسب تعداد متغیرهای به‌کاررفته در آن‌ها و چگونگی ارتباط داخلی آن‌ها از همدیگر متمایز کرد، ولی آشکارترین ویژگی آن‌ها تنوع آن‌هاست؛ یعنی هر مدل، برحسب تعداد کشورهایی که مورد ارزیابی واقع‌شده و چارچوب زمانی مقایسه و پیچیدگی فرمول‌های مورداستفاده، با مدل‌های دیگر فرق دارد در ادامه هرکدام از مدل‌های مفهومی و ریاضی موردبررسی و نقد قرار می‌گیرد[۳۱, ۳۲].

مصداق‌های قدرت سایبری در ابعاد چهارگانه عبارت‌اند از:

- اجباری: کنترل ماشین‌ها یا شبکه‌ها، توسعه منبع غیرمادی قدرت
- نهادی: قرار دادن هنجارها و استانداردها، تحت تأثیر قرار دادن مخاطبان خارجی از طریق نهادهای رسانه‌ای
- ساختاری: تغییر ساختارها در فضای سایبر (مثل سلسله مراتبی به شبکه‌ای)
- مولد: تقویت گفتمان‌های موجود، تولید و انتشار گفتمان‌های جدید

در این مدل، برای دستیابی به رویکرد جامع در تحلیل قدرت سایبری، ابعاد پنج‌گانه میدان دید (اهداف و نواحی متأثر از قدرت)، قلمرو (محدوده موردنظر برای اعمال قدرت و بازیگران)، وزن (میزان اثربخشی قدرت)، هزینه (هزینه‌های موردنیاز برای اعمال قدرت) و ابزارها منابع مادی برای کسب یا اجرای قدرت) در نظر گرفته‌شده است. برخی از مصداق‌های قدرت سایبری در این ابعاد عبارت‌اند از:

- میدان دید: در فضای سایبر هدف یک دولت از اقدامات سایبری باید در برآورد قدرت سایبری مشخص باشد. مثلاً در استفاده یک دولت از تولید، خرید یا توزیع نرم‌افزارهای مخرب مانند بات نت تنها جنبه بازدارندگی آن یا مداخله در دیگر کشورها باشد.
- قلمرو: این مسئله در مورد نوع و تعداد بازیگرانی است که تحت تأثیر قدرت قرار می‌گیرند. مثلاً یک دولت با کنترل‌های سخت‌روی رسانه‌ها یا سانسور در قلمرو فضای سایبر امکان دسترسی بازیگران خاصی به استفاده از این فضا را نمی‌دهد. یا مسائل اجتماعی و فرهنگی مانعی برای ورود بازیگران به فضای سایبر می‌شود.
- وزن: احتمال اثربخشی فعالیت‌های انجام‌شده در فضای سایبر برای افزایش قدرت را نشان می‌دهد. احتمال دستیابی به اهداف خاص توسط یک بازیگر می‌تواند نشان‌دهنده قدرت بیشتر او باشد.
- هزینه: هرچه یک بازیگر بتواند نفوذ ارزان‌تری را روی بازیگر دیگر داشته باشد از قدرت بالاتری برخوردار است. میزان هزینه به هر دو بازیگر بستگی دارد. در فضای سایبر هزینه پایین از ابعاد جذاب هزینه کمی دارد اما ممکن است خسارت مالی بزرگی DDoS دستیابی به قدرت است. مثلاً یک حمله را ایجاد کند. حملات سطح بالاتر مانند استاکس نت، فلیم یا دوکو ازنظر مالی و سیاسی اثربخشی یا وزن زیادی دارند.
- ابزارها: به ابزارهای مورداستفاده برای اجرای نفوذ و قدرت اشاره دارد. ابزارهای قدرت ممکن است در ابعاد سیاسی، اطلاعاتی، اقتصادی یا نظامی بکار گرفته شود.

۳-۴ مدل‌های ترکیبی ریاضی محاسبه قدرت ملی

در این روش، ابتدا متغیرهای موردنظر مؤثر بر قدرت ملی توسط طراح مدل انتخاب می‌شود. سپس با طراحی یک مد ریاضی، نوع رابطه و ترکیب متغیرها مشخص می‌شود. درنهایت بر اساس این مد ریاضی قدرت ملی کشورها موردسنجش قرار می‌گیرد. مهم‌ترین مدل‌های ترکیبی محاسبه قدرت ملی که دارای فرمول ریاضی هستند توسط جرمن، فوکس و کلاین ارائه‌شده است. در ادامه هرکدام از مدل‌های مذکور به‌طور مجزا موردبررسی و نقد قرار می‌گیرد[۳۳].

الف)مدل کلیفورد جرمن

اولین مدل پیچیده چند متغیره غیرخطی را که تلاش کرده بود هم متغیرهای مجزا را در نظر بگیرد و هم ارتباط بین آن‌ها را تبیین نماید، در سال ۱۹۶۰ توسط کلیفورد جرمن مطرح شد. وی با استفاده از ۲۶ متغیر مختلف مدل قدرت جهانی را بر اساس فرمول زیر طرح کرد:

$$G = N(L + P + I + M)$$

نمایانگر زمینهI ، نشان‌دهنده جمعیتP ، نمایانگر سرزمینL ، بیانگر توانایی هسته‌ایN ، در این مدل نشان‌دهنده اندازه نیروی نظامی است. هرکدام از این متغیرها به چندین فاکتور M صنعتی و بالاخره جزئی‌تر تقسیم‌شده بود. مثلاً زمینه صنعتی به فاکتورهای تولید فولاد، زغال، زغال قهوه‌ای، نفت و هیدرو الکتریسیته تقسیم‌شده بود. سپس هرکدام از این متغیرها با توجه به معیارهای مرتبط با هر فاکتور امتیازدهی(نمره دهی)شده بود. سرانجام این اعداد مختلف یعنی وسعت به کیلومترمربع، جمعیت به نفر، سرباز به نفر و ضریب اتمی را با یکدیگر جمع نموده و عدد حاصله نماینده میزان قدرت کشور می‌گردید[۳۴].

نکات مثبت و منفی این مدل را می‌توان شامل موارد زیر دانست:

۱) مهم‌ترین ویژگی مثبت مدل، جامع بودن نسبی آن به دلیل تعداد متغیرهای بکار گرفته هست. به‌طوری‌که به‌عنوان‌مثال زمینه صنعتی خود از ترکیب متغیرهای تولید فولاد، زغال، نفت و هیدرو الکتریسیته به دست می‌آمد.

۲) پرهیز از متغیرهای کیفی و استفاده از متغیرهای کمیت‌پذیر یکی دیگر از نقاط قوت این مدل محسوب می‌شود.

۳) اگرچه این مدل به دلیل تعداد متغیرهای بکار رفته نسبتاً جامع محسوب می‌شود و چنانکه مریت و زینز اذعان کرده‌اند این مدل در بین تمام مدل‌های مطرح‌شده، پیچیده‌ترین آن‌ها محسوب می‌شود اما بازهم بسیاری از ابعاد قدرت مورد غفلت قرارگرفته است، مثلاً به متغیرهای فرهنگی، اجتماعی و اقتصادی کمتر توجه شده یا اصلاً لحاظ نشده‌اند.

۴) اشکالی که بر این مدل و تقریباً تمامی مدل‌های ارائه‌شده وارد است و البته طراحان مدل در آن چندان دخالتی نداشته‌اند، این است که چون این مدل‌ها در دهه‌های قبل طراحی‌شده‌اند، بنابراین منطبق بر متغیرهای جدیدی که در زمان کنونی معیار قدرت یک کشور محسوب می‌شود نیستند.

ب) مدل ویلهم فوکس

یک مدل غیرخطی چند متغیره ترکیبی، متعاقباً در سال ۱۹۶۵ به‌وسیله ویلهلم فوکس پیشنهاد شد. فوکس که خود یک فیزیکدان حرفه‌ای بود تلاش کرد قدرت ملی را از طریق سه متغیر خلاصه؛ یعنی اندازه جمعیت (P)، تولید انرژی(Z) و تولید فولاد (Z۱): که دریکی از نه فرمول اندازه‌گیری قدرت ملی قرارداد شده بود، استخراج کند.

تمام این متغیرها، شکلی از دیگری بودند و صورت زیر را به خود می‌گرفتند:

$$M = {}^{P۲}z_{۱}, = P^{۳\square}\ {}^{۲}Z\ and\ ets$$

علاوه بر مدل فوق، مدل دیگری را نیز برای سنجش قدرت ملی به فوکس نسبت داده‌اند که با ملل فوق کمی تفاوت دارد . این مللی عبارت است از:

$$Power = P۳\sqrt{B}$$

قدرت ملی = مکعب تولید ناخالص ملی ضرب‌در جذر جمعیت کشور

حرف P نماینده تولید ناخالص ملی وB نماینده جمعیت است. با استفاده از این فرمول و پس از ساختن نمودارهای لازم که میزان جمعیت و بازده اقتصادی را در آینده نشان می‌داد، فوکس پیش‌بینی کرده بود که در سال ۱۹۷۰ قدرت چین از قدرت شوروی بیشتر خواهد شد و اینکه در سال ۱۹۷۵ چین باقدرت‌ترین کشور دنیا خواهد گردید.

نکته لازم به ذکر این است که اگرچه این مدل به دو شکل تقریباً متفاوت به فوکس نسبت داده‌شده است اما منبع مورداستفاده برای هر دو یک کتاب مشابه است. به نظر می‌رسد مناسب‌ترین نقدی که بتوان بر این مدل و سایر مدل‌های مشابه وارد نمود، همان نکته و انتقادی است که توسط ریچارد موبر جغرافیدان سیاسی ذکرشده است. موبر معتقد است: قدرت یک کشور جامع‌تر از آن است که فقط با بررسی رابطه بین دو متغیر تولید ناخالص ملی و جمعیت بتوان به آن دست‌یافت:

ج) مدل ری کلاین

یکی دیگر از مدل‌های قدرت ملی در سال ۱۹۷۵ توسط ری کلاین مطرح شد و خیلی زود موردتوجه خاص محافل دانشگاهی و جامعه دفاعی قرار گرفت .فرمول کلاین عبارت بود از:

$$P_p = (C + E + M)\ (S + W)$$

متغیرهای این فرمول عبارت‌اند از:

C= هسته اصلی شامل جمعیت، سرزمین؛

E= ظرفیت اقتصادی شامل درآمد به‌اضافه انرژی به‌اضافه معادن غیر فسیلی به‌اضافه کالاهای ساخته‌شده به‌اضافه غذا به‌اضافه تجارت؛

M= ظرفیت نظامی شامل موازنه استراتژیک به‌اضافه قابلیت‌های جنگی به‌اضافه پاداش بابت تلاش؛

S = ضریب استراتژی ملی؛

W = ویژگی‌های سطح ملی شامل سطح یکپارچگی ملی، توانایی رهبری، ارتباط استراتژی با منافع ملی

نکات مثبت و منفی این فرمول را می‌توان شامل موارد زیر دانست:

۱) استفاده از متغیرهای متعدد و مهم‌تر از آن انتخاب متغیرهایی از حوزه‌های مختلف طبیعی، اقتصادی، سیاسی، نظامی و اجتماعی مهم‌ترین نقاط قوت این مدل نسبت به بیشتر مدل‌های ارائه‌شده است.

۲) وجود متغیرهای کیفی مانند سطح یکپارچگی ملی، توانایی رهبری، موازنه استراتژیک و ...در مدل بدون اینکه برای کمی کردن آن‌ها راه‌حلی پیشنهادشده باشد بزرگ‌ترین نقطه‌ضعف مدل محسوب می‌شود.

۳) مانند بیشتر مدل‌ها این مدل نیز فقط بر متغیرهای مثبت تأکید کرده و متغیرهای دارای بار منفی را نادیده گرفته است که این ازجمله نقاط ضعف مد محسوب می‌شود؛ زیرا اصولاً قدرت ملی حاصل ترکیب و جمع جبری وجوه مثبت و منفی ناصر و بنیان‌های قدرت یک کشور هست.

۵. ارزیابی و تحلیل قدرت سایبری چین و اتحادیه اروپا

در این بخش به بررسی ارزیابی قدرت سایبری کشور چین و اتحادیه اروپا می پردازیم.

۵-۱ قدرت چین در فضای سایبری

چین متوجه شده است که امنیت سایبری، حمله‌های هکری و جنایت‌های سایبری به مشکل عمومی در جهان تبدیل‌شده است؛ بنابراین تنها همکاری بین‌المللی است که آن‌ها را قادر می‌سازد که از جنایت‌های سایبری جلوگیری و از رشد سالم فضای سایبری و اینترنت مطمئن شوند. چین اعتقاد دارد که کشورها در این زمینه می‌بایست با سایرین همکاری نمایند. همه ملت همه باید نظراتشان را اعلام کنند، اما همه آنان باید مسئولیت‌هایشان را نیز بدانند. آن‌ها اعتقاددارند از طریق ارتباطات و مبادلات صادقانه، جامعه بین‌المللی قادر خواهد بود با شیوه‌های مؤثر برای برخورد با تهدیدات سایبری همراه شود. چین همیشه از استفاده امن و صلح‌آمیز از فضای جهانی اطلاعات حمایت کرده است، با این پیش‌فرض که حاکمیت ملی و امنیت حوزه اطلاعاتش نیز حفظ گردد.

الگوهای مدل چین در اقدامات امنیتی -سایبری پیرامون سه محور تدافع، تهاجم و کنترل ابزارهای جبهه متقابل موردبررسی قرارگرفته است. در این پیوند تلاش متخصصان چینی درزمینهٔ کاهش زمان کشف اطلاعات و به‌کارگیری آن در رویارویی‌های امنیتی و حتی رقابت‌های تجاری و اقتصادی از سوی ناظران به‌عنوان عاملی برای تشدید نگرانی‌های واشنگتن در افزایش تهدیدات سایبری تلقی شده است؛ اما این احتمال وجود دارد که کشور چین با بهره‌برداری از آسیب‌پذیری‌های غرب در حوزه سایبری هم به جمع‌آوری علوم ارزشمند با کمترین ریسک بپردازد و هم ضعف‌های حوزه نظامی و سیستم‌های زیربنایی مهم را شناسایی کند. البته این‌یک جاده یک‌طرفه نیست. پکن هم نگران آسیب‌پذیری کشور خود در حوزه اینترنت است. نظریه دفاع سایبری نیروهای مسلح چین مبنی بر ارتباط مستقیم موفقیت دفاعی_امنیتی با مؤلفه میزان کنترل و دسترسی به اطلاعات، ادعاشده است که ارتش چین بر مقابله اطلاعاتی و سایبری در فضای اینترنت تمرکز ویژه‌ای داشته و درمجموع چینی‌ها توانسته‌اند درزمینهٔ تولید سخت‌افزارهای رایانه‌ای و تجهیزات مخابراتی به پیشرفت‌های خیره‌کننده‌ای دست یابند. جمهوری خلق چین همراه با رشد و گسترش پرشتاب اقتصادی و نظامی‌اش، برای بهبود جایگاه خود از سطح یک قدرت منطقه‌ای اثرگذار در شرق آسیا بده یک قدرت جهانی از یک دهه پیش به‌گونه‌ای جدی بهره‌گیری از اهرم‌های قدرت نرم و استفاده از فضای سایبر را در رویکردهای دفاعی_ تهاجمی در دستور کار خود قرار داده است.

فعالیت‌های چین در فضای سایبری نه‌تنها بر جمع‌آوری اطلاعات حساس متمرکز است، بلکه توسعه توانمندی‌های ارتش آزادی‌بخش خلق نیز از دیگر اهداف این دولت است. ایجاد خسارت‌های اقتصادی، تخریب زیرساخت‌های حمایتی و تأثیرگذاری بر نتیجه منازعات مسلحانه متعارف از مهم‌ترین اهداف این دولت در فضای سایبری محسوب می‌شود.

۲-۵ اتحادیه اروپا

برابر افق ۲۰۲۰ اتحادیه اروپا ابزارها و ادوات مبارزه با فعالیت‌های تروریستی که فضای سایبر را هدف گرفته‌اند توسعه داده خواهد شد، همچنین مکانیسم‌هایی برای هماهنگی، برنامه‌ریزی و تحقیق مؤسسات اتحادیه اروپا و دولت‌های عضو و ارائه مشوق‌هایی به اعضاء برای سرمایه‌گذاری بیشتر در R&D وضع خواهد گردید. در این افق بخش‌هایی از امنیت و محرمانگی ICTموردنظر قرار داده‌شده است که این بخش‌ها شامل تحقیق و توسعه تا پیاده‌سازی می‌باشد.

پنج اولویت راهبردی اتحادیه عبارت‌اند از:

- دست‌یابی به انعطاف‌پذیری سایبری
- کاهش اساسی جرم سایبری
- توسعه سیاست‌های دفاع سایبری در حوزه‌های امنیت عمومی و سیاست دفاعی
- توسعه منابع صنعتی و فن آمرانه برای امنیت سایبر
- برقراری سیاست فضای سایبری هماهنگ با بین‌الملل برای اتحادیه و ترویج ارزش‌های اساسی اتحادیه

اهم سیاست‌ها و مأموریت‌های اتحادیه اروپا به شرح زیر است:

- اجرای پروژه آزمایشی با پشتیبانی اتحادیه اروپا برای مقابله با بال نت و بدافزارها و شناخت آسیب‌پذیری‌ها باهدف فراهم کردن زیرساخت همکاری و هماهنگی بین اعضای دولتی اتحادیه و بخش خصوصی
- هم کاری قضایی برای شناخت جرائم سایبری و هم کاری بین اعضاء
- ارتقاء فرصت‌هایی برای تمرین و آموزش دفاع سایبری در مفاهیم نظامی اروپا و بین‌الملل، شامل لحاظ نمودن برنامه دفاع سایبری در برنامه‌های آموزش نظامی موجود.
- حمایت اتحادیه در صورت وقوع حملات سایبری عمده
- ترویج امنیت در تمام سطوح
- توسعه منابع فنی و صنعتی برای امنیت سایبری
- افزایش سرمایه‌گذاری و نوآوری در تحقیق و توسعه
- ترویج تعامل و هماهنگی بین بازیگران بخش نظامی و غیرنظامی در اتحادیه با تأکید بر تبادل بهترین تجارب، تبادل اطلاعات و پیش‌آگاهی، پاس به تهدیدها، ارزیابی تهدید، بالا بردن آگاهی و قائل شدن امنیت سایبری به‌عنوان یک اولویت
- توسعه سیاست‌های دفاع سایبری و قابلیت‌های مرتبط با ساختار سیاست دفاعی و امنیت عمومی
- تمرکز بر فعالیت‌های توسعه قابلیت‌های دفاع و فنّاوری دفاع سایبری
- تعامل با بازی گران بین‌المللی شامل ناتو و دیگر سازمان‌های بین‌المللی و مراکز عالی چندملیتی به‌منظور تضمین قابلیت‌های دفاع مؤثر و پرهیز از کارهای تکراری.
- حمایت از توسعه رمزنگاری

۶. جمع بندی و نتجه گیری

در این مقاله، به بررسی مفهوم قدرت سایبری شامل تعریف قدرت سایبری، ارکان قدرت سایبری، لایه های قدرت سایبری و عوامل اثرگذار بر روی قدرت سایبری پرداختیم. هم چنین مروری بر مهم ترین پژوهش های انجام شده در حوزه قدرت سایبری داشته ایم. با توجه به اینکه اندازه گیری میزان قدرت سایبری کشورها برای طراحی راهبردها و نقشه راه کشورها

بوده و می تواند عامل اثرگذاری برای تصمیمات راهبردی کشورها باشد، رویکردهای اساسی ارزیابی قدرت سایبری کشورها را مورد مطالعه قرار دادیم. در نهایت کشورچین و اتحادیه اروپا را به عنوان دو نمونه مورد ارزیابی و تحلیل قرار می دهیم.

۷. مراجع

[۱] ر.ا.ب.و.خ.ه.و.ع. ولوی, جنگ سرد نوین و رقابت بین قدرت های جهانی در فضای سایبری, ششمین کنفرانس سراسری دانش و فناوری علوم تربیتی مطالعات اجتماعی و روانشناسی ایران, (۱۳۹۹).

[۲] ر.ا. بشارت, و.م.ذ. امیری, تأثیر قدرت سایبری بر منطقه گرایی اعضای شورای همکاری خلیج فارس, (۱۳۹۹).

[۳] ب.ر. و, ش.ع.ی. و, م.م. شهربابک, معرفی الگویی برای اندازهگیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران, فصلنامه علمی راهبرد دفاعی، سال هجدهم، شماره۶۹, (۱۳۹۹).

[۴] م.ر. و, م.غ.ث. و, ع.م.ا. و, م.آ. و, ا.ن. فرخی, ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید برُبعد بازدارندگی سایبری, قصلنامه مدیریت نظامی، سال بیستم، شماره ۲, (۱۳۹۹).

[۵] ح. آریان, شناسایی عوامل قدرت هوشمند در فضای سایبری، پایان نامه کارشناسی ارشد، دانشگاه پیام نور استان تهران، مرکز پیام نور تهران غرب, (۱۳۹۷).

[۶] ا.ز.ز.و.پ.و. پور, قدرت بازدارندگی در فضای سایبر، دو فصلنامه علمی-پژوهشی رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی ۴۷-۷۴., (۱۳۹۷).

[۷] خ.ه.و.ع. ولوی, ارائه الگوی راهبردی ارتقای قدرت سایبری جمهوری اسلامی ایران در تراز جهانی، دانشگاه عالی دفاع ملی., (۱۳۹۷).

[۸] خ.ه. و, م.و. و, م.م. صفت, شناسایی عوامل و مؤلفه های اثرگذار بر تدوین رهنامه قدرت سایبزی ج.ا.ایزان مبتنی بر سیاست های ابلاغی و اسناد بالادستی, فصلنامه راهبرد دفاعی، سال شانزدهم، شماره۶۳ (۱۳۹۷).

[۹] ع.ا. دهقانی, بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه وچین علیه زیرساختهای حیاتی آمریکا،فصلنامه رهیافتهای سیاسی و بینالمللی، سال هشتم،شماره ۴، پیاپی ۵۰., (۱۳۹۷).

[۱۰] م.م.ق.خ.و.د. حسینی, حاکمیت شبکهای در نهادهای پژوهشی امنیت. سایبری، فصلنامه فرآیند مدیریت و توسعه، دوره ۳۰ ، شماره ۱, (۱۳۹۶).

[۱۱] ح. شهبا, بررسی نقش قدرت سایبری در هندسه قدرت جمهوری اسلامی ایران، پایان نامه کارشناسی ارشد، دانشگاه شهید باهنر کرمان., (۱۳۹۶).

[۱۲] طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن، پژوهشفران مدیریت راهبردی امنیت فضای سایبری، دانشکده امنیت ملی، مطالعه گروهی دانشگاه عالی دفاع ملی, (۱۳۹۵).

[۱۳] م.آ. جاوید, تاثیر قدرت سایبری ایالات متحده آمریکا بر سیاست خارجی این کشور(۲۰۰۱-۲۰۱۵) پایان نامه کارشناسی ارشد، دانشگاه خوارزمی, (۱۳۹۴).

[۱۴] ع. درویش, ارتش سایبری و پیشبینی بعد از حمله سایبری، نخستین کنفرانس بین المللی فناوری اطلاعات, (۱۳۹۴).

[۱۵]Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, A. Schwarzenbach, National Cyber Power Index ۲۰۲۰.

[۱۶]C.G.U.O. Yuqi H A N, Shiying M A, et al., Modeling cascading failures and itigation strategies in PMU based cyberphysical power systems, Journal of Modern Power Systems and Clean Energy, pp. ۹۵۷-۹۴۴., **۲۰۱۸**.

[۱۷]X.L. Su Z, Xin S, et al, A future outlook for cyber-physical power system," Energy Internet and Energy System Integration (EI**۲**), IEEE Conference on. IEEE, pp. ۴-۱., **۲۰۱۷**.

[۱۸]K.D.K.K.D.P.R.K.P. R., Cyber-physical systems a perspective at the centennial,Proceedings of the IEEE, pp. ۱۳۸۰-۱۲۸۷**, ۲۰۱۲.**

[۱۹]V.V.T. Ansari M H, Bahrak B, et al **,**.Graph theoretical defense mechanisms against false data injection attacks in smart grids, Journal of Modern Power Systems and Clean Energy, pp. -۸۶۰ ۸۷۱, **۲۰۱۸**.

[۲۰]Y.W. Xinyi Liang, Ming Ni, Manli Li, Survivability Index and Evaluation Framework for Cyber Physical Power Systems, **۲۰۲۰**.

[۲۱]X. Tong Gong Cheng, Dian, Yu, Shu, Zi, Ji, Maturity Model of Cyber Ecosystem, Systems Engineering and Electronics ۶۱**(**۱۱**)**. **۲۰۱۸**.

[۲۲]W.L. Shawn, Cyber Power and the International System, Columbia University, Doctoral Dissertation., **۲۰۱۷**.

[۲۳]R. Bebber, Cyber Power and Cyber Effectiveness: An Analytic Framework, Comparative Strategy ۶۳**(**۵**):**۶۲۳., **۲۰۱۷**.

[۲۴]S. Monterey, Offense-defense theory analysis of Russian cyber capability California: Naval Postgraduate School., **۲۰۱۵**.

[۲۵]J. Rowland, Rice, Mason and Shenoi, Sujeet, The Anatomy of Cyber Power, International Journal of Critical Infrastructure Protection.,**۲۰۱۴**

[۲۶]D.T. Kuehl, From Cyberspace to Cyber power: Defining the problem.,**۲۰۰۹**.

[۲۷] ج. روشندل, امنیت ملی و نظام بین الملل. تهران: انتشارات سمت . (۱۳۹۲).

[۲۸] س.ه. زرقانی, تحلیل و ارزیابی متغیرها و شاخص‌های قدرت نظامی. فصلنامه راهبرد دفاعی، سال ششم.. (۱۳۸۷).

[۲۹] ب.ر.ق.ت.ن.د.ب.ت.ا. خوارزمی, قدرت، ترجمه نجف دریا بندری،انتشارات خوارزمی, (۱۳۶۷).

[۳۰]R. Dohl, The concept of power, Bebariora Lscience, n**۲,۱۹۵۷**.

[۳۱] ح. بهزادی, اصول روابط بین الملل، انتشارات دهخدا, (۱۳۵۲).

[۳۲]Morgenthou. Y, politicamong Nations, New york: Alfred A. Knopf, **۱۹۶۷**

[۳۳] پ.خ.و.ا. محمدی, نقش پدافند هوایی در استحکام قدرت ملی نظام جمهوری اسلامی ایـران, علـوم سیاسـی :: نشـریه مطالعات دفاعی استراتژیک :: ص ۶۳ تا ۸۶, (۱۳۹۷).

[۳۴] و. جونز, " منطق روابط بین الملل"، ترمم داوود حیدری، ، تهران، دفتر مطالعاات سیاسی بین المللی, (۱۳۷۳).

[۳۵] س.ح.س. زاده, " اصول و روابط بین الملل" تهران: نشر دادگستر, (۱۳۷۸).

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December: 25-26, 2024

Improving the PF_4 Algorithm through a Novel Selection Strategy

Mahdi Dehghani Darmian[1]
Department of Mathematics, National University of Skills (NUS), Tehran, Iran

Abstract

In this paper, we improve the PF_4 algorithm [3, 5], an efficient extension of Faugère's F_4 algorithm [7] for parametric polynomial ideals. Our enhancement involves installing a novel selection strategy on the PF_4 algorithm. The Improved-PF_4 algorithm takes a parametric polynomial ideal and two monomial orderings on the variables and parameters as input, returning a Gröbner system of the ideal w.r.t. a compatible elimination product of the specified orderings. We have implemented this enhanced algorithm in `Maple`, providing timing and memory usage data to compare its performance against our previous version of the PF_4 algorithm.

Keywords: Selection strategy, Gröbner systems, Improved-PF_4 algorithm, PGBMain algorithm, DisPGB algorithm.

Mathematics Subject Classification [2010]: 13P10, 13P25

1 Introduction

Gröbner bases, a specialized type of generating set for polynomial ideals, are powerful computational tools in computer algebra with significant applications in mathematics, science, and engineering. They were introduced by Buchberger in his Ph.D. thesis, along with the first algorithm for computing them, under the supervision of Gröbner [2]. Buchberger later enhanced his algorithm by introducing two criteria to eliminate redundant reductions [1]. However, due to its time-consuming nature, Lazard proposed a linear algebra-based method for computing Gröbner bases in 1983 [11]. In 1999 and 2002, Faugère presented the well-known F_4 [7] and F_5 [8] algorithms, respectively. The F_4 algorithm retains the mathematical concepts of Buchberger's method but computes multiple normal forms simultaneously by creating a sparse matrix and employing fast linear algebra for reductions.

This paper presents an improvement to the PF_4 algorithm [3, 5] through a new selection strategy for computing Gröbner systems—an extension of Gröbner bases—for parametric polynomial ideals. A Gröbner system consists of a finite set of triples (branches), where each branch contains parametric constraints (comprising null and non-null parametric sets) and a corresponding set of polynomials. For any specialization, there exists a branch such that the specialization satisfies its constraints, and the specialized polynomial set forms a Gröbner basis for the corresponding parametric ideal. Weispfenning introduced the concept of Gröbner systems [14], proved the existence of such systems for any given parametric polynomial ideal [14, Proposition 3.4 and Theorem 2.7], and developed the first algorithm for their computation [14, Theorem 3.6]. In 2002, Montes [12] proposed a more efficient algorithm (DisPGB) for computing Gröbner systems (see also [6, 9]). Subsequently, Suzuki and Sato introduced an effective enhancement for computing Gröbner systems in [13], utilizing recursive computations of reduced Gröbner bases within an extended polynomial ring.

In 2010, Kapur et al. designed an efficient algorithm (the PGBMain algorithm [10]) for computing Gröbner systems by combining Weispfenning's [15] and Suzuki-Sato algorithms. The PGBMain algorithm computes the Gröbner basis over a polynomial ring with respect to both the variables and parameters at each iteration. This step

[1] speaker

can be costly, as the complexity of Gröbner basis computations is significantly influenced by the number of variables and the degree of the polynomials involved. Thus, developing an efficient algorithm that reduces computations in a polynomial ring in terms of only the variables is essential. Conversely, the DisPGB algorithm operates solely within a polynomial ring in terms of the variables. Like Buchberger's algorithm, it computes parametric S-polynomials and adds the polynomial to the basis set if its remainder is non-zero (see also [9]). However, the DisPGB can produce numerous branches with undecidable coefficients, leading to inefficiencies.

To address this issue, we introduced a parametric version of the F_4 algorithm (so-called PF_4 algorithm) [3, 5], based on parametric linear algebra techniques and foundational ideas from the DisPGB structure [12]. We proposed a parametric F_4 algorithm for computing Gröbner systems for parametric polynomial ideals. In this paper, we enhance the PF_4 algorithm [3, 5] through a new selection strategy. Our new algorithm, termed the Improved-PF_4 algorithm, along with the original PF_4 algorithm, has been implemented in `Maple`, and their efficiencies are discussed across a range of parametric polynomial ideals.

Below, we briefly review the basic notations and definitions related to Gröbner bases and Gröbner systems.

Throughout this paper, we consider $\mathcal{R} = \mathbb{K}[x_1, \ldots, x_n]$, the polynomial ring in $x_1, \ldots, x_n$ over a field $\mathbb{K}$. Let $\mathcal{I} = \langle f_1, \ldots, f_k \rangle \subset \mathcal{R}$ be the ideal generated by the f_i. A monomial ordering $\prec$ is defined on the set of all monomials in $\mathcal{R}$. For any $f \in R$, the *leading monomial* $\mathrm{LM}_\prec(f)$ is the greatest monomial appearing in f, and its coefficient, the *leading coefficient* $\mathrm{LC}_\prec(f)$. The *leading term* is then $\mathrm{LT}_\prec(f) = \mathrm{LC}_\prec(f)\mathrm{LM}_\prec(f)$. The *leading monomial ideal* of $\mathcal{I}$ is $\mathrm{LM}_\prec(\mathcal{I}) = \langle \mathrm{LM}_\prec(f) \mid f \in \mathcal{I} \rangle$. A finite subset $\{g_1, \ldots, g_m\} \subset \mathcal{I}$ is a *Gröbner basis* for $\mathcal{I}$ with respect to $\prec$ if $\mathrm{LM}_\prec(\mathcal{I}) = \langle \mathrm{LM}_\prec(g_1), \ldots, \mathrm{LM}_\prec(g_m) \rangle$.

Now consider $\mathcal{S} = \mathbb{K}[\mathbf{a}, \mathbf{x}]$, where $\mathbb{K}$ is a field, $\mathbf{a} = a_1, \ldots, a_m$ are parameters, and $\mathbf{x} = x_1, \ldots, x_n$ are variables. Let $\prec_\mathbf{x}$ and $\prec_\mathbf{a}$ be monomial orders on the variables and parameters, respectively. The product ordering $\prec_{\mathbf{x},\mathbf{a}}$ is defined such that for $\alpha, \beta \in \mathbb{N}^n$ and $\gamma, \delta \in \mathbb{N}^m$, we have $\mathbf{x}^\alpha \mathbf{a}^\gamma \prec_{\mathbf{x},\mathbf{a}} \mathbf{x}^\beta \mathbf{a}^\delta$ if either $\mathbf{x}^\alpha \prec_\mathbf{x} \mathbf{x}^\beta$ or $\mathbf{x}^\alpha = \mathbf{x}^\beta$ and $\mathbf{a}^\gamma \prec_\mathbf{a} \mathbf{a}^\delta$.

Consider the specialization $\sigma : \mathbb{K}[\mathbf{a}] \to \overline{\mathbb{K}}$ where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$, allowing substitution of parameters in $f \in \mathbb{K}[\mathbf{a}]$ with elements from $\overline{\mathbb{K}}^m$. For a finite set $F \subset \mathcal{R}$, we denote the variety of F as $\mathbb{V}(F)$, the set of common zeros of F.

We define a Gröbner system for a parametric polynomial ideal as follows:

Definition 1.1. Let $F \subset \mathcal{S}$ and $\mathcal{G} = \{(G_i, N_i, W_i)\}_{i=1}^{\ell}$ be a finite set of triples, with $N_i, W_i \subset \mathbb{K}[\mathbf{a}]$ and $G_i \subset \mathcal{S}$. The set $\mathcal{G}$ is a *Gröbner system* of $\langle F \rangle$ with respect to $\prec_{\mathbf{x},\mathbf{a}}$ on $V \subseteq \overline{\mathbb{K}}^m$ if for each i:

- For any specialization σ satisfying (N_i, W_i), the set $\sigma(G_i) \subset \overline{\mathbb{K}}[\mathbf{x}]$ forms a Gröbner basis of $\langle \sigma(F) \rangle$ with respect to $\prec_\mathbf{x}$. (Here, σ satisfies (N_i, W_i) if $\sigma(p) = 0$ for all $p \in N_i$ and $\sigma(q) \neq 0$ for some $q \in W_i$.)
- $V \subseteq \bigcup_{i=1}^{\ell} \mathbb{V}(N_i) \setminus \mathbb{V}(W_i)$.

Each (N_i, W_i, G_i) is a branch of the Gröbner system $\mathcal{G}$, where N_i is the null condition set and W_i the non-null condition set. Furthermore, $\mathcal{G}$ is a Gröbner system of F if $V = \overline{\mathbb{K}}^m$.

Example 1.2. Let $F = \{(1-c)y - ax^2, x + by^2\} \subset \mathbb{K}[a, b, c, x, y]$, where a, b, c are parameters and x, y are variables. Using our implementation of the PF_4 algorithm in `Maple`, we obtain the following CGS for $\langle F \rangle$ with respect to the product ordering $y \prec_{lex} x$ and $c \prec_{lex} b \prec_{lex} a$:

$$\begin{cases} ([\,], & [ab^2], & [ab^2y^4 - y + cy, x + by^2]) \\ ([ab^2], & [c-1], & [cy - y, x + by^2]) \\ ([c-1, ab^2], & [\,], & [x + by^2]). \end{cases}$$

For example, if $a = 2$, $b = 1$, and $c = 3$, the first branch corresponds to these parameter values. Thus, $\{2y^4 - y + 3y, x + y^2\}$ forms a Gröbner basis for the ideal $\langle F \rangle_{|a=2,b=1,c=3} = \langle -2y - 2x^2, x + y^2 \rangle$.

2 PF_4 Algorithm

The PF_4 algorithm [3, 5] outperforms the DisPGB algorithm by utilizing row-reduction techniques on a *sparse matrix* to simultaneously reduce multiple S-polynomials. In this section, we review the PF_4 algorithm, which generalizes the F_4 algorithm for polynomial ideals with parametric coefficients. During each iteration of the F_4 algorithm, both

linear and non-linear reductions are performed, complicating the management of parametric variations. To address this, we employed a modified version of the GES algorithm [4], which computes a Gaussian elimination system for a parametric matrix, equivalent to a parametric linear system of the input matrix. We adapted this algorithm for non-linear polynomials to achieve linear inter-reduction, seeking their Gaussian forms under parametric constraints. Specifically, we linearized the input polynomials by substituting each monomial with new variables. The core of the GES algorithm is the LDS algorithm [4], which evaluates the dependency of a linear parametric polynomial relative to a set of parametric polynomials without relying on Gröbner systems. The input to the LDS algorithm consists of (N, W, F, f), where (N, W) denotes a pair of condition sets, F is a collection of linear parametric polynomials forming a parametric Gröbner basis under the specified constraints, and f is a linear parametric polynomial. The LDS algorithm outputs a finite set of triples of the form $(N_i, W_i, [flag, Q, g])$, where (N_i, W_i) is a pair of condition sets, the flag is a Boolean variable, Q indicates the quotients of the division, and g is the normal form of f w.r.t. F. If the flag is true, then $g = 0$, indicating that f is linearly dependent on F with respect to (N_i, W_i). Conversely, if the flag is false, f is linearly independent modulo F under the same conditions.

Algorithm 1 LDS (Linear Dependency System)

Require: $G \subset \mathcal{S}$; a linear set which is a reduced Gröbner basis w.r.t. the product of the monomial orderings $\prec_{\mathbf{x}}$ and $\prec_{\mathbf{a}}$ provided that a conditions pair (N, W) is satisfied and $g \in \mathcal{S}$; a parametric linear polynomial
Ensure: A linear dependency system of g on (N, W, G)
  Sys:= {}
  f, Q :=NormalForm(g,GröbnerBasis($N, \prec_{\mathbf{a}}$), $\prec_{\mathbf{a}}$)
  f', Q' :=NormalForm($f, G, \prec_{\mathbf{x}}$)
  if $f' = 0$ **then**
    Sys:=Sys $\bigcup\{(N, W, [true, Q', 0])\}$
  else
    $A := \{a_{i_1}, \ldots, a_{i_t}\}$ where $f' = a_{i_1}x_{i_1} + \cdots + a_{i_t}x_{i_t}$ with $a_{i_j} \neq 0$ and $x_{i_1} \succ_{\mathbf{x}} \cdots \succ_{\mathbf{x}} x_{i_t}$
    for j **from** 1 **to** t **do**
      if a_{i_j} is not constant **then**
        Sys:=Sys $\bigcup\{(N \cup \{a_{i_1}, \ldots, a_{i_{j-1}}\}, W \cup \{a_{i_j}\}, [false, Q', f'|_{a_{i_1}=0,\ldots,a_{i_{j-1}}=0}])\}$
      else
        Sys:=Sys $\bigcup\{(N \cup \{a_{i_1}, \ldots, a_{i_{j-1}}\}, W, [false, Q', f'|_{a_{i_1}=0,\ldots,a_{i_{j-1}}=0}])\}$
        Return(Sys)
      end if
    end for
    Sys:=Sys $\bigcup\{(N \bigcup A, W, [true, Q', 0])\}$
  end if
  Return(Sys)

Example 2.1. Consider $(N, W) = ([m, n], [a - 1, a - b, 1 - b])$ as a specification, $G = [u + v, (a - 1)y - cz, (a - b)x - acz - bv, (b - 1)yx - czx + (bv + cz)y + c^2z^2]$ a linear Gröbner basis provided the conditions pair (N, W), and $g = av - bw + mz + nx - u - cy$, a parametric polynomial. We fix the monomial orderings $n \prec_{lex} m \prec_{lex} c \prec_{lex} b \prec_{lex} a$ and $w \prec_{lex} v \prec_{lex} u \prec_{lex} z \prec_{lex} y \prec_{lex} x$ on the parameters and the variables, respectively. So a linear dependency system of g on G acording to (N, W) using our `Maple` implementation of the LDS algorithm is as follow:

$$\text{Sys} = \begin{cases} ([m, n], [c, a - 1, a - b, 1 - b], & [false, [-1, \frac{c}{1-a}, 0, 0], \frac{c^2z}{1-a} + (a + 1)v - bw]), \\ ([m, n, c], [a - 1, a + 1, a - b, 1 - b], & [false, [-1, \frac{c}{1-a}, 0, 0], \frac{c^2z}{1-a} + (a + 1)v - bw]), \\ ([m, n, c, a + 1], [b, b + 1, 1 - b], & [false, [-1, \frac{c}{1-a}, 0, 0], \frac{c^2z}{1-a} - bw]), \\ ([m, n, c, a + 1, b], [\,], & [true, [-1, \frac{c}{1-a}, 0, 0], 0]). \end{cases}$$

Definition 2.2. Let A be a parametric matrix over $\mathbb{K}[\mathbf{a}] = \mathbb{K}[a_1, \ldots, a_m]$. A finite set of triples $\{(N_i, W_i, M_i)\}_{i=1}^{\ell}$ is called a *Gaussian elimination system* of A if for each specialization $\sigma : \mathbb{K}[a] \to \bar{\mathbb{K}}$, there is an i such that the following conditions hold

- The matrix $\sigma(M_i)$ is a Gaussian elimination form of $\sigma(A)$,
- $\sigma(p) = 0$ for each $p \in N_i$ and $\sigma(q) \neq 0$ for each $q \in W_i$.
- $\bigcup_{i=1}^{\ell} \mathbb{V}(N_i) \setminus \mathbb{V}(\prod_{w \in W_i} w) = \overline{\mathbb{K}}^m$

Using the LDS algorithm, we developed an efficient method for computing a Gaussian elimination system for a parametric matrix or a set of parametric polynomials; namely the GES algorithm [4]. In this algorithm, the global

variable Sys is initialized as an empty set, which ultimately serves as the output Gaussian elimination system. Specifically, each segment stored in Sys is a triple (N, W, G), where (N, W) represents a pair of condition sets, and G is the Gaussian elimination form of the input set of parametric polynomials according to (N, W).

Algorithm 2 GES (Gaussian Elimination System)

Require: $N \subset \mathbb{K}[\mathbf{a}]$; null condition set, $W \subset \mathbb{K}[\mathbf{a}]$; non-null condition set, $F \subset \mathbb{K}[\mathbf{a}, \mathbf{x}]$; a parametric polynomial set
Ensure: A Gaussian elimination system of F according to N and W

```
Sys:= {}
M := Mon(F) = [m_1, ..., m_t] (the set of all monomials in terms of the x_i's appearing in F)
[Y_1, ..., Y_t] :=A list of tag variables corresponding to Mon(F)
L := φ(F) where φ is a linear map sending each m_i into Y_i
A := {(N, W, {}, L[1], L)}
while A ≠ {} do
    a := A[1] and A := A \ {a}
    if a[5] = {} then
        G := φ^{-1}(a[3])
        Sys:=Sys ⋃{(a[1], a[2], G)}
    else
        G := a[5] \ {a[4]}
        g := G[1]
        P :=LDS(a[1], a[2], a[3], a[4])
        for i from 1 to |P| do
            Let P[i] = (N_1, W_1, [flag, Q, f])
            if flag = true then
                A := A ∪ {(N_1, W_1, a[3], g, G)}
            else
                A := A ∪ {(N_1, W_1, a[3] ∪ {f}, g, G)}
            end if
        end for
    end if
end while
Return (Sys)
```

In the following, we compute the Gaussian elimination system for a parametric matrix utilizing our `Maple` implementation of the efficient GES algorithm [4, Algorithm 3].

Example 2.3. Let us consider the following parametric matrix A where a, b, c are parameters.

$$A = \begin{bmatrix} a & 1 & -1 \\ -1 & b & 1 \\ 1 & -1 & c \end{bmatrix}$$

We get the following Gaussian elimination system of A using our `Maple` implementation of the above GES algorithm.

$$\begin{cases} [\,], & [a+1, c+b+a+abc], & \begin{bmatrix} 1 & -1 & c \\ 0 & a+1 & -1-ac \\ 0 & 0 & a+b+c+abc \end{bmatrix} \\ [a+1], & [b-1, c-1], & \begin{bmatrix} 1 & -1 & 1 \\ 0 & b-1 & 2 \\ 0 & 0 & c-1 \end{bmatrix} \\ [c-1, a+1], & [b-1], & \begin{bmatrix} 1 & -1 & 1 \\ 0 & b-1 & 2 \\ 0 & 0 & 0 \end{bmatrix} \\ [b-1, a+1], & [\,], & \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \\ [c+b+a+abc], & [a+1], & \begin{bmatrix} 1 & -1 & c \\ 0 & a+1 & -1-ac \\ 0 & 0 & 0 \end{bmatrix}. \end{cases}$$

We now recall the PF_4 algorithm [3, 5] for computing Gröbner systems of parametric polynomial ideals. This algorithm takes a parametric polynomial set F and two monomial orderings on variables and parameters, returning

a Gröbner system for the ideal generated by F. The global variable OUTSYS is initialized as an empty sequence, to which new branches are added during each iteration of the PF_4 and PF_4Basis algorithms; the engine of the PF_4 algorithm. Ultimately, OUTSYS will represent a Gröbner system of the input ideal.

Algorithm 3 PF_4

Require: $F \subset \mathbb{K}[\mathbf{a}, \mathbf{x}] = \mathbb{K}[a_1, \ldots, a_m, x_1, \ldots, x_n]$, $\prec_{\mathbf{x}}, \prec_{\mathbf{a}}$; two monomial orderings
Ensure: G; A Gröbner system of $\langle F \rangle$ with respect to $\prec_{\mathbf{x},\mathbf{a}}$
  $OUTSYS := NULL$
  A :=GES([ ], [ ], F)
  for $(N_n, W_n, F_n) \in A$ **do**
    if F_n = [ ] **then**
      OUTSYS:= OUTSYS, $(N_n, W_n, [\,])$
    end if
    if there is any constant or non-zero parameter in F_n **then**
      OUTSYS:= OUTSYS, $(N_n, W_n, [1])$
    else
      $t := |F_n|$ (the cardinality of F_n)
      B := [[{i, j}, deg(lcm(LM$_{\prec_{\mathbf{x}}}$(F$_n$[i]), LM$_{\prec_{\mathbf{x}}}$(F$_n$[j])))] | 1 ≤ i < j ≤ t, gcd(LM$_{\prec_{\mathbf{x}}}$(F$_n$[i]), LM$_{\prec_{\mathbf{x}}}$(F$_n$[j])) ≠ 1]
      if B = [ ] **then**
        OUTSYS:= OUTSYS, (N_n, W_n, F_n)
      else
        $SYS := [[N_n, W_n, F_n, t, B]]$
      end if
    end if
    PF$_4$Basis(SYS)
  end for

In the PF_4Basis algorithm, the Newpolys procedure takes two polynomial lists, F and G, returning those polynomials $f \in F$ where LM(f) $\notin \langle$LM(G)$\rangle$.

Algorithm 4 PF_4Basis

Require: $N \subset \mathbb{K}[\mathbf{a}]$; null condition set, $W \subset \mathbb{K}[\mathbf{a}]$; non-null condition set, $F \subset \mathbb{K}[\mathbf{a}, \mathbf{x}]$; t; the cardinality of F and $Cpairs$; a list of pairs so that the first component is a pair of integers $\{i, j\}$ and second component is deg(lcm$_{\prec_{\mathbf{x}}}$(LM(F[i]), LM$_{\prec_{\mathbf{x}}}$(F[j])))
Ensure: Decomposing the space of parameters into a finite set of parametric cells and for each cell associating a finite set of parametric polynomials
  $B := Cpairs$
  while $SYS \neq$ [ ] **do**
    $sys := SYS[1]$ and remove it from SYS
    $G := sys[3]$
    B := $sys[5]$
    Select $Bp \subseteq B$ using degree-normal selection strategy
    $B := B \setminus Bp$
    $Bsys := B$
    $L := \{\frac{\text{lcm(LM(f}_i\text{),LM(f}_j\text{))}}{\text{LM(f}_i\text{)}}.f_i,\ \frac{\text{lcm(LM(f}_i\text{),LM(f}_j\text{))}}{\text{LM(f}_j\text{)}}.f_j \mid \{i, j\} \in Bp\}$
    H :=ComputeM(L, G)
    Ges :=GES(sys[1], sys[2], H)
    $allNPi$:= [Newpolys($Ges[i][3], H$), $i = 1, \ldots, \left| Ges \right|$]
    for j **from** 1 **to** $\left| allNPi \right|$ **do**
      $t := sys[4]$
      G := NormalSet($sys[3], Ges[j][1], \prec_{\mathbf{a}}$);
      $B := Bsys$
      for ℓ **from** 1 **to** $\left| allNPi[j] \right|$ **do**
        $t := t + 1$
        B :=Update($allNPi[j][\ell], G, B$)
        $G := [op(G), allNPi[j][\ell]]$
        if B = [ ] **then**
          OUTSYS:= OUTSYS, $(Ges[j][1], Ges[j][2], G)$
        else
          $SYS := [op(SYS), [Ges[j][1], Ges[j][2], G, t, B]]$
        end if
      end for
    end for
    $\{\text{PF4Basis}(SYS[m])\}_{m=1}^{|SYS|}$
  end while
  Return (OUTSYS)

Example 2.4. Let $F = [(c^2 - 1)x^2 + b^2 - 1, (a^2 - 1)xy^2 + c + b] \subset \mathbb{K}[a, b, c][x, y]$ where x, y are varibles and a, b, c are parameters. We consider the monomial orderings $y \prec_{lex} x$ and $c \prec_{lex} b \prec_{lex} a$. Using our implementation of

the PF4 algorithm in Maple, we obtain the following Gröbner system of $\langle F\rangle$ w.r.t. the product ordering $y \prec_{lex} x$ and $c \prec_{lex} b \prec_{lex} a$ saved in OUTSYS as follows:

$$\begin{cases}
([a^2-1],[b+c,c-1,c+1], & [1]),\\
([c^2-1],[a-1,a+1,b-1,b+1], & [1]),\\
([c^2-1,a^2-1],[b-1,b+1], & [1]),\\
([c^2-1,b^2-1,a^2-1],[b+c], & [1]),\\
([c^2-1,b+c,a^2-1],[\,], & [\,]),\\
([b^2-1],[a-1,a+1,b+c,c-1,c+1,2bc+c^2+1], & [c^2x^2-x^2,a^2xy^2-xy^2+b+c,bc^2x+c^3x-bx-cx,2bc^3+c^4-2bc-1]),\\
([b+c,a^2-1],[c-1,c+1], & [c^2x^2+c^2-x^2-1]),\\
([c^2-1,b^2-1],[a-1,a+1], & [a^2xy^2-xy^2+b+c]),\\
([b+c],[a-1,a+1,c-1,c+1], & [c^2x^2+c^2-x^2-1,a^2xy^2-xy^2,a^2c^2y^2-a^2y^2-c^2y^2+y^2]),\\
([\,],[a-1,a+1,b-1,b+1,b+c,c-1,c+1], & [c^2x^2+b^2-x^2-1,a^2xy^2-xy^2+b+c,a^2b^2y^2-a^2y^2-b^2y^2-\\
 & bc^2x-c^3x+bx+cx+y^2,y^4a^4b^2-y^4a^4-2a^2b^2y^4+2a^2y^4+\\
 & b^2c^2+(y^4-1)b^2+2bc^3-2bc+c^4-c^2-y^4]).
\end{cases}$$

3 Improvement of PF_4 Algorithm

This section introduces a novel selection strategy for efficiently choosing the next polynomial f_i to process. Effective selection is crucial because poor choices can unnecessarily increase the number of branches in the generating set before computing a Gröbner system. Our strategy combines several straightforward heuristics, which serve as benchmarks:

Diversity: Among the generators of the input ideal, select the polynomial with the fewest distinct parameters in its coefficients.

Degree: Among the input polynomials, choose the one with the lowest total degree concerning the parametric coefficients, which means selecting the polynomial with the lowest powers of the parameters.

Position: From the input polynomials, pick the one where the first parametric coefficient appears later.

Using these criteria, we can present an algorithm to sort polynomials in the input ideal or their related matrix coefficient rows. This algorithm takes as input two parametric polynomials from the input ideal F (or two rows of the matrix of coefficients of F) and compares them based on the specified criteria.

Algorithm 5 Comparison

Require: $f_1, f_2 \in F \subset S = \mathbb{K}[\mathbf{a},\mathbf{x}] = \mathbb{K}[a_1,\ldots,a_m,x_1,\ldots,x_n]$
Ensure: Returns either true or false
  C_1 := number of parameters appeared in f_1
  C_2 := number of parameters appeared in f_2
  D_1 := max degree of parametric coefficients in f_1
  D_2 := max degree of parametric coefficients in f_2
  P_1 := position of first parameter in f_1
  P_2 := position of first parameter in f_2
  if $C_2 < C_1$ **then**
    false
  else if $D_2 < D_1$ **then**
    false
  else if $P_2 > P_1$ **then**
    false
  else
    true
  end if

We can sort a list of parametric polynomials F using the logical function Comparison. By calling `sort(F,Comparison)`, we obtain a sorted list of polynomials based on the Comparison commands.

Example 3.1. Let us consider $F = [(a-1)x_1 + x_2 + (a+1)x_3 + (c^2-1)x_4, 2x_1 + 2x_2 - bx_3 + (c+1)x_4, (a+2)x_1 + 3x_2 - x_3 + (a-2)x_4, (a+b)x_1 + (c-3)x_2 + (-b-1)x_3 + 2x_4] \subset \mathbb{K}[a,b,c][x_1,x_2,x_3,x_4]$ where a, b, c are parameters

and x_1, x_2, x_3, x_4 are variables. Using our Maple implementation of Comparison algorithm we have:
$\texttt{sort(F, Comparison)} = [(a+2)x_1 + 3x_2 - x_3 + (a-2)x_4, 2x_1 + 2x_2 - bx_3 + (c+1)x_4, (a-1)x_1 + x_2 + (a+1)x_3 + (c^2-1)x_4, (a+b)x_1 + (c-3)x_2 + (-b-1)x_3 + 2x_4]$.

We can now install the Comparison algorithm in the PF_4 procedure, referred to as the Improved-PF_4 algorithm, to prevent the generation of additional branches, thereby improving timing and memory efficiency in Gröbner system computations.

Algorithm 6 Improved-PF_4

Require: $F \subset \mathbb{K}[\mathbf{a}, \mathbf{x}] = \mathbb{K}[a_1, \ldots, a_m, x_1, \ldots, x_n]$, $\prec_{\mathbf{x}}, \prec_{\mathbf{a}}$; two monomial orderings
Ensure: G; A Gröbner system of $\langle F \rangle$ with respect to $\prec_{\mathbf{x},\mathbf{a}}$

```
OUTSYS := NULL
F := sort(F, Comparison)
A :=GES([ ], [ ], F)
for (N_n, W_n, F_n) ∈ A do
  if F_n = [ ] then
    OUTSYS:= OUTSYS, (N_n, W_n, [ ])
  end if
  if there is any constant or non-zero parameter in F_n then
    OUTSYS:= OUTSYS, (N_n, W_n, [1])
  else
    t := |F_n| (the cardinality of F_n)
    B := [[{i, j}, deg(lcm(LM_≺x(F_n[i]), LM_≺x(F_n[j])))] | 1 ≤ i < j ≤ t, gcd(LM_≺x(F_n[i]), LM_≺x(F_n[j])) ≠ 1]
    if B = [ ] then
      OUTSYS:= OUTSYS, (N_n, W_n, F_n)
    else
      SYS := [[N_n, W_n, F_n, t, B]]
    end if
  end if
  PF4Basis(SYS)
end for
```

Example 3.2. Let $F = [(m^5 - b)x + n - 1, y + (b^3m^2 - n)z - 1, b^3z^2 - mz - 1] \subset \mathbb{K}[b, m, n][x, y, z]$, where x, y, z are variables and b, m, n are parameters. We use the monomial orderings $z \prec_{lex} y \prec_{lex} x$ and $n \prec_{lex} m \prec_{lex} b$. Applying our implementation of the Improved-PF_4 algorithm in `Maple`, we derive the following Gröbner system for the ideal $\langle F \rangle$ w.r.t. the elimination product ordering of these monomial orderings:

$$\begin{cases} ([m^5 - b], [m, -1 + n], & [1]), \\ ([m, b], [\,], & [1]), \\ ([\,], [b, -m^5 + b], & [b^3z^2 - mz - 1, b^3m^2z - nz + y - 1, m^5x - bx + n - 1]), \\ ([-1 + n, -m^5 + b], [m], & [m^{15}z^2 - mz - 1, m^{17}z + y - z - 1]) \\ ([b], [m], & [-mz - 1, my - m + n, m^5x + n - 1]). \end{cases}$$

As evident, the computed Gröbner system with the Improved-PF_4 algorithm has five branches. This is even though the Gröbner system calculated using our `Maple` implementation of the PF_4 algorithm is as follows, which has six branches, that is, one branch more than the system computed by Improved-PF_4 algorithm.

$$\begin{cases} ([m^5 - b], [m, -1 + n], & [1]), \\ ([m, b], [-1 + n], & [1]), \\ ([-1 + n, m, b], [\,], & [1]), \\ ([\,], [b, -m^5 + b], & [m^5x - bx + n - 1, b^3m^2z - nz + y - 1, b^3z^2 - mz - 1]), \\ ([b], [m], & [m^5x + n - 1, -nz + y - 1, -mz - 1]), \\ ([-1 + n, -m^5 + b], [m], & [m^{17}z + y - z - 1, m^{15}z^2 - mz - 1]). \end{cases}$$

The second branch of the first system, $([m^5 - b], [m, -1 + n], [1])$, contains the information of both the second and third branches of the second system, namely $([m, b], [-1 + n], [1])$ and $([-1 + n, m, b], [\,], [1])$. The PF_4 algorithm

generates new branches when encountering an undecidable leading coefficient, leading to many redundant branches and reduced efficiency. This issue can be solved by employing selection strategies to sort the input polynomial ideals.

4 Examples and Comparison

This section compares the performance of the Improved-PF_4 algorithm with the PF_4 algorithm, using implementations in `Maple 18`. We selected specific parametric ideals in the ring $\mathcal{S} = \mathbb{K}[a, b, c, d, m, n, r, t][x, y, z, u, v, w]$ and aimed to compute a Gröbner system for each ideal with respect to the orderings $w \prec_{lex} v \prec_{lex} u \prec_{lex} z \prec_{lex} y \prec_{lex} x$ and $t \prec_{lex} r \prec_{lex} n \prec_{lex} m \prec_{lex} d \prec_{lex} c \prec_{lex} b \prec_{lex} a$.

- EX.1 = $[abcxyz - a - b - c, abxy - a - b, ax^3 - bc, by^3 - c, cz^3 - a]$
- EX.2 = $[ab^4cuxz - a - c, aby^2 - a^2 + b^2, abuxz - c]$
- EX.3 = $[(d - c)yz - b - a, abz^3 - (d - 1)y, acx^3 - d, by^3 - cx]$
- EX.4 = $[b(1 - c)tzx - b + a + n, (d - a)y - t + m, cax^2 - (1 - n)x, x - b]$
- EX.5 = $[y + m - n, b(1 - c)tzx - b + a + n, (d - a)y - t + m, cax^2 - (1 - n)x, x^2 - b]$
- EX.6 = $[(bd - a)y + c - b, cax^2z - (1 - r)x, x^2 - b, y + m - n, t^2(n - c)zx + a - b]$
- EX.7 = $[a(r - t)x^2 + a - 1, (-ab + cd)z - n + r, abcx - (a - r)u, x^2 - b, y + m - n, -rt + z^2]$
- EX.8 = $[arx^3 - (n - a)x, (-ab + d)z^2 - n + r, abcx - (a - r)u, x^2 - b, y + m - n, -rt + z^2]$
- EX.9 = $[amny^3 - rx, (-ab + 2)yx^2 - cx^2, -ty + y^2, z + b - c, x^2 - d, uv - m]$
- EX.10= $[(-ab + n)x^2 - cz^2, z^3 - az, z + b - c, -duv + x^2 - m, mny^4 - r - x]$
- EX.11= $[a^2bcx^3yz^2 - av + nu - b, abxy^2 - d - m, ax^4 - bt - d, ry^2 - c, cz^3 - a - n]$

Example	Method	Time (Sec)	Used Memory (GB)	Branch
EX.1	Improved-PF_4	3.51	0.82	11
	PF_4	4.74	1.25	14
EX.2	Improved-PF_4	0.17	0.21	5
	PF_4	0.35	0.24	6
EX.3	Improved-PF_4	8.37	1.82	30
	PF_4	10.71	2.03	32
EX.4	Improved-PF_4	1.94	0.31	28
	PF_4	2.51	0.35	34
EX.5	Improved-PF_4	2.03	0.25	20
	PF_4	7.26	1.19	55
EX.6	Improved-PF_4	1.38	0.31	26
	PF_4	2.76	0.53	44
EX.7	Improved-PF_4	2.94	0.69	27
	PF_4	4.63	1.65	53
EX.8	Improved-PF_4	10.74	8.33	21
	PF_4	73.21	16.57	39
EX.9	Improved-PF_4	0.59	0.05	37
	PF_4	4.63	0.86	56
EX.10	Improved-PF_4	8.25	1.46	101
	PF_4	12.87	1.63	126
EX.11	Improved-PF_4	1.86	0.59	52
	PF_4	3.82	1.01	65

The results are presented in the tables above, with timings recorded on a personal computer equipped with a Ryzen 6800 processor, 8 GB RAM, and a 64-bit Windows 10 operating system. The third and fourth columns indicate the CPU time (in seconds) and memory usage (in gigabytes) for each procedure, respectively. The last column displays the number of branches in the computed Gröbner system. A comparison of the timing columns and our tests across various examples demonstrates the efficiency of our implemented Improved-PF_4 algorithm.

Acknowledgment

References

[1] Buchberger, B. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. Symbolic and algebraic computation, EUROSAM '79, int. Symp., Marseille 1979, Lect. Notes Comput. Sci. 72, 3-21 (1979)., 1979.

[2] Buchberger, B. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. Translation from the German. *J. Symb. Comput. 41*, 3-4 (2006), 475–511.

[3] Dehghani Darmain, M., and Hashemi, A. A Parametric F_4 Algorithm. *Iranian Journal of Mathematical Sciences and Informatics 19*, 1 (2024), 117–133.

[4] Dehghani Darmian, M., and Hashemi, A. Parametric FGLM algorithm. *J. Symb. Comput. 82* (2017), 38–56.

[5] Dehghani Darmian, M., and Hashemi, A. Generalization of the F_4 Algorithm to Parametric Polynomial Ideals. In *7th International Conference on Combinatorics, Cryptography, Computer Science and Computation, I4C 2022*. 2022, pp. 1014–1021.

[6] Dehghani Darmian, M., Hashemi, A., and Montes, A. Erratum to "A new algorithm for discussing Gröbner bases with parameters" [J. Symbolic Comput. 33 (1-2) (2002) 183-208]. *J. Symb. Comput. 46*, 10 (2011), 1187–1188.

[7] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra 139*, 1-3 (1999), 61–88.

[8] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 international symposium on symbolic and algebraic computation, ISSAC 2002, Lille, France, July 07–10, 2002*. New York, NY: ACM Press, 2002, pp. 75–83.

[9] Hashemi, A., Dehghani Darmian, M., and M.-Alizadeh, B. Applying Buchberger's criteria on Montes's DisPGB algorithm. *Bull. Iran. Math. Soc. 38*, 3 (2012), 715–724.

[10] Kapur, D., Sun, Y., and Wang, D. A new algorithm for computing comprehensive Gröbner systems. In *Proceedings of the 35th international symposium on symbolic and algebraic computation, ISSAC 2010, Munich, Germany, July 25–28, 2010*. New York, NY: Association for Computing Machinery (ACM), 2010, pp. 29–36.

[11] Lazard, D. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. Computer algebra, EUROCAL '83, Proc. Conf., London 1983, Lect. Notes Comput. Sci. 162, 146-156 (1983)., 1983.

[12] Montes, A. A new algorithm for discussing Gröbner bases with parameters. *J. Symb. Comput. 33*, 2 (2002), 183–208.

[13] Suzuki, A., and Sato, Y. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *In Proceedings of the 2006 international symposium on symbolic and algebraic computation, ISSAC 06, Genova, Italy, July 9–12, 2006*. New York, NY: ACM Press, 2006, pp. 326–331.

[14] Weispfenning, V. Comprehensive Gröbner bases. *J. Symb. Comput. 14*, 1 (1992), 1–29.

[15] Weispfenning, V. Canonical comprehensive Gröbner bases. *J. Symb. Comput. 36*, 3-4 (2003), 669–683.

Email: mdehghanidarmian@nus.ac.ir
Email: m.dehghanidarmian@ipm.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Enhancement of the CSS Algorithm for Solving ODE Systems with Parametric Coefficients Through Parametric Linear Algebra

Mahdi Dehghani Darmian[1]
Department of Mathematics, National University of Skills (NUS), Tehran, Iran

Abstract

In this paper, we enhance the CSS algorithm [5], which addresses parametric ODE systems through Gröbner systems. Our enhancement utilizes parametric linear algebra techniques to reduce the computational complexity of Gröbner systems. The Enhanced-CSS algorithm takes a parametric ODE system as input and returns a solution for the input parametric ODE system so-called *comprehensive solution system*. We have implemented this enhanced algorithm in `Maple` and demonstrate its structure with a simple example.

Keywords: CSS algorithm, Enhanced-CSS algorithm, comprehensive solution systems, Parametric linear ODE systems, Gröbner systems.
Mathematics Subject Classification [2010]: 93C15, 13P10

1 Introduction

Many engineering and scientific problems can be modeled using differential equations with parametric coefficients, requiring repeated analysis across various parameter values. Thus, this paper focuses on the solution of first-order parametric ordinary differential equations (ODEs), a topic not previously explored in the literature. We consider systems with an equal number of unknown functions and equations, expressed as

$$\frac{dx_j}{dt} = a_{j1}x_1 + \cdots + a_{jn}x_n + g_j(t), \quad j = 1, \ldots, n,$$

where n is a positive integer, a_{ji} are parametric polynomials, and $g_j(t)$ are arbitrary functions of the independent variable t. A first-order linear system of ODEs with parametric coefficients can be succinctly written as

$$\dot{\mathbf{x}}(t) = \mathbf{A}(a_1, \ldots, a_m)\mathbf{x}(t) + \mathbf{g}(t).$$

Here, $\mathbf{A}(a_1, \ldots, a_m)$ is the coefficient matrix containing parametric entries. These systems can also be represented in matrix form as follows:

$$\frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{bmatrix}.$$

Dehghani Darmian, in [5], utilized Gröbner systems from computer algebra to develop a *comprehensive solution system* for systems of parametric ODEs. He partitioned the parameter space into a finite number of cells, providing corresponding solutions for each, and introduced the CSS algorithm to compute a comprehensive solution system for such systems. In the following section, we will summarize the CSS algorithm.

[1] speaker

2 Comprehensive Solution Systems and CSS Algorithm

In this section, we restate from [5] the concept of a comprehensive solution system for parametric first-order ODEs system and outline the CSS algorithm for its computation using Gröbner systems. Gröbner systems, an extension of Gröbner bases for polynomials with parametric coefficients introduced by Weispfenning in 1992 [18], allow us to partition the parameter space into a finite set of cells, each associated with a set of polynomials. For given parameter values, we identify the corresponding cell, and the polynomials within it form a Gröbner basis for the ideal defined by those values.

Our focus is on the polynomial ring $\mathcal{R} = \mathbb{K}[x_1, \ldots, x_n]$ over a field $\mathbb{K}$. Let $\mathcal{I} = \langle f_1, \ldots, f_k \rangle \subset \mathcal{R}$ be a polynomial ideal generated by the polynomials f_i. For any polynomial $f \in \mathcal{R}$, the leading monomial with respect to a monomial ordering $\prec$, denoted by $\mathrm{LM}_\prec(f)$, is the largest such monomial in f. Its coefficient is the leading coefficient, $\mathrm{LC}_\prec(f)$, and the leading term is given by $\mathrm{LT}_\prec(f) = \mathrm{LC}_\prec(f) \cdot \mathrm{LM}_\prec(f)$. The leading monomial ideal of $\mathcal{I}$ is defined as $\mathrm{LM}_\prec(\mathcal{I}) = \langle \mathrm{LM}_\prec(f) \mid f \in \mathcal{I} \rangle$. A finite subset $\{g_1, \ldots, g_m\} \subset \mathcal{I}$ is a Gröbner basis for $\mathcal{I}$ w.r.t. $\prec$ if $\mathrm{LM}_\prec(\mathcal{I}) = \langle \mathrm{LM}_\prec(g_1), \ldots, \mathrm{LM}_\prec(g_m) \rangle$. The concept of Gröbner bases and the first algorithm for computing them were introduced by Buchberger in his Ph.D. thesis under Gröbner's supervision. For further details, readers may refer to [1].

Using these notions, we define Gröbner bases for ideals with polynomial generators containing parametric coefficients, termed Gröbner systems. These systems find applications across mathematics, science, and engineering, particularly in parametric linear algebra [4, 6, 10], automated geometry theorem proving [14], robotics [13, 15], algebraic geometry [8, 14, 15, 18], electrical networks [15, 16], and beyond. They are especially valuable for analyses involving varying parameter values.

Gröbner systems generalize Gröbner bases for polynomial ideals over fields to those with parametric coefficients. We consider the polynomial ring $\mathcal{S} = \mathbb{K}[\mathbf{a}, \mathbf{x}]$, with $\mathbf{x} = x_1, \ldots, x_n$ as variables and $\mathbf{a} = a_1, \ldots, a_m$ as parameters, ensuring the sets $\{\mathbf{x}\}$ and $\{\mathbf{a}\}$ are disjoint. A term in $\mathcal{S}$ can be expressed as $\mathbf{a}^\gamma \mathbf{x}^\alpha$, where $\mathbf{a}^\gamma \in \mathbb{K}[\mathbf{a}]$ is a coefficient of $\mathbf{x}^\alpha$. We define two monomial orderings: $\prec_\mathbf{x}$ for the variables and $\prec_\mathbf{a}$ for the parameters. To compute Gröbner systems, we establish a product order $\prec_{\mathbf{x},\mathbf{a}}$, where for $\gamma, \delta \in \mathbb{N}^m$ and $\alpha, \beta \in \mathbb{N}^n$, we have $\mathbf{a}^\gamma \mathbf{x}^\alpha \prec_{\mathbf{x},\mathbf{a}} \mathbf{a}^\delta \mathbf{x}^\beta$ if $\mathbf{x}^\alpha \prec_\mathbf{x} \mathbf{x}^\beta$, or if both are equal and $\mathbf{a}^\gamma \prec_\mathbf{a} \mathbf{a}^\delta$. Furthermore, a specialization of parameters is defined as a morphism $\sigma : \mathbb{K}[\mathbf{a}] \to \overline{\mathbb{K}}$, where $\overline{\mathbb{K}}$ represents the algebraic closure of $\mathbb{K}$.

A parametric polynomial ideal consists of a system of polynomial equations generated by polynomials with parametric coefficients. A parametric linear polynomial is defined as one where the power of each variable x_i is at most one, allowing parametric coefficients to be polynomials of any power in $\mathbb{K}[\mathbf{a}]$.

We now revisit the Gröbner system for parametric polynomial ideals, as introduced by Weispfenning in [18]. He demonstrated that every parametric polynomial ideal has a Gröbner system [18, Proposition 3.4 and Theorem 2.7] and proposed an algorithm for its computation [18, Theorem 3.6]. Since then, various algorithms have emerged for computing these Gröbner systems, each with its pros and cons [2, 3, 6, 7, 8, 9, **?**, 11, 15, 17].

Definition 2.1. Let $F = \{f_1, \ldots, f_k\} \subset \mathcal{S}$ and $\mathcal{G} = \{(N_i, W_i, G_i)\}_{i=1}^{\ell}$ be a finite triple set where $N_i, W_i \subset \mathbb{K}[\mathbf{a}]$ and $G_i \subset \mathcal{S}$ are finite for $i = 1, \ldots, \ell$. The set $\mathcal{G}$ is called a Gröbner system for $\langle F \rangle$ with respect to $\prec_{\mathbf{x},\mathbf{a}}$ over $\mathcal{V} \subseteq \overline{\mathbb{K}}^m$ if:

- $\sigma(G_i)$ is a Gröbner basis of $\langle \sigma(F) \rangle$ with respect to $\prec_\mathbf{x}$ for any specialization $\sigma : \mathbb{K}[\mathbf{a}] \to \overline{\mathbb{K}}$ satisfying (N_i, W_i);
- $\mathcal{V} \subseteq \bigcup_{i=1}^{\ell} \mathbb{V}(N_i) \setminus \mathbb{V}(W_i)$, where $\mathbb{V}(N)$ denotes the common zeros of a set of generators for N.

Each triple (N_i, W_i, G_i) is referred to as a branch of the Gröbner system $\mathcal{G}$ for $1 \leq i \leq \ell$. If $\mathcal{V} = \overline{\mathbb{K}}^m$, then $\mathcal{G}$ is typically called a Gröbner system of F. Each pair (N_i, W_i) is termed a specification or parametric constraint (with N_i and W_i as the null and non-null condition sets, respectively). A parametric constraint (N, W) is considered inconsistent if for any polynomial $f \in W$, f is in the radical ideal generated by N.

Example 2.2. Let $F = \{(1-c)y - ax^2, x + by^2\} \subset \mathbb{K}[a, b, c, x, y]$, where a, b, c are parameters and x, y are variables. Using our implementation of the PF_4 algorithm in `Maple`, we obtain the following CGS for $\langle F \rangle$ with respect to the product ordering $y \prec_{lex} x$ and $c \prec_{lex} b \prec_{lex} a$:

$$\begin{cases} ([\,], & [ab^2], & [ab^2y^4 - y + cy, x + by^2]) \\ ([ab^2], & [c-1], & [cy - y, x + by^2]) \\ ([c-1, ab^2], & [\,], & [x + by^2]). \end{cases}$$

For example, if $a = 2$, $b = 1$, and $c = 3$, the first branch corresponds to these parameter values. Thus, $\{2y^4 - y + 3y, x + y^2\}$ forms a Gröbner basis for the ideal $\langle F\rangle_{|a=2,b=1,c=3} = \langle -2y - 2x^2, x + y^2\rangle$.

We are now prepared to represent a comprehensive solution system for parametric first-order ODEs. We start by linearizing the ODEs through the substitution of all functional variables and their derivatives with new variables A_i, rearranging the equations to set the right-hand sides to zero. Next, we construct an ideal in $\mathbb{R}[\mathbf{a}, \mathbf{A}]$ corresponding to the ODEs and compute its Gröbner system, where $\mathbf{a}$ represents the sequence of parameters and $\mathbf{A}$ denotes the sequence of new tag variables A_i.

Definition 2.3. Let *sys* be a system of first-order ODEs with parametric coefficients. A finite triple set $L = \{(N_i, W_i, S_i)\}_{i=1}^{\ell}$ is a *comprehensive solution system* of *sys* if, for each i and any specialization $\sigma : \mathbb{R}[\mathbf{a}] \to \mathbb{R}' \supseteq \mathbb{R}$ that meets the parametric constraints (N_i, W_i), the solution set of $\sigma(S_i)$ is equivalent to that of $\sigma(sys)$.

Based on this definition, we introduce the CSS algorithm to compute a comprehensive solution. In this algorithm, the variable **LIST** starts as an empty set and ends as a comprehensive solution system. Each entry in **LIST** comprises a triple (N_i, W_i, S_i), where (N_i, W_i) represents a parametric constraint, and S_i is a solution set for the parametric ODE system corresponding to (N_i, W_i). If T is a list or set, the i-th element is denoted by $T[i]$. Additionally, the transformation ψ is a bijection that maps each functional variable m_i and its derivatives to tag variables A_i. The inverse ψ^{-1} replaces any variable A_i with the corresponding functional variable m_i.

Algorithm 1 CSS (Comprehensive Solution System)

Require: $sys = \{\frac{dx_j}{dt} = a_{j1}x_1 + \cdots + a_{jn}x_n + g_j(t)\}_{j=1}^{n}$: system of parametric first-order ODEs
Ensure: A Comprehensive Solution System of *sys*
  $F := \{\frac{dx_j}{dt} - (a_{j1}x_1 + \cdots + a_{jn}x_n + g_j(t))\}_{j=1}^{n}$
  $L := \psi(F)$; a linearization of F
  $G := \{(N_i, W_i, G_i)\}_{i=1}^{\ell}$, a Gröbner system of L
  LIST:= { }
  for i **from** 1 **to** ℓ **do**
    F_i' := the system $\{\psi^{-1}(G_i[j]) = 0 \mid j = 1, \ldots, n\}$
    S_i := the solution set of F_i' obtained via classical methods
    LIST:= LIST $\bigcup$ $\{(N_i, W_i, S_i)\}$
  end for
  Return (LIST)

We demonstrate this technique with a simple example.

Example 2.4. Consider the following system of two parametric first-order ODEs:

$$sys = \begin{cases} \dot{x}(t) = (a-1)x(t) + by(t) + d \\ \dot{y}(t) = (b-c)x(t) + ay(t) - 1 \end{cases}$$

We define $F = \{\dot{x}(t) - (a-1)x(t) - by(t) - d = 0, \dot{y}(t) - (b-c)x(t) - ay(t) + 1 = 0\}$ and apply a bijective linear transformation ψ to derive the linearization

$$L = \psi(F) = \{A_3 - (a-1)A_1 - bA_2 - dA_5, A_4 - (b-c)A_1 - aA_2 + A_5\}.$$

Using the GES-GVW-CGS algorithms [2] for computing Gröbner systems, we obtain the following Gröbner system for L:

$$\begin{cases} ([a-1],[b,b-c], & [bA_2+dA_5-A_3, bA_1-cA_1+A_2-A_4-A_5]) \\ ([b,a-1],[c], & [-dA_5+A_3, cA_1-A_2+A_4+A_5]) \\ ([c,b,a-1],[1], & [-dA_5+A_3, A_2-A_4-A_5]) \\ ([b-c,a-1],[c], & [-cA_4-cA_5-dA_5+A_3, A_2-A_4-A_5]) \\ ([a^2-b^2+bc-a],[b,a-1,b-c], & [-adA_5+aA_3-bA_4-bA_5, aA_1+bA_2+dA_5-A_1-A_3]) \\ ([b,a],[c], & [-cdA_5+cA_3-A_4-A_5, -dA_5+A_1+A_3]) \\ ([c,b,a],[1], & [A_4+A_5, -dA_5+A_1+A_3]) \\ ([b-c,a],[c], & [A_4+A_5, -cA_2-dA_5+A_1+A_3]) \\ \\ ([\,],[(a-1)(a^2-b^2+bc-a)], & [(a^2-b^2+bc-a)A_2+(1-bd+cd-a)A_5+(1-a)A_4+ \\ & (b-c)A_3, aA_1+bA_2+dA_5-A_1-A_3]). \end{cases}$$

Transforming all G_i back into the original functions and derivatives results in a system of nine triples:

$$\begin{cases} ([a-1],[b,b-c], & [by(t)+d-\dot{x}(t), bx(t)-cx(t)+y(t)-\dot{y}(t)-1]) \\ ([b,a-1],[c], & [-d+\dot{x}(t), cx(t)-y(t)+\dot{y}(t)+1]) \\ ([c,b,a-1],[1], & [-d+\dot{x}(t), y(t)-\dot{y}(t)-1]) \\ ([b-c,a-1],[c], & [-c\dot{y}(t)-d+\dot{x}(t), y(t)-\dot{y}(t)-1]) \\ ([a^2-b^2+bc-a],[b,a-1,b-c], & [-ad+a\dot{x}(t)-b\dot{y}(t)-b, ax(t)+by(t)+d-\dot{x}(t)]) \\ ([b,a],[c], & [-cd+c\dot{x}(t)-\dot{y}(t)-1, -d+\dot{x}(t)]) \\ ([c,b,a],[1], & [\dot{y}(t)+1, -d+\dot{x}(t)]) \\ ([b-c,a],[c], & [\dot{y}(t)+1, -cy(t)-d+\dot{x}(t)]) \\ \\ ([\,],[(a-1)(a^2-b^2+bc-a)], & [(a^2-b^2+bc-a)y(t)+(1-bd+cd-a)+(1-a)\dot{y}(t)+ \\ & (b-c)\dot{x}(t), ax(t)+by(t)+d-\dot{x}(t)]). \end{cases}$$

The solution sets S_i can be computed using established methods such as the Laplace transform, the elimination method, or operator method D [12], applied to the third component of the branches (e.g., `PDEtools:-dsolve(sys)` in `Maple 18`). Due to the length and complexity of some solutions, we focus on the fourth branch, which is defined by the conditions $b-c=0$, $a-1=0$, and $x\neq 0$:

$$\{x(t) = C_2(ce^t) + (c+d)t + C_1,\ y(t) = C_2e^t + 1\}.$$

For instance, with $a=1$, $b=2$, $c=2$, and $d=-1$ (values in (N_4, W_4)), the resulting solution set is:

$$\{x(t) = 2C_2e^t + t + C_1,\ y(t) = C_2e^t + 1\}.$$

Therefore, for any $1 \leq i \leq 9$ and each specialization σ corresponding to (N_i, W_i), we can obtain a solution set for a system of parametric first-order ODEs, referred to as a comprehensive solution system.

3 Enhanced-CSS Algorithm and Parametric Lineaar Algebra

Computing comprehensive solution systems using Gröbner systems presents challenges. Suzuki and Sato note that calculating Gröbner systems for parametric linear ideals is often "slow and inefficient" [17], a sentiment supported by the comparison in [6, Page 48]. To address these inefficiencies, we adopt a modified version of the GES algorithm from [6, Algorithm 3], which serves as a parametric form of the Gaussian elimination method and avoids Gröbner system complexities. This approach helps us compute comprehensive solution systems based on the LDS algorithm introduced in [6].

Before proceeding, we briefly review parametric linear algebra techniques essential for achieving our goal outlined in [6, Section 3]. The GES algorithm outputs a Gaussian elimination system for a matrix with parametric entries, equivalent to a linear system with parametric coefficients. Our application, however, focuses on first-order ordinary differential equations (ODEs), seeking to establish the solution set according to specified conditions. This requires linearizing the input ODEs by substituting the functional variables with new variables to simplify the system.

A key component of the GES algorithm is the LDS algorithm [6, Algorithm 2], which enhances the overall efficiency and design by checking parametric linear dependencies. The LDS algorithm analyzes the dependencies within a linear parametric polynomial relative to parametric polynomials without relying on Gröbner systems, streamlining our analysis. To illustrate these concepts, we provide the following example, and for further information on the LDS algorithm and its applications, readers may refer to [6].

Example 3.1. Consider $(N, W) = ([m, n], [a-1, a-b, 1-b])$ as a specification, $G = [u+v, (a-1)y-cz, (a-b)x-acz-bv, (b-1)yx-czx+(bv+cz)y+c^2z^2]$ as a linear Gröbner basis for the pair (N, W), and $g = av-bw+mz+nx-u-cy$, a parametric polynomial. We set the monomial orderings $n \prec_{lex} m \prec_{lex} c \prec_{lex} b \prec_{lex} a$ and $w \prec_{lex} v \prec_{lex} u \prec_{lex} z \prec_{lex} y \prec_{lex} x$. Thus, using our `Maple` implementation of the LDS algorithm, the linear dependency system of g on G according to (N, W) is:

$$\text{Sys} = \begin{cases} ([m,n],[c,a-1,a-b,1-b], & [false,[-1,\frac{c}{1-a},0,0],\frac{c^2z}{1-a}+(a+1)v-bw]), \\ ([m,n,c],[a-1,a+1,a-b,1-b], & [false,[-1,\frac{c}{1-a},0,0],\frac{c^2z}{1-a}+(a+1)v-bw]), \\ ([m,n,c,a+1],[b,b+1,1-b], & [false,[-1,\frac{c}{1-a},0,0],\frac{c^2z}{1-a}-bw]), \\ ([m,n,c,a+1,b],[\,], & [true,[-1,\frac{c}{1-a},0,0],0]). \end{cases}$$

Using the LDS algorithm, we can efficiently implement the modified GES algorithm to compute a Gaussian elimination system for parametric polynomials. In the GES algorithm, Sys starts as an empty set and evolves into a Gaussian elimination system. Each entry in Sys is a triple (N, W, G), where (N, W) represents a parametric constraint and G denotes the Gaussian elimination form of the input parametric polynomials associated with (N, W). If B is a list or set, its i-th element is denoted as $B[i]$.

Algorithm 2 GES (Gaussian Elimination System)

Require: $F \subset \mathbb{R}[\mathbf{a}, \mathbf{A}]$; $\mathbf{a}$ is a sequence of parameters, and $\mathbf{A}$ represents the variables A_i.
Ensure: A Gaussian elimination system for F

```
Sys:= {}
A := {(N, W, {}, L[1], L)}
while A ≠ {} do
  a := A[1] and A := A \ {a}
  if a[5] = {} then
    Sys:=Sys ⋃{(a[1], a[2], a[3])}
  else
    G := a[5] \ {a[4]} and g := G[1]
    P :=LDS(a[1], a[2], a[3], a[4])
    for i = 1 to |P| do
      Let P[i] = (N1, W1, [flag, Q, f])
      if flag = true then
        A := A ∪ {(N1, W1, a[3], g, G)}
      else
        A := A ∪ {(N1, W1, a[3] ∪ {f}, g, G)}
      end if
    end for
  end if
end while
Return (Sys)
```

The algorithm's operation is illustrated step-by-step in [6, Example 15], with the results below.

Example 3.2. Consider $F = \{(a-b)xy+z-1, ay+x^2-2, (a-1)y^3-x^2-bz\} \subset \mathbb{K}[a, b][x, y, z]$, a set of polynomials

with parametric coefficients. Applying the GES algorithm yields the following Gaussian elimination system for F:

$$\begin{cases} ([\,], & [a-b, a-1], & [axy - bxy + z - 1, ay + x^2 - 2, ay^3 - y^3 + ay - bz - 2]), \\ ([a-1], & [b-1], & [-bxy + xy + z - 1, x^2 + y - 2, -bz + y - 2]), \\ ([a-b], & [b-1], & [z - 1, by + x^2 - 2, by^3 - y^3 + by - b - 2]), \\ ([a-b, b-1], & [\,], & [z - 1, x^2 + y - 2, y - 3]). \end{cases}$$

Integrating the GES algorithm into the CSS algorithm improves its performance, leading to the Enhanced-CSS algorithm.

Algorithm 3 Enhanced-CSS

Require: $sys = \{\frac{dx_j}{dt} = a_{j1}x_1 + \cdots + a_{jn}x_n + g_j(t)\}_{j=1}^{n}$: a system of parametric first-order ODEs
Ensure: A Comprehensive Solution System of sys
  $F := \{\frac{dx_j}{dt} - (a_{j1}x_1 + \cdots + a_{jn}x_n + g_j(t))\}_{j=1}^{n}$
  $L := \psi(F)$; linearization of F
  $G := \{(N_i, W_i, G_i)\}_{i=1}^{\ell}$: a Gaussian elimination system of L using the GES algorithm
  LIST:= { }
  for $i = 1$ **to** ℓ **do**
    F'_i := the system $\{\psi^{-1}(G_i[j]) = 0 \mid j = 1, \ldots, n\}$
    S_i := the solution set of F'_i using established classical methods
    LIST:= LIST $\bigcup$ $\{(N_i, W_i, S_i)\}$
  end for
  Return (LIST)

Theorem 3.3. *The* Enhanced-CSS *algorithm terminates after a finite number of iterations and effectively computes a complete solution system.*

Proof. The termination of the Enhanced-CSS algorithm follows from the termination of the GES algorithm, while its correctness aligns with that of the CSS algorithm. □

All algorithms in this paper are implemented in `Maple 18`. Benchmark results indicate that the Enhanced-CSS algorithm, utilizing parametric linear algebra techniques, significantly outperforms the CSS algorithm based on Gröbner system computations. Nonetheless, Gröbner systems remain valuable tools for addressing mathematical, scientific, and engineering problems, such as solving parametric first-order ordinary differential equations. They aid in simplifying complex multivariable polynomial issues into clearer solutions, which is particularly useful in solving systems of parametric first-order ODEs, where parameter space partitioning can enhance computational efficiency.

Acknowledgment

References

[1] Cox, D., Little, J., and O'Shea, D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. 3rd ed.*, 3rd ed. ed. New York, NY: Springer, 2007.

[2] Dehghani Darmain, M. Improvement of an Incremental Signature-Based Comprehensive Gröbner System Algorithm. *Math.Comput.Sci. 18*, 12 (2024).

[3] Dehghani Darmain, M., and Hashemi, A. A Parametric F_4 Algorithm. *Iranian Journal of Mathematical Sciences and Informatics 19*, 1 (2024), 117–133.

[4] Dehghani Darmian, M. Efficient Algorithm for Computing Inverse of Parametric Matrices. *Scientific Annals of Computer Science 34*, 1 (2024), 1–22.

[5] Dehghani Darmian, M. Utilizing Gröbner systems to Solve Parametric Linear ODE Systems. In *17th Seminar on Differential Equations and Dynamical Systems*. 2024, p. accepted.

[6] Dehghani Darmian, M., and Hashemi, A. Parametric FGLM algorithm. *J. Symb. Comput. 82* (2017), 38–56.

[7] Dehghani Darmian, M., Hashemi, A., and Montes, A. Erratum to "A new algorithm for discussing Gröbner bases with parameters" [J. Symbolic Comput. 33 (1-2) (2002) 183-208]. *J. Symb. Comput. 46*, 10 (2011), 1187–1188.

[8] Hashemi, A., Dehghani Darmian, M., and Barkhordar, M. Gröbner systems conversion. *Math. Comput. Sci. 11*, 1 (2017), 61–77.

[9] Hashemi, A., Dehghani Darmian, M., and Barkhordar, M. Universal Gröbner basis for parametric polynomial ideals. In *Mathematical software – ICMS 2018. 6th international conference, South Bend, IN, USA, July 24–27, 2018. Proceedings*. Cham: Springer, 2018, pp. 191–199.

[10] Hashemi, A., M.-Alizadeh, B., and Dehghani Darmian, M. Minimal polynomial systems for parametric matrices. *Linear Multilinear Algebra 61*, 2 (2013), 265–272.

[11] Kapur, D., Sun, Y., and Wang, D. A new algorithm for computing comprehensive Gröbner systems. In *Proceedings of the 35th international symposium on symbolic and algebraic computation, ISSAC 2010, Munich, Germany, July 25–28, 2010*. New York, NY: Association for Computing Machinery (ACM), 2010, pp. 29–36.

[12] Logan, J. D. *A first course in differential equations*, 3rd ed. ed. Undergraduate Texts Math. Cham: Springer, 2015.

[13] Manubens, M., and Montes, A. Improving the DisPGB algorithm using the discriminant ideal. *J. Symb. Comput. 41*, 11 (2006), 1245–1263.

[14] Manubens, M., and Montes, A. Minimal canonical comprehensive Gröbner systems. *J. Symb. Comput. 44*, 5 (2009), 463–478.

[15] Montes, A. A new algorithm for discussing Gröbner bases with parameters. *J. Symb. Comput. 33*, 2 (2002), 183–208.

[16] Montes, A., and Castro, J. Solving the load flow problem using the Gröbner basis. *SIGSAM Bull. 29*, 1 (1995), 1–13.

[17] Suzuki, A., and Sato, Y. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *In Proceedings of the 2006 international symposium on symbolic and algebraic computation, ISSAC 06, Genova, Italy, July 9–12, 2006*. New York, NY: ACM Press, 2006, pp. 326–331.

[18] Weispfenning, V. Comprehensive Gröbner bases. *J. Symb. Comput. 14*, 1 (1992), 1–29.

Email: m.dehghanidarmian@gmail.com
Email: m.dehghanidarmian@ipm.ir

طراحی الگوریتم های رمزنگاری پساکوانتومی مبتنی بر توابع هش

رحیم اصغری [*۱]، محمد الهیاری [۲]

۱- گروه ریاضی، دانشگاه ملی مهارت ایران، تهران، ایران.

۲- گروه مهندسی برق، دانشگاه صنعتی ارومیه، ارومیه، ایران.

چکیده

رمزنگاری پسا کوانتومی بر پایه استفاده از مسائل ریاضی بسیار دشواری طراحی شده است که حتی برای کامپیوترهای کوانتومی نیز حل آن‌ها به زمان و منابع محاسباتی بسیار زیادی نیاز دارد. این الگوریتم‌ها از ویژگی‌هایی مانند سختی محاسباتی در مسائل مشبکه ای، چندجمله‌ای‌ها، یا توابع هش بهره می‌برند و تضمین می‌کنند که هیچ روش کوانتومی شناخته‌شده‌ای نمی‌تواند به سرعت و کارآمدی آن‌ها را بشکند. در این مقاله به بررسی الگوریتم های رمزنگاری مبتنی بر توابع هش می پردازیم.

کلمات کلیدی: امنیت سایبری، رمزنگاری پساکوانتومی، توابع هش.

۱. مقدمه

رمزنگاری پسا کوانتومی به‌عنوان یکی از شاخه‌های کلیدی در علوم رمزنگاری، بر توسعه الگوریتم‌هایی متمرکز است که در برابر تهدیدات محاسبات کوانتومی ایمن باشند. این شاخه علمی در پاسخ به توانایی کامپیوترهای کوانتومی در شکستن الگوریتم‌های رمزنگاری سنتی مانند RSA و ECC طراحی شده است. ضرورت رمزنگاری پسا کوانتومی در حفظ امنیت اطلاعات و سیستم‌های دیجیتال در عصری که فناوری‌های کوانتومی در حال پیشرفت هستند، به وضوح مشخص می‌شود[۱].

این حوزه رمزنگاری از مفاهیم پیشرفته ریاضی بهره می‌گیرد و الگوریتم‌هایی طراحی می‌کند که حتی در حضور کامپیوترهای کوانتومی نیز مقاوم بمانند. الگوریتم‌های رمزنگاری پسا کوانتومی عمدتاً بر پایه مشکلات ریاضیاتی دشوار مانند مسائل مشبکه ها، توابع هش و کدهای تصحیح خطا هستند که تاکنون راه‌حلی کارآمد برای شکستن آن‌ها توسط محاسبات کوانتومی ارائه نشده است. این ویژگی‌ها تضمین می‌کند که حتی در صورت توسعه فناوری کوانتومی، امنیت سیستم‌های ارتباطی به خطر نیفتد.

از نظر استراتژیک، رمزنگاری پسا کوانتومی به‌عنوان سنگ‌بنای امنیت زیرساخت‌های دیجیتال در برابر نفوذپذیری فناوری‌های آینده عمل می‌کند. این فناوری نه‌تنها برای محافظت از اطلاعات حساس در حال حاضر اهمیت دارد، بلکه برای اطمینان از دوام و قابلیت اعتماد زیرساخت‌های ارتباطی و اطلاعاتی در آینده ضروری است. رمزنگاری پسا کوانتومی با ارائه راه‌حل‌های پایدار و مقاوم در برابر تهدیدات نوظهور، یکی از کلیدهای اصلی حفظ امنیت در عصر دیجیتال محسوب می‌شود[۲].

رمزنگاری پسا کوانتومی بر پایه استفاده از مسائل ریاضی بسیار دشواری طراحی شده است که حتی برای کامپیوترهای کوانتومی نیز حل آن‌ها به زمان و منابع محاسباتی بسیار زیادی نیاز دارد. این الگوریتم‌ها از ویژگی‌هایی مانند سختی

[*] **Corresponding author:** استادیار گروه ریاضی
Email: rasghari@nus.ac.ir, meisam.mathhome@gmail.com

محاسباتی در مسائل مشبکه ای، چندجمله‌ای‌ها، یا توابع هش بهره می‌برند و تضمین می‌کنند که هیچ روش کوانتومی شناخته‌شده‌ای نمی‌تواند به سرعت و کارآمدی آن‌ها را بشکند. یکی از اصول مهم در طراحی این الگوریتم‌ها، حفظ امنیت در برابر الگوریتم‌هایی مانند شور (برای شکستن RSA و ECC) و گروور* (برای جستجوی سریع در فضاهای کلید) است[۳].

ویژگی کلیدی رمزنگاری پسا کوانتومی، سازگاری آن با سخت‌افزار و پروتکل‌های کلاسیک است، به گونه‌ای که می‌توان آن‌ها را بدون نیاز به تغییرات اساسی در زیرساخت‌های فعلی پیاده‌سازی کرد. این الگوریتم‌ها برخلاف رمزنگاری کوانتومی که به تجهیزات خاص کوانتومی وابسته‌اند، به‌صورت کاملاً نرم‌افزاری روی سیستم‌های کنونی قابل اجرا هستند. انعطاف‌پذیری بالا، امنیت اثبات‌شده ریاضی، و قابلیت استانداردسازی، رمزنگاری پسا کوانتومی را به گزینه‌ای جذاب برای جایگزینی الگوریتم‌های رمزنگاری فعلی تبدیل کرده است[۴].

در این مقاله به بررسی الگوریتم های رمزنگاری پساکوانتومی مبتنی بر توابع هش می پردازیم. در بخش دوم، مروری بر

۲. الگوریتم های رمزنگاری مبتنی بر توابع هش

الگوریتم‌های مبتنی بر تابع هش یکی از قدیمی‌ترین و ساده‌ترین روش‌های رمزنگاری هستند که امنیت آن‌ها بر اساس مقاومت تابع‌های هش در برابر حملات مختلف بنا شده است. این الگوریتم‌ها از ویژگی‌های خاص تابع‌های هش، مانند مقاومت در برابر برخورد و معکوس‌سازی، استفاده می‌کنند تا امنیت داده‌ها را تضمین کنند. برخلاف بسیاری از روش‌های پیچیده‌تر، الگوریتم‌های مبتنی بر هش نیازی به عملیات ریاضی سنگین ندارند و به همین دلیل ساختاری ساده و قابل اعتماد دارند[۱۰].

این الگوریتم‌ها بیشتر در حوزه امضای دیجیتال کاربرد دارند. امضاهای دیجیتال مبتنی بر هش، مانند امضای لمپورت† و امضای مرکل ‡ ، با استفاده از کلیدهای یک‌بارمصرف طراحی شده‌اند. در این سیستم‌ها، کلیدهای خصوصی و عمومی برای هر پیام منحصربه‌فرد هستند و امنیت پیام با استفاده از مقاومت تابع هش تضمین می‌شود. ساختار درخت مرکل در این الگوریتم‌ها، با استفاده از یک هش ریشه‌ای، امکان ایجاد تعداد زیادی امضای دیجیتال با اندازه کلید عمومی کوچک را فراهم می‌کند، که این ویژگی به کاهش پیچیدگی کمک می‌کند[۵, ۶, ۷].

یکی از مزایای بزرگ این الگوریتم‌ها، مقاومت بالا در برابر حملات کوانتومی است. در حالی که بسیاری از الگوریتم‌های سنتی مانند RSA و ECC در برابر رایانه‌های کوانتومی آسیب‌پذیر هستند، الگوریتم‌های مبتنی بر هش می‌توانند در برابر حملات کوانتومی مقاومت کنند. حتی با وجود الگوریتم گروور، که سرعت جستجوی تابع را افزایش می‌دهد، امنیت تابع‌های هش تنها به میزان جزئی کاهش می‌یابد و همچنان سطح بالایی از امنیت را ارائه می‌دهد.

برخلاف الگوریتم‌های دیگر مانند مبتنی بر شبکه های مشبکه یا کدگذاری، الگوریتم‌های هش نیازی به ذخیره‌سازی کلیدهای بزرگ یا اجرای عملیات پیچیده ندارند. این ویژگی باعث می‌شود که پیاده‌سازی آن‌ها در سیستم‌های محدود به منابع، مانند دستگاه‌های اینترنت اشیا و موبایل‌ها، آسان‌تر و کارآمدتر باشد. به‌علاوه، از آنجایی که تابع‌های هش به صورت بومی در بسیاری از زبان‌های برنامه‌نویسی و سخت‌افزارها پشتیبانی می‌شوند، استفاده از آن‌ها در نرم‌افزارها و پروتکل‌های امنیتی رایج است[۸].

با وجود مزایای متعدد، این الگوریتم‌ها چالش‌هایی نیز دارند. یکی از این چالش‌ها، اندازه نسبتاً بزرگ امضاهای دیجیتال و محدودیت تعداد امضاها برای هر مجموعه کلید است. در امضاهای لمپورت، برای هر بیت پیام نیاز به یک کلید خصوصی و

* Grover
† Lamport Signatures
‡ Merkle Signatures

عمومی جداگانه است، که منجر به مصرف منابع زیادی می‌شود. همچنین، مدیریت کلیدهای یک‌بارمصرف نیازمند دقت بالایی است، زیرا استفاده مجدد از کلید می‌تواند امنیت کل سیستم را به خطر بیندازد.
الگوریتم‌های مبتنی بر تابع هش یک روش امن و ساده برای رمزنگاری در عصر پسا کوانتومی ارائه می‌دهند. با وجود چالش‌های مرتبط با اندازه امضا و محدودیت تعداد امضاها، این الگوریتم‌ها به دلیل سادگی، امنیت بالا، و قابلیت پیاده‌سازی در محیط‌های محدود به منابع، همچنان یکی از انتخاب‌های مهم برای کاربردهای امنیتی، به‌ویژه در امضای دیجیتال و تأیید پیام‌ها، هستند. پیشرفت‌های مداوم در بهینه‌سازی این الگوریتم‌ها می‌تواند محدودیت‌های فعلی را کاهش دهد و کاربردهای آن‌ها را گسترش دهد[۹].

۲-۱ ویژگی‌های الگوریتم‌های مبتنی بر تابع هش

در این بخش مروری بر خواص مهم الگوریتم های رمزنگاری مبتنی بر هش می پردازیم که شامل موارد زیر هستند:

- **امنیت مبتنی بر سختی تابع‌های هش:** امنیت این الگوریتم‌ها بر پایه خصوصیات ریاضی تابع‌های هش مانند مقاومت در برابر معکوس‌سازی*، مقاومت در برابر برخورد† و مقاومت در برابر برخورد ثانویه‡ استوار است. این ویژگی‌ها تضمین می‌کنند که تولید دو ورودی مختلف با یک خروجی مشابه یا یافتن ورودی متناظر با یک خروجی خاص عملاً غیرممکن است[۱۱,۱۲].
- **سادگی ساختار و شفافیت:** الگوریتم‌های مبتنی بر تابع هش دارای ساختار ساده و قابل درکی هستند. این ویژگی باعث می‌شود که اثبات‌های امنیتی آن‌ها شفاف‌تر باشند. برخلاف الگوریتم‌هایی که از عملیات‌های ریاضی پیچیده مانند ضرب در میدان‌های محدود یا منحنی‌های بیضوی استفاده می‌کنند، این الگوریتم‌ها صرفاً بر عملیات هش متکی هستند[۱۰].
- **مقاومت در برابر حملات کوانتومی**: ین الگوریتم‌ها در برابر حملات کوانتومی مقاوم هستند. الگوریتم گروور، که سرعت جستجوی تابع را دو برابر می‌کند، تنها سطح امنیتی تابع‌های هش را به میزان جزئی کاهش می‌دهد(2^n به $2^{\frac{n}{2}}$) این امر باعث می‌شود که الگوریتم‌های مبتنی بر هش برای دوران پسا کوانتومی انتخابی مناسب باشند[۱۰].
- **کاربردهای متنوع:** این الگوریتم‌ها عمدتاً در سیستم‌های امضای دیجیتال استفاده می‌شوند. برای مثال، امضاهای لمپورت و مرکل نمونه‌های معروف این الگوریتم‌ها هستند. همچنین، ساختار درخت مرکل امکان ایجاد امضاهای دیجیتال متعدد با استفاده از یک ریشه هش را فراهم می‌کند، که این موضوع کارایی را افزایش و اندازه کلید عمومی را کاهش می‌دهد[۱۱].
- **پیاده‌سازی آسان و مناسب برای دستگاه‌های محدود به منابع:** به دلیل عدم نیاز به ذخیره‌سازی کلیدهای بزرگ و اجرای عملیات پیچیده، الگوریتم‌های مبتنی بر تابع هش برای سیستم‌های محدود به منابع، مانند دستگاه‌های اینترنت اشیا و موبایل‌ها، بسیار مناسب هستند. همچنین، تابع‌های هش در بسیاری از زبان‌های برنامه‌نویسی و سخت‌افزارها به صورت بومی پشتیبانی می‌شوند، که این ویژگی پیاده‌سازی آن‌ها را آسان‌تر می‌کند[۱۲].
- **چالش‌های مرتبط با اندازه امضا و مدیریت کلید:** یکی از چالش‌های این الگوریتم‌ها، اندازه بزرگ امضاهای دیجیتال در برخی روش‌ها و محدودیت تعداد امضاها برای هر مجموعه کلید است. برای مثال، امضاهای لمپورت

* Preimage Resistance
† Collision Resistance
‡ Second Preimage Resistance

به ازای هر بیت پیام نیاز به یک کلید خصوصی و عمومی جداگانه دارند. این موضوع باعث افزایش مصرف منابع و پیچیدگی مدیریت کلیدها می‌شود.

- **مقاومت در برابر خطاهای سخت‌افزاری و نرم‌افزاری:** به دلیل سادگی فرآیند هش‌گذاری و استفاده نکردن از محاسبات حساس به دقت عددی، این الگوریتم‌ها در برابر خطاهای سخت‌افزاری و نرم‌افزاری مقاوم‌تر هستند. این ویژگی در محیط‌های با منابع محدود یا شرایط سخت عملیاتی، مانند سامانه‌های نهفته، بسیار ارزشمند است.

الگوریتم‌های مبتنی بر تابع هش با ارائه امنیت قوی، سادگی در طراحی و پیاده‌سازی، و مقاومت در برابر حملات کوانتومی، یکی از گزینه‌های مهم در رمزنگاری پسا کوانتومی محسوب می‌شوند. با وجود چالش‌هایی مانند اندازه امضا و مدیریت کلیدها، این الگوریتم‌ها به دلیل قابلیت اعتماد و تطبیق‌پذیری بالا همچنان جایگاه ویژه‌ای در زمینه امنیت اطلاعات دارند.

نمونه هایی از الگوریتم مبتنی بر هش شامل امضای لامپورت و امضای مرکل است.

۳. نقش الگوریتم‌های مبتنی بر هش در امنیت پسا کوانتومی

الگوریتم‌های مبتنی بر هش به‌عنوان یکی از مؤثرترین رویکردها برای ارائه امنیت پسا کوانتومی شناخته می‌شوند. این الگوریتم‌ها به دلیل ساختار ساده، بازده بالا، و مقاومت در برابر تحلیل‌های کوانتومی مانند الگوریتم شور، به‌ویژه در طراحی پروتکل‌های رمزنگاری و امنیت مشبکه های بلاکچینی، اهمیت بالایی دارند.

الگوریتم‌های مبتنی بر هش از توابع هش رمزنگارانه برای ایجاد امنیت در پروتکل‌های مختلف استفاده می‌کنند. این توابع با دریافت یک ورودی دلخواه، یک خروجی با طول ثابت تولید می‌کنند که به آن هش می‌گویند. این خروجی به‌عنوان یک اثر انگشت دیجیتال عمل می‌کند و به‌طور منحصربه‌فرد نمایانگر داده ورودی است. توابع هش رمزنگارانه به دلیل ویژگی‌های امنیتی منحصربه‌فردشان، در حوزه‌هایی مانند رمزنگاری، بلاکچین، و امنیت اطلاعات بسیار حیاتی هستند[۱۱].

یکی از ویژگی‌های کلیدی این توابع، یک‌طرفه بودن است. این بدان معناست که با داشتن خروجی (هش)، بازگشت به ورودی اولیه غیرممکن یا بسیار دشوار است. این ویژگی تضمین می‌کند که حتی اگر مهاجمی به هش دسترسی پیدا کند، نمی‌تواند داده‌های اصلی را بازیابی کند. این خاصیت، امنیت اطلاعات را در سیستم‌های ذخیره‌سازی و انتقال داده به‌شدت افزایش می‌دهد.

ویژگی دیگر، مقاومت در برابر برخورد است. این ویژگی به این معناست که یافتن دو ورودی مختلف که هش یکسان تولید کنند، عملاً غیرممکن است. این خاصیت از بروز تناقض و آسیب‌پذیری در سیستم‌هایی که به هش وابسته‌اند، جلوگیری می‌کند. توابع هش مقاوم در برابر برخورد برای ایجاد امضای دیجیتال و تضمین صحت داده‌ها، نقشی اساسی دارند.

اثر بهمنی * ویژگی مهم دیگری است که تضمین می‌کند هر تغییر کوچک در ورودی، خروجی کاملاً متفاوتی تولید کند. این خاصیت باعث می‌شود که حتی تغییرات جزئی در داده اصلی قابل شناسایی باشند و امنیت کلی سیستم تقویت شود. انتشار اثر تغییر یکی از دلایلی است که توابع هش در شناسایی تغییرات و محافظت از یکپارچگی داده‌ها بسیار مؤثر هستند[۱۲].

ظهور کامپیوترهای کوانتومی تهدیدی جدی برای سیستم‌های رمزنگاری سنتی مبتنی بر کلید عمومی ایجاد کرده است. این سیستم‌ها، مانند RSA و ECC، به ریاضیات پیچیده‌ای متکی هستند که با استفاده از الگوریتم شور توسط کامپیوترهای کوانتومی می‌توان به‌سرعت رمزگشایی شوند. این توانایی کامپیوترهای کوانتومی به معنای کاهش امنیت این

* Avalanche Effect

سیستم‌ها به سطحی غیرقابل قبول است و نیاز به روش‌های جایگزین و مقاوم در برابر کوانتوم را به‌طور جدی مطرح می‌کند.

در این میان، توابع هش رمزنگارانه به‌دلیل ساختار خاص خود، در برابر الگوریتم شور مصون هستند. این توابع نیازی به کلیدهای عمومی یا خصوصی ندارند و بر مبنای عملیات ساده‌تر و مقاوم‌تری عمل می‌کنند. با این حال، کامپیوترهای کوانتومی می‌توانند از طریق الگوریتم جستجوی گروور، که جستجوی فضای کلیدها را بهینه می‌کند، حملاتی را علیه این توابع انجام دهند. تأثیر گروور به‌صورت خطی است و نه نمایی، که نشان می‌دهد توابع هش نسبت به رمزنگاری کلید عمومی، مقاومت بیشتری در برابر حملات کوانتومی دارند.

برای مقابله با تأثیر گروور، طول خروجی توابع هش باید افزایش یابد. به‌عنوان مثال، برای توابع هش با خروجی ۲۵۶ بیتی، امنیت در برابر گروور معادل ۱۲۸ بیت خواهد بود که همچنان سطح قابل قبولی از امنیت را فراهم می‌کند. در نتیجه، افزایش طول خروجی هش به ۵۱۲ بیت یا بیشتر می‌تواند امنیت را به میزان قابل توجهی افزایش دهد و مقاومت در برابر حملات کوانتومی را تضمین کند[۱۱,۱۲].

یکی از مزایای مهم توابع هش در دنیای پسا کوانتومی، سادگی و کارایی محاسباتی آن‌ها است. برخلاف سیستم‌های رمزنگاری کلید عمومی که نیاز به عملیات ریاضی پیچیده دارند، توابع هش با الگوریتم‌های ساده‌تری کار می‌کنند که نیاز به منابع محاسباتی کمتری دارند. این ویژگی باعث می‌شود که توابع هش، گزینه‌ای مناسب برای پیاده‌سازی در سیستم‌های گسترده و مقیاس‌پذیر مانند بلاکچین و اینترنت اشیا باشند.

الگوریتم‌های مبتنی بر هش یکی از پایه‌های امنیت در دنیای پسا کوانتومی محسوب می‌شوند. با تنظیم پارامترهایی مانند طول خروجی و استفاده از توابع هش قوی‌تر، می‌توان این الگوریتم‌ها را برای مقابله با تهدیدات کوانتومی آماده کرد. این ویژگی‌ها توابع هش را به یک انتخاب استراتژیک برای طراحی سیستم‌های امنیتی نسل بعد تبدیل می‌کند و نقش آن‌ها در حفظ امنیت داده‌ها در آینده بسیار حیاتی خواهد بود.

۴. انواع الگوریتم‌های مبتنی بر هش

الگوریتم‌های مبتنی بر هش کاربردهای متنوعی در حوزه رمزنگاری و امنیت اطلاعات دارند. این کاربردها از امضای دیجیتال گرفته تا بلاکچین و پروتکل‌های اثبات دانش صفر، به‌دلیل ویژگی‌های منحصربه‌فرد توابع هش از جمله امنیت بالا، سادگی محاسباتی، و مقاومت در برابر حملات کوانتومی، به یکی از اجزای اصلی سیستم‌های امنیتی مدرن تبدیل شده‌اند. در این بخش، به بررسی سه کاربرد کلیدی این الگوریتم‌ها پرداخته می‌شود.

- **امضای دیجیتال مبتنی بر هش:** امضای دیجیتال یکی از شناخته‌شده‌ترین و پرکاربردترین موارد استفاده از الگوریتم‌های مبتنی بر هش است. در دنیای پسا کوانتومی، امضاهای دیجیتال مبتنی بر هش مانند امضای لامپورت و امضای مرکله به‌عنوان جایگزین‌های مقاوم در برابر کوانتوم مطرح شده‌اند.
- **امضای لامپورت**: این امضا بر مبنای جفت کلیدهای تک‌بارمصرف (*One-Time Key Pairs*) عمل می‌کند. برای هر پیام، مجموعه‌ای از هش‌ها تولید می‌شود که امضای پیام را تشکیل می‌دهند. اگرچه این امضا به دلیل حجم بالای کلیدها محدودیت‌هایی دارد، اما به دلیل سادگی و مقاومت در برابر حملات کوانتومی، یک گزینه مطمئن محسوب می‌شود[۱۲].
- **امضای مرکل**: برای کاهش حجم کلید و افزایش مقیاس‌پذیری، از ساختار درخت مرکله استفاده می‌شود. در این روش، مجموعه‌ای از امضاهای لامپورت به‌صورت سلسله‌مراتبی سازماندهی شده و ریشه درخت به‌عنوان یک کلید عمومی عمل می‌کند. این روش کارآمدی بیشتری را در پیاده‌سازی امضاهای دیجیتال مقاوم در برابر کوانتوم فراهم می‌کند[۱۱].

این امضاها علاوه بر ارائه امنیت بالا، به دلیل سادگی محاسباتی، در سیستم‌های حساس و مبتنی بر داده‌های بزرگ مانند بلاکچین و اینترنت اشیا کاربرد گسترده‌ای دارند.

۴-۱ پروتکل‌های اثبات دانش صفر *

الگوریتم‌های مبتنی بر هش در پروتکل‌های اثبات دانش صفر نیز به‌طور گسترده استفاده می‌شوند. این پروتکل‌ها به کاربران اجازه می‌دهند تا بدون افشای داده‌های اصلی، صحت یک بیانیه را اثبات کنند. برای مثال، در یک تراکنش مالی، طرفین می‌توانند بدون افشای مبلغ تراکنش، تأیید کنند که تراکنش معتبر است.

در این پروتکل‌ها، توابع هش نقش اساسی در ایجاد تعهدات رمزنگارانه ایفا می‌کنند. تعهدات مبتنی بر هش، تضمین می‌کنند که داده‌ها در طول فرآیند تغییر نمی‌کنند[۱۰].

ویژگی مقاومت در برابر برخورد توابع هش، صحت و امنیت این پروتکل‌ها را تضمین می‌کند، چرا که طرفین نمی‌توانند با تغییر داده‌ها، هش مشابهی تولید کنند. پروتکل‌های اثبات دانش صفر مبتنی بر هش در برنامه‌های متنوعی از جمله حفاظت از حریم خصوصی، رأی‌گیری الکترونیکی، و هویت دیجیتال کاربرد دارند و نقش کلیدی در سیستم‌های امنیتی آینده ایفا می‌کنند[۱۲].

۵. نقاط قوت الگوریتم‌های مبتنی بر هش در برابر کامپیوترهای کوانتومی

الگوریتم‌های مبتنی بر هش به دلیل ویژگی‌های منحصر به فرد خود به‌عنوان یکی از پایدارترین گزینه‌ها برای مقابله با تهدیدات کوانتومی شناخته می‌شوند. در ادامه، سه ویژگی کلیدی این الگوریتم‌ها که آن‌ها را در برابر کامپیوترهای کوانتومی مقاوم می‌کند، مورد بررسی قرار می‌گیرد.

- **سادگی ساختار:** یکی از مهم‌ترین نقاط قوت الگوریتم‌های مبتنی بر هش، سادگی ساختار آن‌ها است. این الگوریتم‌ها به‌طور عمده به عملیات‌هایی مانند توابع فشرده‌سازی، ترکیب‌بندی، و محاسبات خطی وابسته هستند، که در مقایسه با سیستم‌های رمزنگاری کلید عمومی مانند RSA و ECC، پیچیدگی بسیار کمتری دارند. این سادگی به دو مزیت کلیدی منجر می‌شود:
  - امکان بررسی دقیق‌تر امنیت توابع هش توسط متخصصان رمزنگاری، چرا که تحلیل و آزمایش آن‌ها زمان و منابع کمتری نیاز دارد.
  - کاهش پیچیدگی حملات: ساختار ساده الگوریتم‌های مبتنی بر هش، احتمال کشف و بهره‌برداری از ضعف‌های ساختاری را به میزان قابل توجهی کاهش می‌دهد. از این رو، الگوریتم‌های مبتنی بر هش به دلیل طراحی ساده و مستقیم خود، برای دفاع در برابر حملات کوانتومی بهینه‌تر هستند.
- **استقلال از ریاضیات پیچیده:** الگوریتم‌های مبتنی بر هش برخلاف بسیاری از سیستم‌های رمزنگاری متداول مانند RSA یا ECC، به ساختارهای ریاضی پیچیده‌ای نظیر نظریه اعداد یا منحنی‌های بیضوی متکی نیستند. در حالی که کامپیوترهای کوانتومی می‌توانند این سیستم‌ها را با استفاده از الگوریتم شور به‌طور مؤثر رمزگشایی کنند، توابع هش به دلیل عدم استفاده از این ساختارها، در برابر حملات کوانتومی مصون‌تر هستند. این ویژگی همچنین باعث می‌شود که پیاده‌سازی و بهینه‌سازی توابع هش در سخت‌افزارها و نرم‌افزارها ساده‌تر باشد. علاوه بر این، عدم وابستگی به

* Zero-Knowledge Proofs

ریاضیات پیچیده، احتمال ظهور آسیب‌پذیری‌های پیش‌بینی‌نشده را کاهش می‌دهد و الگوریتم‌های مبتنی بر هش را به گزینه‌ای پایدار برای امنیت پسا کوانتومی تبدیل می‌کند.

- **مقیاس‌پذیری بالا:** مقیاس‌پذیری بالا یکی دیگر از نقاط قوت الگوریتم‌های مبتنی بر هش است. یکی از مهم‌ترین تهدیدات کوانتومی برای این الگوریتم‌ها، الگوریتم گروور است که باعث می‌شود فضای جستجوی توابع هش به‌صورت خطی کاهش یابد. با این حال، این تأثیر خطی است و نه نمایی، که به این معناست که امنیت الگوریتم با افزایش طول خروجی هش قابل حفظ و تقویت است.

برای مثال، اگر یک تابع هش ۲۵۶ بیتی توسط کامپیوتر کوانتومی با الگوریتم گروور مورد حمله قرار گیرد، سطح امنیت آن معادل ۱۲۸ بیت خواهد بود. افزایش طول خروجی به ۵۱۲ بیت، امنیت را به سطح ۲۵۶ بیت بازمی‌گرداند، که برای بسیاری از کاربردها، استانداردی بسیار قوی محسوب می‌شود. این امکان برای تنظیم طول هش به صورت دینامیک، الگوریتم‌های مبتنی بر هش را برای طراحی سیستم‌های امنیتی مقاوم در برابر تهدیدات آینده بسیار مناسب می‌کند.

الگوریتم‌های مبتنی بر هش با ترکیب ساختار ساده، عدم وابستگی به ریاضیات پیچیده و مقیاس‌پذیری بالا، ابزار قدرتمندی برای مقابله با تهدیدات کامپیوترهای کوانتومی ارائه می‌دهند. این ویژگی‌ها باعث می‌شوند که توابع هش در بسیاری از سیستم‌های امنیتی پسا کوانتومی از جمله بلاکچین، امضاهای دیجیتال، و پروتکل‌های اثبات دانش صفر، نقش حیاتی ایفا کنند[۱۰,۱۱,۱۲].

۵-۱ مقایسه الگوریتم‌های پسا کوانتومی

با ظهور کامپیوترهای کوانتومی، نیاز به الگوریتم‌های مقاوم در برابر حملات کوانتومی افزایش یافته است. الگوریتم‌های پسا کوانتومی با طراحی‌های مختلف برای مقابله با الگوریتم‌هایی مانند شور و گروور توسعه یافته‌اند. در این بخش، برخی از شناخته‌شده‌ترین خانواده‌های این الگوریتم‌هاکه شامل موارد ذیل می شوند را با هم مقایسه می نماییم.

- رمزنگاری‌های مبتنی بر مشبکه
- رمزنگاری‌های مبتنی بر کد
- رمزنگاری‌های مبتنی بر هش
- رمزنگاری‌های مبتنی بر چند متغیره

مبنای مقایسه شامل موارد زیر است:

امنیت: همه الگوریتم‌ها برای مقاومت در برابر حملات کوانتومی طراحی شده‌اند و امنیت آن‌ها بر سختی مسائل ریاضی خاص استوار است.

اندازه کلید: الگوریتم‌های مبتنی بر ایزومورفیسم و تابع هش معمولاً کلیدهای کوچک‌تری دارند، در حالی که الگوریتم‌های مبتنی بر کدگذاری کلیدهای بزرگ‌تری نیاز دارند.

کارایی: الگوریتم‌های مبتنی بر مشبکه های مشبکه و نظریه اعداد معمولاً سرعت بالایی دارند، اما نیازمند بهینه‌سازی برای کاهش پیچیدگی محاسباتی هستند.

کاربردها: این الگوریتم‌ها در حوزه‌های مختلفی از جمله رمزنگاری کلید عمومی، امضای دیجیتال، و رمزنگاری هممورفیک کاربرد دارند.

جدول۱. مقایسه انواع الگوریتم های رمزنگاری پساکوانتومی[۱۰, ۱۱, ۱۲, ۱۳]

الگوریتم	مبنای امنیتی	مزایا	معایب	اندازه کلید	کاربردها
مبتنی بر کدگذاری	مسائل کدهای تصحیح خطا (مانند McEliece)	امنیت قوی، ساختار ساده	اندازه کلید بسیار بزرگ	بزرگ (کیلوبایت تا مگابایت)	رمزنگاری کلید عمومی
مبتنی بر مشبکه های مشبکه	مسائل مشبکه های مشبکه (SVP, CVP)	امنیت بالا، اندازه کلید متوسط	پیچیدگی محاسباتی بالا	متوسط (کیلوبایت)	رمزنگاری هوموورفیک، امضای دیجیتال
مبتنی بر تابع هش	مقاومت در برابر معکوس‌سازی و برخورد هش	امنیت قوی، ساختار ساده	اندازه بزرگ امضا، محدودیت تعداد امضاها	کوچک (بایت‌ها)	امضای دیجیتال
مبتنی بر نظریه اعداد	سختی مسائل چندمتغیره غیرخطی	سرعت بالا، انعطاف‌پذیری	اندازه کلید بزرگ، آسیب‌پذیری در برابر حملات خاص	بزرگ (کیلوبایت)	امضای دیجیتال، رمزنگاری کلید عمومی
مبتنی بر ایزومورفیسم	سختی یافتن ایزومورفیسم بین منحنی‌های بیضوی	اندازه کلید کوچک، امنیت در برابر حملات کوانتومی	سرعت رمزگذاری/رمزگشایی پایین	کوچک (بایت‌ها)	تبادل کلید، رمزنگاری کلید عمومی
مبتنی بر منطق حلقوی	مسئله LWE در حوزه حلقوی	اندازه کلید کوچک، مناسب برای منابع محدود	پیچیدگی محاسباتی در رمزنگاری هوموورفیک	متوسط (کیلوبایت)	رمزنگاری هوموورفیک، تبادل کلید امن

۶. چالش‌ها و فرصت‌ها

ظهور الگوریتم‌های پسا کوانتومی برای مقابله با تهدیدات ناشی از کامپیوترهای کوانتومی، چالش‌ها و فرصت‌های متعددی را به همراه دارد. این الگوریتم‌ها با وجود ظرفیت بالای خود در ارائه امنیت، همچنان با موانع عملیاتی و تحقیقاتی مواجه‌اند که باید برطرف شوند. در عین حال، آن‌ها امکان ایجاد سیستم‌های ایمن‌تر و بهینه‌تر را فراهم می‌کنند که می‌تواند تأثیر قابل‌توجهی بر امنیت سایبری داشته باشد.

۶-۱ افزایش حجم کلید و پیام

یکی از مهم‌ترین چالش‌های الگوریتم‌های پسا کوانتومی، افزایش حجم کلید و پیام در بسیاری از این روش‌ها است. برای مثال، در رمزنگاری مبتنی بر کد و مشبکه ، کلیدهای عمومی و خصوصی بسیار بزرگ‌تر از الگوریتم‌های سنتی مانند RSA یا ECC هستند. این افزایش حجم، چالش‌هایی را در زمینه ذخیره‌سازی، انتقال، و پردازش داده‌ها ایجاد می‌کند و ممکن است کارایی سیستم‌های موجود را کاهش دهد. این مشکل به‌ویژه در دستگاه‌هایی با منابع محدود مانند اینترنت اشیا اهمیت بیشتری پیدا می‌کند[۱۴].

۶-۲ نیاز به استانداردسازی

نیاز به استانداردسازی یکی دیگر از چالش‌های مهم است. در حال حاضر، الگوریتم‌های متعددی در حوزه پسا کوانتوم پیشنهاد شده‌اند، اما هنوز استانداردهای جامعی برای انتخاب، پیاده‌سازی، و ارزیابی این الگوریتم‌ها وجود ندارد. فرایند استانداردسازی باید معیارهایی مانند امنیت، کارایی، و قابلیت پیاده‌سازی در مقیاس‌های بزرگ را در نظر بگیرد. تلاش‌هایی مانند پروژه استانداردسازی رمزنگاری پسا کوانتومی توسط NIST ، گام مهمی در این مسیر است، اما تکمیل این فرایند به زمان و تحقیقات بیشتری نیاز دارد.

۷. نتیجه‌گیری

در این مقاله به بررسی سیستم های رمزنگاری پساکوانتومی پرداختیم. انواع سیستم های رمزنگاری پساکوانتومی را معرفی کرده و به طور خاص تحلیلی از سیستم های رمزنگاری مبتنی بر توابع هش با جزئیات کامل بیان شد. در انتها مقایسه انواع الگوریتم های پساکوانتومی از چهار منظر امنیت، کارایی، اندازه کلید، کاربردها و معایب و مزایا آورده شد.

۸. مراجع

[۱]. Alvarado, M., Gayler, L., Seals, A., Wang, T., & Hou, T. (۲۰۲۳). A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges. arXiv preprint arXiv:۲۳۱۲.۱۰۴۳۰.

[۲]. Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K., & Hoang, T.-T. (۲۰۲۳). A Survey of Post-Quantum Cryptography: Start of a New Race. Cryptography, ۷(۳), ۴۰.

[۳]. Liu, T., Ramachandran, G., & Jurdak, R. (۲۰۲۴). Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. arXiv preprint arXiv:۲۴۰۱.۱۷۵۳۸.

[۴].Weger, V., Gassner, N., & Rosenthal, J. (۲۰۲۲). A Survey on Code-Based Cryptography. arXiv preprint arXiv:۲۲۰۱.۰۷۱۱۹.

[۵]. Debris-Alazard, T. (۲۰۲۳). Code-based Cryptography: Lecture Notes. arXiv preprint arXiv:۲۳۰۴.۰۳۵۴۱.

[۶]. Sendrier, N. (۲۰۱۷). Code-based Public-Key Cryptography. ECRYPT-CSA Executive School on Post-Quantum Cryptography.

[۷]. Tokareva, N. (۲۰۲۳). Post-Quantum Cryptosystems: Open Problems and Solutions. Lattice-Based Cryptography. Journal of Mathematical Sciences, ۲۴۸(۴), ۵۰۸–۵۲۰

[۸]. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (۲۰۱۶). Post-Quantum Key Exchange—A New Hope. In ۲۵th USENIX Security Symposium (pp. ۳۲۷–۳۴۳). USENIX Association.

[۹]. Peikert, C. (۲۰۱۴). Lattice Cryptography for the Internet. In Proceedings of the ۲۰۱۴ ACM SIGSAC Conference on Computer and Communications Security (pp. ۱۹۷–۲۰۶). ACM.

[۱۰]. Pereira, G., Puodzius, C., & Barreto, P. S. L. M. (۲۰۱۱). Shorter Hash-Based Signatures. Journal of Systems and Software, ۸۴(۱۱), ۱۹۸۳–۱۹۸۹.

[۱۱]. Garcia, L. (۲۰۰۵). On the Security and the Efficiency of the Merkle Signature Scheme. IACR Cryptology ePrint Archive, ۲۰۰۵, ۱۹۲.

[۱۲]. Naor, D., Shenhav, S., & Wool, A. (۲۰۰۸). One-Time Signatures Revisited: Practical Fast Signatures Using Fractal Merkle Tree Traversal. In IEEE Symposium on Security and Privacy (pp. ۱۱۰–۱۲۴). IEEE.

[۱۳]. Bulygin, S., Petzoldt, A., & Buchmann, J. (۲۰۱۰). Progress in Cryptology – INDOCRYPT ۲۰۱۰. In Lecture Notes in Computer Science (Vol. ۶۴۹۸, pp. ۱۳۳–۱۴۵). Springer.

[۱۴]. Petzoldt, A., Bulygin, S., & Buchmann, J. (۲۰۱۰). Selecting Parameters for the Rainbow Signature Scheme. IACR Cryptology ePrint Archive, ۲۰۱۰, ۴۳۷.

فیلتر U-Net Kalman (UNetKF):
نمونه ای از جذب داده های گروهی(Ensemble) به کمک یادگیری ماشین

سمیه راشکی [۱] ، انیسه ابراهیمی [۲]

۱- سمیه راشکی، دانشجوی دکتری دانشگاه تهران، s.rashki@uoz.ac.ir

۲- انیسه ابراهیمی، دانشجوی دانشکده فرخی سیستانی، anisehebrahimi9@gmail.com

چکیده

محبوبیت تکنیک های یادگیری ماشین شاهد افزایشی فوق العاده در علوم آب و هوا بوده است. جذب داده ها[۱] (DA) که مشاهدات و مدل های عددی را ترکیب می کند، پتانسیل زیادی برای ترکیب تکنیک های یادگیری ماشین و هوش مصنوعی (ML/AI) دارد. در این مقاله از U-Net که نوعی شبکه خنثی کانولوشنی[۲] (CNN) است، برای پیش بینی کوواریانس های گروهی محلی برای الگوریتم فیلتر کالمن جمعی[۳] (EnKF) استفاده شده است.

با استفاده از یک مدل شبه ژئواستروفی دو لایه[۴]، U-Nets با استفاده از داده های آزمایش های EnKF DA آموزش داده می شوند. سپس از شبکه‌های آموزش دیده برای پیش بینی ماتریس های کوواریانس خطای محلی وابسته به جریان در آزمایش های فیلتر کالمن U-Net (UNetKF) استفاده می شود که با روش های سنتی سه بعدی متغیر[۵] (3DVar)، 3DVar گروهی[۶] (En3DVar) و EnKF مقایسه می شود. عملکرد UNetKF می تواند با 3DVar، En3DVar یا EnKF مطابقت داشته باشد یا از آن فراتر رود. ما همچنین نشان می دهیم که U-Nets آموزش دیده را می توان به یک مدل با وضوح بالاتر برای پیاده سازی UNetKF منتقل کرد، که دوباره به صورت رقابتی به 3DVar و EnKF، به ویژه برای اندازه های گروه کوچک، عمل می کند.

کلمات کلیدی: الگوریتم فیلتر کالمن، جذب داده های گروهی، شبکه u

۱- مقدمه

تلفیق داده ها به طور گسترده در زمینه های علوم زمین،هواشناسی و علوم اقلیمی برای برآورد وضعیت فعلی و تاریخی اجزای سیستم زمین، فراهم کردن شرایط اولیه برای پیش بینی های عددی آب و هوا و اقلیم مورد استفاده قرار گرفته است. از زمان معرفی آن (Evensen, 1994)، فیلتر کالمن گروهی[۷] (EnKF) و انواع آن به طور گسترده ای در آب و هوا مورد استفاده قرار گرفت. (Anderson, 2001; Houtekamer & Mitchell, 1998; Hunt et al., 2007; S. Zhang et al., 2007;

[1] Data assimilation
[2] convolutional neutral network
[3] Ensemble Kalman Filter
[4] 2-layer quasigeostrophic model
[5] 3-dimensional variational
[6] ensemble 3DVar
[7] Ensemble Kalman Filter

Houtekamer & Zhang, 2016). فیلترهای کالمن مبتنی بر گروه با استفاده از مجموعه ای از شبیه سازی های مدل، روش های قبلی درون یابی بهینه[1] (OI) یا DA و متغیر سه بعدی (3DVar) برای تخمین آمار عدم قطعیت و خطای مدل وابسته به جریان بلادرنگ بهبود می بخشند. پذیرش گسترده فیلترهای کالمن مبتنی بر گروه با حداقل تغییرات آن در کد مدل موجود و انعطاف پذیری آن در پیاده سازی برای محاسبات موازی تسهیل می شود. (Anderson, 2003; S. Zhang et al., 2007; Anderson et al., 2009). یکی از منابع خطای مداوم برای فیلترهای کالمن مبتنی بر گروه، خطاهای نمونه برداری است که به دلیل اندازه های محدود گروه رخ می‌دهد. این خطا در مدل های دینامیکی گران قیمت محاسباتی، بیشتر دیده می‌شود. طرح های متعددی برای کاهش این موضوع در طول دهه ها پیشنهاد و اصلاح شده است، مانند روش های بومی سازی و تورم (F. Zhang et al., 2004; Buehner & Charron, 2007; Anderson, 2007, 2009). اگرچه نشان داده شده است که اندازه های گروهی متوسط به ترتیب ده ها می تواند منجر به برآورد موفقیت آمیز حالت در مدل های آب و هوایی جهانی شود (Lu et al., 2020; S.Zhang et al., 2007)، این محدودیت محاسباتی تنها زمانی بدتر می شود که پیچیدگی و وضوح مدل بیشتر شود.

در سال های اخیر، توسعه روش های هوش مصنوعی (AI) و یادگیری ماشین (ML) به پیشرفت بالقوه هیجان انگیز برای تحقیقات آب و هوا، به ویژه برای DA اشاره کرده است. هم افزایی بالقوه بین DA و ML باعث ایجاد طیف گسترده ای از مطالعات شده است که سعی در معرفی AI/ML به DA یا بالعکس دارند (Boukabara et al., 2021). برای جذب داده های مبتنی بر گروه به طور خاص، اکثر مطالعات تلاش کردند تا با استفاده از روش های ML برای ساخت یا گسترش گروه مدل، محدودیت اندازه گروه را کاهش دهند. به عنوان مثال، Grooms (۲۰۲۱) از رمزگذارهای خودکار متغیر (VAEs) برای تولید آنالوگ های مدل برای روش درون یابی بهینه گروهی (EnOI) استفاده کرد. پنی و همکاران (۲۰۲۲) استفاده از شبکه های عصبی بازگشتی (RNNs) را به عنوان مدل های جایگزین برای برآورد آمار خطای پیش بینی و دستیابی به برآورد وضعیت مبتنی بر داده خالص پیشنهاد کردند. پیشرفت سریع مدل‌های آب و هوا و اقلیم مبتنی بر ML به آینده‌ای هیجان‌انگیز اشاره می‌کند که در آن مجموعه‌های بسیار بزرگ را می‌توان به طور موثر برای همسان‌سازی داده‌های مجموعه با استفاده از این مدل‌های مبتنی بر داده تولید کرد (Bi et al., 2023; Kochkov et al., 2023; Lam et al., 2023). نمونه‌های دیگر برنامه‌های کاربردی ML مرتبط با DA عبارتند از Bonavita & Laloyaux (۲۰۲۰) و Farchi و همکاران (۲۰۲۱) که استفاده از روش‌های یادگیری ماشین را برای تخمین و تصحیح خطای مدل در سیستم‌های DA متغیر ۴ بعدی (4DVar) بررسی کردند. هاتفیلد و همکاران (۲۰۲۱) که توانایی شبیه سازهای شبکه عصبی (NN) را برای ارائه مدل های خطی مماس و الحاقی برای 4DVar ارزیابی کردند. چن و همکاران (۲۰۲۲) یک تکنیک تصحیح سوگیری مدل مشابه را با مدل پیش‌بینی NOAA به کار بردند و نشان دادند که می‌توان آن را به طور مکرر برای بهبود مهارت پیش‌بینی به کار برد.

در این مقاله، امکان استفاده از U-Net، یک کلاس از شبکه‌های عصبی کانولوشنال (CNN)، برای پیش‌بینی کوواریانس‌های خطای مجموعه برای EnKF را آزمایش می‌کنیم. ما این رویکرد را برای گروه DA به کمک ML، Ensemble U-Net Kalman Filter (UNetKF) می نامیم. اصول در این مقاله باید برای اجزای مدل سیستم زمین چندگانه قابل اجرا باشد.

۲- طراحی مدل و آزمایش

کد مود عددی مورد استفاده در این پژوهش، pyqg است که یک کتابخانه پایتون است که سیستم های شبه ژئواستروفیک[2] (QG) را با استفاده از روش های شبه طیفی مدل سازی می کند. از آن برای نمایش یک چارچوب منبع باز برای آموزش، آزمایش و ارزیابی پارامترسازی زیرشبکه مبتنی بر داده در یک مدل اقیانوس استفاده شده است (راس و همکاران، ۲۰۲۳). مدل های QG

[1] Optimal Interpolation
[2] quasigeostrophic

ساده سازی معقولی را برای مدل های گردش عمومی (GCM) ارائه می دهند. در این مطالعه از یک مدل دو لایه ایده آل از pyqg استفاده شده است. پارامترهای مدل شامل نسبت ضخامت لایه (بالا / پایین) delta = 0.05، سرعت منطقه ای لایه بالایی U1 = 0.025 (m/s)، سرعت منطقه ای لایه پایین U2 = 0.0 (m/s)، گرادیان گرداب سیاره ای (پارامتر کوریولیس) $\beta = 5 \times 10^{-12}$ $(m/s)^{-1}$، و ضریب پسا پایین $r_{ek} = 3.5 \times 10^{-8}$ $(m/s)^{-1}$ با توجه به نسبت ضخامت کوچک، تنوع مکانی و زمانی بین دو لایه متفاوت است، شبیه به یک لایه اختلاط اقیانوس فوقانی و یک لایه متوسط عمیق اقیانوس زیرسطحی.

ما مدل QG دو لایه را با دامنه مربع دو دوره ای ۱۰۰۰ کیلومتر پیکربندی می کنیم. از یک چارچوب مدل مغرضانه ایده آل استفاده می شود که در آن یک شبیه سازی ۵۰ ساله "اجرای طبیعت" یا "حقیقت" با یک شبکه ۱۲۸ × ۱۲۸ یا وضوح ~ ۷.۸ کیلومتر انجام می شود. "مشاهدات" از گرداب بالقوه از هر دو لایه هر ۱۰ روز یکبار از "حقیقت" در ۵۰ مکان تصادفی نمونه برداری می شود. فرکانس DA نیز برای همه آزمایش ها ۱۰ روز تنظیم شده است. شبکه مشاهده برای تقلید آزادانه شبکه‌های رصد دنیای واقعی طراحی شده است، که در آن مکان‌های مشاهدات معمولاً با زمان تغییر می‌کنند.

انحراف معیار خطاهای تصادفی "مشاهده" به ترتیب 10^{-5} و $5\times10^{-7} m^2 s^{-1}$ k kg^{-1} برای لایه های بالا و پایین است. این خطاها به طور دلخواه انتخاب می شوند تا در درجه اول با خطاهای نماینده مربوطه مطابقت داشته باشند، یعنی انحرافات استاندارد فضایی معمولی در یک دامنه کوچک در "حقیقت" با وضوح بالا که ممکن است فقط با یک نقطه شبکه در مدل پیش بینی با وضوح پایین نشان داده شود. چنین خطاهای نماینده زمانی بوجود می آیند که ما مشاهدات بسیار محلی در محل را در مکان های مدل شبکه ای جذب می کنیم که در آن هر نقطه شبکه میانگین منطقه خاصی را نشان می دهد. سایر گزینه های فراوانی جذب داده ها، فرکانس مشاهده، چگالی و خطا نیز در آزمایش های اضافی آزمایش می شوند و نتیجه گیری ها به طور قابل توجهی تغییر نمی کنند. دو نسخه دیگر از مدل QG دو لایه، از جمله QG-H(igh) با وضوح بالاتر با شبکه ۶۴ × ۶۴ و QG-L(ow) با وضوح پایین تر با شبکه ۳۲ × ۳۲، برای نمایش کلاس های مختلف "GCM" برای "دنیای واقعی" استفاده می شود. آزمایش های DA بر اساس جذر میانگین مربعات خطا (RMSE) گرداب بالقوه بین تجزیه و تحلیل مدل روزانه و "حقیقت" ارزیابی می شوند که به صورت خطی برای مطابقت با وضوح آزمایش های DA درون یابی می شود. اهمیت تفاوت در RMSE بین آزمایش های مختلف DA با استفاده از t-test استاندارد و سطح اطمینان ۹۵٪ آزمایش می شود، جایی که درجه آزادی (DOF) هر سری زمانی بر اساس مقیاس زمانی خودهمبستگی آن تنظیم می شود (Panofsky & Brier، ۱۹۶۸):

$$DOF = N\Delta t \,/\, 2T_e \qquad (۱)$$

N طول سری زمانی است. Δt فاصله زمانی است. T_e زمان واپاشی e-folding خودهمبستگی است، یعنی زمانی که ضریب خودهمبستگی سری زمانی به 1/e کاهش می یابد.

۳- روش‌های جذب داده‌ها

3Dvar برای چندین دهه یک روش DA محبوب بوده است (دربر و روزاتی، ۱۹۸۹؛ لورنک، ۱۹۸۶)، و هنوز هم توسط سیستم های تحلیل مجدد اقیانوس[1] عملیاتی استفاده می شود (واترز و همکاران، ۲۰۱۵؛ زو و همکاران، ۲۰۱۷). راه حل (تحلیل x^a) 3Dvar با به حداقل رساندن تابع هزینه به دست می آید (Lorenc, 1986)

$$\boldsymbol{\mathcal{J}(x)} = ½\,(\boldsymbol{x} - \boldsymbol{x}^{\,b})^{T}\,\boldsymbol{B}^{-1}\,(\boldsymbol{x} - \boldsymbol{x}^{\,b}) + ½\,(\boldsymbol{y}^{\,o} - \boldsymbol{H(x)})^{T}\boldsymbol{R}^{-1}\,(\boldsymbol{y}^{\,o} - \boldsymbol{H(x)}) \qquad (۲)$$

جایی که $\boldsymbol{y}^o$ مشاهدات، $\boldsymbol{x}^{\,b}$ پیش بینی مدل، $\boldsymbol{H}$ عملگر رصدی از مدل به فضای مشاهده ای، $\boldsymbol{R}$ ماتریس کوواریانس خطای مشاهده ای، و $\boldsymbol{B}$ پس زمینه اقلیم شناختی یا ماتریس کوواریانس قبلی است. برای بدست آوردن $\nabla_x \boldsymbol{\mathcal{J}(x^a)} = 0$، می توانیم به صورت افزایشی $\boldsymbol{x^a} = \boldsymbol{x^b} + \boldsymbol{\delta x}$، و بصورت خطی $\boldsymbol{H(x^a)} = \boldsymbol{H(x^b + \delta x)} \approx \boldsymbol{H(x^b)} + \boldsymbol{H(\delta x)}$ بنویسیم و دریافت کنیم:

[1] ocean reanalysis systems

$$\delta \boldsymbol{x} = (\boldsymbol{B}^{-1} + \boldsymbol{H}^{T}\boldsymbol{R}^{-1}\mathrm{H})^{-1}\boldsymbol{H}^{T}\boldsymbol{R}^{-1}(\boldsymbol{y}^{o} - \boldsymbol{H}(\boldsymbol{x}^{b})) \quad (۳)$$

یا معادل راه حل درونیابی بهینه

$$\delta \boldsymbol{x} = \boldsymbol{B}\boldsymbol{H}^{T}(\boldsymbol{R} + \boldsymbol{H}\boldsymbol{B}\boldsymbol{H}^{T})^{-1}(\boldsymbol{y}^{o} - \boldsymbol{H}(\boldsymbol{x}^{b})) \quad (۴)$$

پس‌زمینه یا کوواریانس قبلی $\boldsymbol{B}$ برای 3Dvar بر اساس شبیه‌سازی‌های کنترل جداگانه ۵۰۰ ساله به دنبال Parrish & Derber (۱۹۹۲) محاسبه می‌شود. پس از آزمایش طول‌های مختلف پیش‌بینی، کوواریانس‌های خطای پیش‌بینی ۶۰ روزه متوالی در طول ۵۰۰ سال به عنوان کوواریانس پس‌زمینه 3Dvar انتخاب می‌شوند. شکل ساختار کوواریانس به طور قابل توجهی در پنجره های پیش بینی مختلف تغییر نمی کند، در حالی که بزرگی با طول پنجره پیش بینی افزایش می یابد. نتایج مشابه 3Dvar را نیز می‌توان با تنظیم تجربی کوواریانس‌های پس‌زمینه از پنجره‌های پیش‌بینی کوتاه‌تر به‌دست آورد.

3Dvar گروهی (En3Dvar) برای دستیابی به عملکرد بهتر، میانگین مجموعه چندین تجزیه و تحلیل 3Dvar مستقل را می گیرد.

EnKF تقریبی از فیلتر کالمن است. از مجموعه ای از تحقق مدل برای انتشار و تخمین آمار خطای پیش بینی مدل استفاده می کند. در شکل سنتی خود با مشاهدات آشفته، EnKF همچنین می تواند به صورت افزایشی نوشته شود.

$$\delta \boldsymbol{x}i = \mathbf{K}(\boldsymbol{y}^{o} - \boldsymbol{y}_{i}{}^{b}),\ i = 1, \dots, N, \text{ where } \boldsymbol{y}_{i}{}^{b} = \boldsymbol{H}(\boldsymbol{x}_{i}{}^{b}) + \boldsymbol{\varepsilon}_{i} \quad (۵)$$

$$\mathbf{K} = \boldsymbol{B}_{ens}\boldsymbol{H}^{T}(\boldsymbol{R} + \boldsymbol{H}\boldsymbol{B}_{ens}\boldsymbol{H}\boldsymbol{T})^{-1} \quad (۶)$$

جایی که $\delta \boldsymbol{x}i$ افزایش DA، $\boldsymbol{K}$ افزایش کالمن، $\boldsymbol{y}o$ مشاهده، $\boldsymbol{x}i\boldsymbol{b}$ پیش بینی مدل، $\boldsymbol{\varepsilon}i$ اغتشاشات اضافه شده در پیش بینی مدل، $\boldsymbol{y}i\boldsymbol{b}$ مدل آشفته در فضای مشاهده پیش بینی می کند. و N اندازه گروه است و i تک تک اعضای گروه. $\boldsymbol{H}$ و $\boldsymbol{R}$ همان ماتریس هایی هستند که در بالا در 3Dvar توضیح داده شد و $\boldsymbol{B}ens$ کوواریانس خطای مدل است که از آشفتگی های پیش بینی مجموعه نسبت به میانگین پیش بینی مجموعه محاسبه می شود:

(۷)

برای پیاده سازی UNetKF، معادله EnKF (۴) و (۵) یکسان را در نظر می گیریم، اما کوواریانس خطای مدل مجموعه ای $\boldsymbol{B}ens$ را با کوواریانس پیش بینی شده U-Net در بهره کالمن جایگزین می کنیم.

(۸)

جایی که $\boldsymbol{B}_{UNet}$ توسط U-Net یا از پیش‌بینی مدل میانگین گروه $\boldsymbol{x}\bar{\boldsymbol{i}}^{\boldsymbol{b}} = 1/N \sum_{1}^{N} \boldsymbol{x}_{\boldsymbol{i}}{}^{b}$ زمانی که چندین عضو گروه استفاده می‌شود، یا از پیش‌بینی مدل $\boldsymbol{x}^{b}$ زمانی که UNetKF از یک عضو قطعی استفاده می‌کند، پیش‌بینی می‌شود. جزئیات U-Net از جمله معماری و آموزش آن در قسمت بعدی توضیح داده خواهد شد.

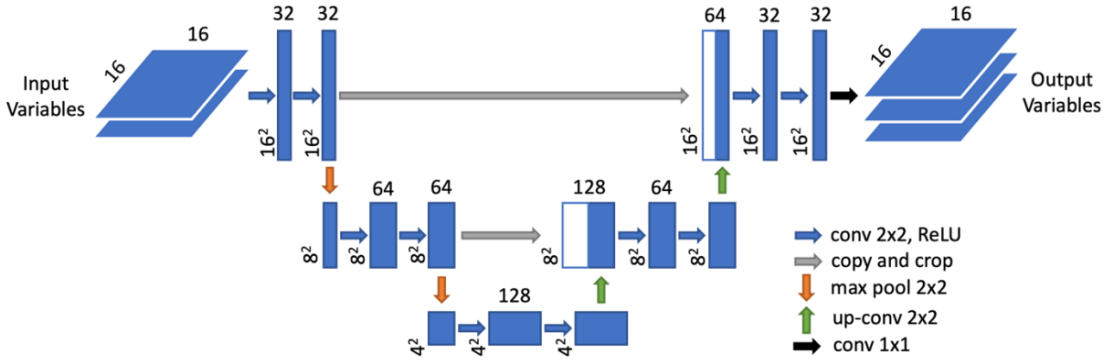
محلی سازی کوواریانس برای تمام روش های DA با استفاده از حاصل ضرب Schur ماتریس کوواریانس ($B/B_{ens}/B_{UNet}$) و یک ماتریس محلی سازی W با همان اندازه اعمال می شود، که در آن مقادیر بر اساس تابع Gaspari & Cohn (۱۹۹۹) و فاصله فیزیکی بین هر جفت از نقاط شبکه مدل محاسبه می شوند.

۴- شبکه U (U-Net)

۴-۱- معماری

شبکه عصبی کانولوشنال (CNN) دسته ای از شبکه های عصبی مصنوعی است که معمولاً برای تجزیه و تحلیل تصاویر استفاده می شود. توانایی شناسایی و استخراج ویژگی‌ها از تصاویر، CNN را برای کاربردهای خاص ژئوفیزیک مناسب می‌سازد. سی‌ان‌ان و انواع آن در پارامترسازی زیرشبکه و پیش‌بینی هوای یادگیری ماشین استفاده شده‌اند (Rasp & Thuerey, 2021؛

Weyn et al., 2020 ؛Sønderby et al., 2020). U-Net نوعی از CNN است که ابتدا برای تقسیم‌بندی تصویر زیست پزشکی استفاده شد (رونبرگر و همکاران، ۲۰۱۵)، و بعداً توسط سنجش از دور و تحقیقات سیستم اطلاعات جغرافیایی مورد استفاده قرار گرفت (جان و ژانگ، ۲۰۲۲؛ لاگرکوئیست و همکاران، ۲۰۲۱).). UNet نه تنها می تواند ویژگی ها را از یک تصویر استخراج کند، بلکه می تواند چنین ویژگی هایی را به اندازه تصویر اصلی برای اهداف تقسیم بندی یا طبقه بندی بازگرداند. یکی دیگر از پیشرفت‌های کلیدی UNet، اتصالات پرش بین لایه‌های با ابعاد بالاتر (فلش‌های خاکستری در شکل ۱) است که به شبکه کمک می‌کند تا قبل از کاهش ابعاد بیشتر، ویژگی‌های با وضوح بالاتر را از داده‌های ورودی بیاموزد. یک نمایش شماتیک از معماری U-Net را می توان در Ronneberger و همکاران (۲۰۱۵) یافت و با پارامترهای به روز شده برای این مطالعه در شکل ۱ بازتولید شده است. مدل های U-Net را می توان با استفاده از کتابخانه های یادگیری عمیق موجود ساخت، برای این مطالعه از PyTorch استفاده کردیم.



شکل ۱. معماری U-Net با ابعاد و نمادها به دنبال Ronneberger و همکاران (۲۰۱۵). این مثال با داده‌های آموزشی آزمایش‌های QG-L DA مطابقت دارد، که در آن متغیرهای ورودی (16×16×2) و خروجی (16×16×3) به‌ترتیب ماتریس‌های گردابه پتانسیل موضعی و ماتریس‌های کوواریانس مجموعه موضعی هستند.

مسیر انقباض U-Net (سمت چپ شکل ۱) از سه کاربرد کانولوشن دوگانه ۲×۲ تشکیل شده است. هر کانولوشن (فلش آبی) برای حفظ اندازه یکسان بین تصاویر ورودی و خروجی و شامل یک واحد خطی اصلاح شده (ReLU) است. دو پیچ دوگانه اول با عملیات جمع آوری حداکثر ۲×۲ (فلش نارنجی) با گام ۲ برای نمونه برداری پایین دنبال می شوند. هر مرحله در مسیر گسترده (سمت راست شکل ۱) متشکل از یک پیچ ۲×۲ رو به بالا (فلش سبز) برای نمونه برداری، یک الحاق با نقشه ویژگی با وضوح بالا مربوطه از مسیر انقباض (فلش خاکستری)، و دوبل کانولوشن ۲×۲ و ReLU (فلش آبی) است. کانولوشن نهایی ۱×۱ (فلش سیاه) با تعداد کانال های موجود در تصاویر خروجی مطابقت دارد. در این مقاله، به‌جای بررسی فراپارامترهای جامع‌تر، بر روی ۲ پارامتر اصلی در این معماری U-Net، تعداد مراحل پایین‌نمونه‌سازی و تعداد ویژگی‌ها پس از اولین کانولوشن تمرکز خواهیم کرد. که اغلب به ترتیب به عنوان عمق و عرض U-Net نامیده می شوند. U-Net پیش فرض همانطور که در شکل ۱ نشان داده شده است، دارای ۲ مرحله نمونه برداری پایین و ۳۲ ویژگی پس از اولین کانولوشن است.

۲-۴- روش‌ها و داده‌ها

آزمایش‌های EnKF با طول‌های مختلف در QG-L و QG-H برای تولید داده‌های آموزشی برای U-Net انجام می‌شوند. این آزمایش‌ها جدا از آزمایش‌هایی هستند که در بخش ۲ توضیح داده شد، اما از همان تنظیمات پیروی می‌کنند. مزیت اصلی EnKF نسبت به 3DVar استفاده از کوواریانس های خطای پیش بینی وابسته به جریان است که بر اساس مجموعه ای از شبیه سازی

های مدل آشفته تخمین زده می شود. بنابراین، ما پیش‌بینی می‌کنیم که حالت مدل پس‌زمینه (جریان)، حتی بدون آمار آشفتگی مجموعه صـــریح، می‌تواند اطلاعات مرتبطی در مورد کوواریانس‌های خطای پیش‌بینی کوتاه‌مدت ارائه دهد که در طول زمان تغییر می‌کنند.

ماتریس های کوواریانس جمعی-میانگین پیش بینی شـــده مدل (ورودی برای U-Net) و ماتریس های کوواریانس گروهی محلی (خروجی برای U-Net) در هر مرحله DA برای آموزش ذخیره می شـوند. حتی برای مدل های دینامیکی سـاده مانند مدل QG مورد اســتفاده در این مطالعه، ذخیره ماتریس های کوواریانس کامل برای هر نقطه شـــبکه مدل در هر مرحله DA ممنوع اســت. خوشـبختانه، به دلیل اسـتفاده از طرح های محلی سـازی در اکثر سـیسـتم های DA گروهی، ما فقط باید ماتریس های کوواریانس محلی را ذخیره کنیم که به اندازه کافی بزرگ هســتند تا شــعاع محلی ســازی مورد نظر را پوشــش دهند. به دنبال ماتریس های کوواریانس محلی شده، گرداب پتانسیل پیش بینی میانگین مدل نیز در اطراف هر نقطه شبکه مدل قرار می گیرد تا به عنوان داده های آموزشــی عمل کند. همچنین می توان تمام اختلالات گروه را ذخیره کرد و کوواریانس ها را در طول فرآیند آموزش محاســبه کرد. کارایی نسبی بین ذخیره سازی ماتریس های کوواریانس موضعی یا آشفتگی‌های گروهی وابسته به مورد خواهد بود.

در یک آزمایش EnKF با (QG-H) QG-L، ۱۰۲۴ (۴۰۹۶) نمونه آموزشـــی جفتی از هر مرحله DA وجود دارد، که در آن هر مکان مدل، ۱ نمونه جفتی از گردابه پتانسیل موضعی و ماتریس کوواریانس گروهی موضعی را ارائه می دهد. نمونه های داده ها به نمونه های آموزشـی و نمونه های اعتبار سـنجی تقسـیم می شـوند که به ترتیب ۸۰ و ۲۰ درصـد داده ها هسـتند. برای داده های آموزشی از QG-L (شکل ۱)، هر نمونه ورودی دارای شکل 16×16×2 است که از ۲ لایه مدل گردابه پتانسیل موضعی در اطراف یک نقطه مرجع مرکزی تشکیل شده است، و هر نمونه خروجی دارای شکل 16×16×3 است که از ۳ ماتریس کوواریانس موضعی تشکیل شده است. که حاوی کوواریانس بین هر نقطه شبکه و همان نقطه مرجع مرکزی است. ۳ ماتریس کوواریانس لایه های مدل ۱ و ۲ به صورت جداگانه و همچنین کوواریانس متقاطع بین لایه های مدل ۱ و ۲ هستند. [۱]

آزمایش‌های EnKF که داده‌های آموزشـــی را ارائه می‌کنند در جدول ۱ فهرســـت شـــده‌اند. آزمایش گروه بزرگ ۱۲۸۰ عضـــوی DATA_L1280 با QG-L می‌تواند خطای نمونه‌گیری را برای ارائه بهترین داده‌های آموزشی ممکن به حداقل برساند. در حالی که DATA_L20 و DATA_L80 واقع بینانه تر برای آزمایش استحکام U-Net آموزش دیده با داده های پر سر و صدا بیشتر اســـتفاده می شـــوند، و همچنین بیشـــتر نماینده لندازه های گروه در دنیای واقعی هســـتند. به طور خاص، DATA_L20 (و DATA_H20) تنها ۲ ســال فرصــت دارد تا آموزش U-Net را با اندازه گروه کوچک و در دســترس بودن داده محدود آزمایش کند. شعاع محلی سازی و ضریب آرامش آزمایشات تمرینی به تنظیم گسترده نیاز ندارند، تا زمانی که پخش گروهی معقول را حفظ کنند. ما پارامترهای مختلف DA را برای آزمایش‌های آموزشـــی آزمایش کردیم که منجر به U-Netهای آموزش‌دیده مشـــابه می‌شود. U-Net ها همچنین با داده های آموزشی از آزمایش های EnKF در QG-H برای مقایسه با U-Net های انتقال یافته در آزمایش های UNetKF در QG-H آموزش دیده اند. کاربرد U-Nets فهرست شده در جدول ۱ در آزمایشات UNetKF در بخش ۵ به تفصیل توضیح داده خواهد شد.

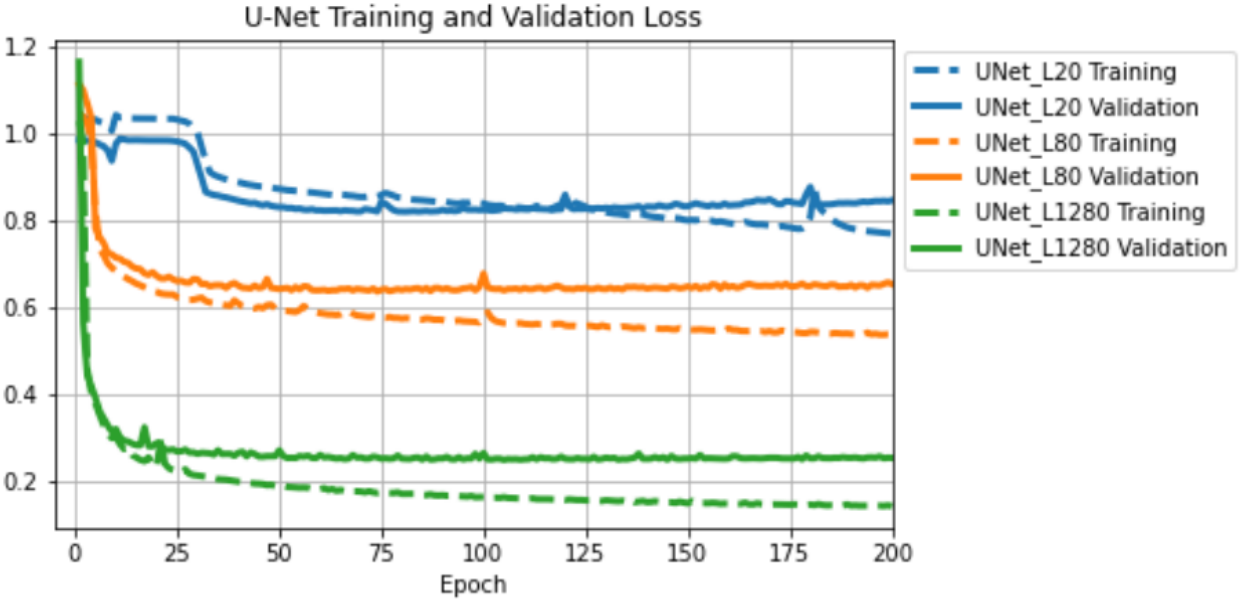
جدول ۱. لیست آزمایش های DA که داده های آموزشی را ارائه می دهند.

	Numerical model for DA	Data length	Ensemble size	Localizationradius	Relaxation factor	Trained U-Net
DATA_L20	QG-L	2 years	20	100 km	0.6	UNet_L20
DATA_L80	QG_L		80	100 km	0.5	UNet_L80
DATA_L1280	QG-L		1280	100 km	0.45	UNet_L1280
DATA_H20	QG_H	9 years	20	100 km	0.6	UNet_H20
	QG-H		80	100 km	0.45	

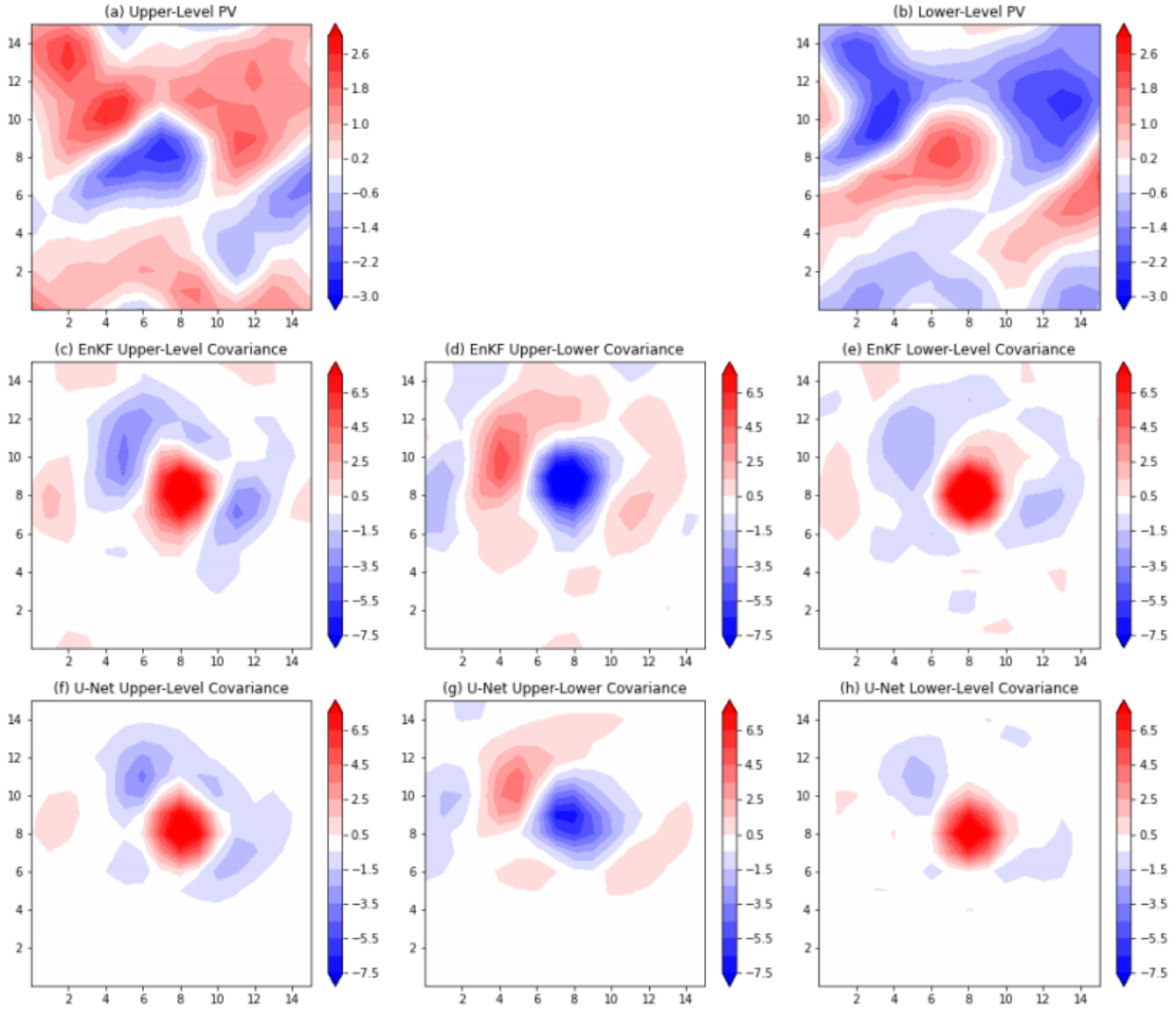
DATA_H80		9 years 2 years 9 years				UNet_H80

۳-۴- آموزش و ارزیابی U-Net

آموزش U-Net از اندازه های دسته ای از ۸۰۰۰ تا ۳۲۰۰۰ بسته به حافظه گرافیکی موجود، نرخ یادگیری ۰.۰۰۲، تابع هزینه ریشه میانگین مربعات خطا (RMSE) و بهینه ساز گرادیان تصادفی PyTorch Adam استفاده می کند. انتخاب پارامترهای آموزشی از حوصله این مقاله خارج است. شکل ۲ تلفات آموزشی و اعتبارسنجی را در ۲۰۰ دوره آموزشی برای UNet_L20، UNet_L80 و UNet_L1280 نشان می دهد. اگر چه تلفات آموزش به طور کلی با ادامه آموزش کاهش می یابد، افت اعتبار سنجی راکد می شود، یا حتی پس از تعداد معینی از دوره ها افزایش می یابد. آموزش معمولاً زمانی متوقف می شود که کاهش اعتبار سنجی متوقف شود تا از تطبیق بیش از حد با داده های آموزشی جلوگیری شود. حداقل خطای اعتبارسنجی در دوره ۸۱ برای UNet_L20، دوره ۷۴ برای UNet_L80، و دوره ۱۰۵ برای UNet_L1280 رخ می دهد. ما U-Nets را در دوره‌هایی با حداقل خطاهای اعتبارسنجی انتخاب می‌کنیم تا در آزمایش‌های بعدی UNetKF مورد استفاده قرار گیرند.



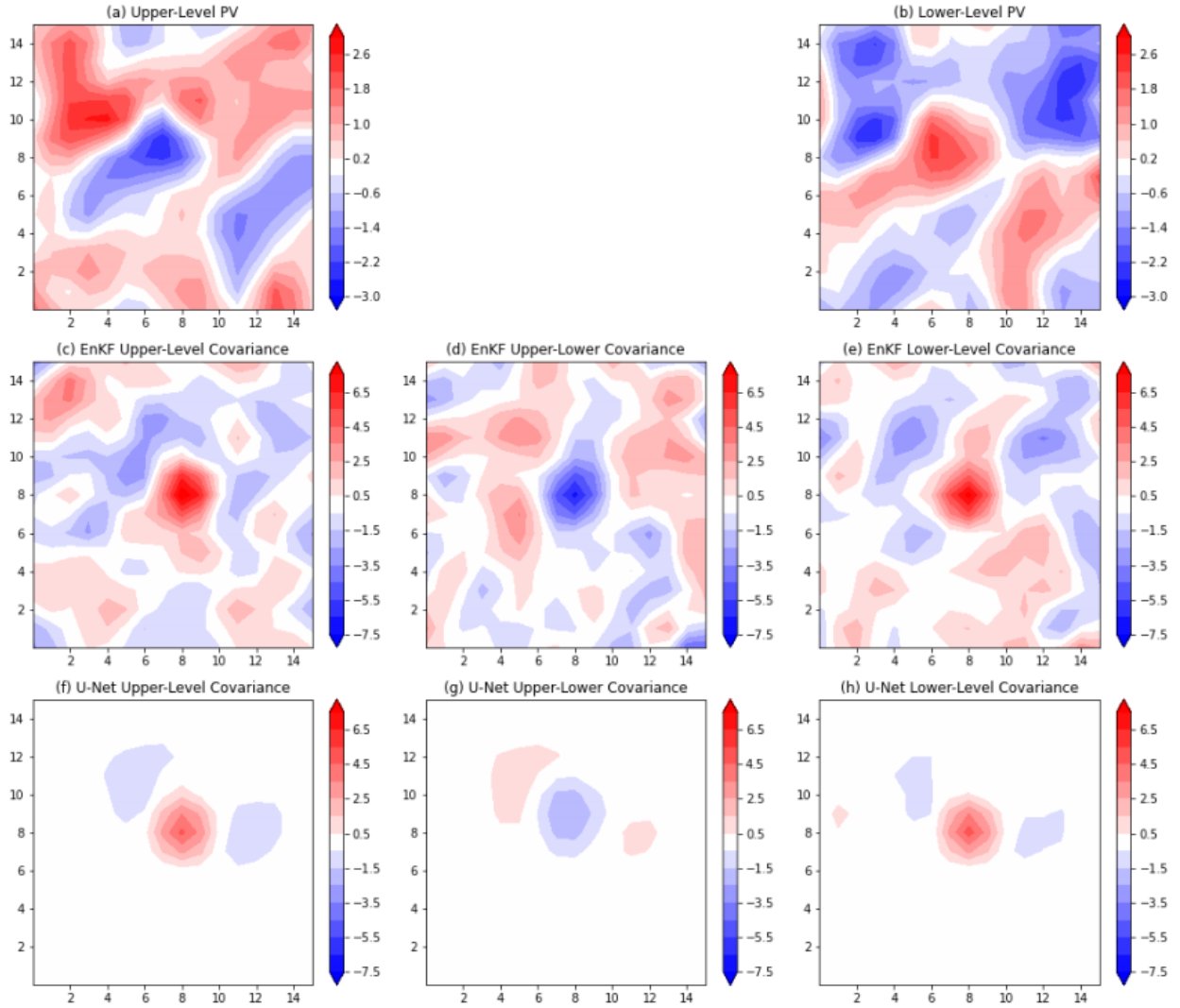
شکل ۲. تلفات آموزشی و اعتبارسنجی در طول آموزش UNet_L1 و UNet_L2.



شکل ۳. مثالی از UNet_L1280 برای یک نمونه داده اعتبارسنجی. (a و b) گردابه پتانسیل سطح بالا و پایین به ترتیب. (c-e) کوواریانس های گروه EnKF به ترتیب در سطح بالا، بین سطوح بالا و پایین و در سطح پایین تر. (f-h) کوواریانس‌های پیش‌بینی‌شده توسط UNet_L1 که به ترتیب (a) و (b) به عنوان ورودی‌ها مربوط به (c-e) هستند.

قابل توجه است که با افزایش اندازه گروه در داده های آموزشی از DATA_L20 به DATA_L1280، خطاهای آموزشی و اعتبارسنجی کاهش می یابد. دلیل اصلی این است که داده های آموزشی DATA_L1280، به ویژه کوواریانس های گروهی، "نویز" کمتری نسبت به داده های DATA_L20 دارند. "نویز" به خطاهای نمونه برداری جعلی بزرگتر هنگام محاسبه کوواریانس های گروه بر اساس یک گروه کوچکتر در DATA_L20 نسبت به DATA_L1280 اشاره دارد. شکل ۳ و شکل ۴ به ترتیب یک مثال در میان نمونه های داده های اعتبارسنجی برای UNet_L1280 و UNet_L20 نشان می دهد. نمونه شامل گرداب پتانسیل میانگین گروهی محلی برای هر دو سطح (پانل بالا)، کوواریانس های گروه EnKF محلی (پانل میانی) برآورد شده بر اساس آشفتگی‌های گروهی و کوواریانس های محلی پیش بینی شده U-Net (پانل پایین) با استفاده از پانل بالایی به عنوان ورودی است. گرداب های بالقوه در شکل a-b۳ و شکل a-b۴ مشابه به نظر می رسند زیرا آنها تجزیه و تحلیل میانگین گروهی در

اطراف یک نقطه شبکه مدل به طور همزمان هستند. اگرچه کوواریانس های اطراف نقطه شبکه مرجع مرکزی الگوهای مشابهی را نشان می دهند (شکل c-e۳ و شکل c-e۴)، کوواریانس های گروهی از DATA_L20 (شکل c-e۴) دارای مقادیر غیر صفر بزرگتر بین نقاط شبکه مرکزی و محیطی هستند، یعنی مکان های مدل که از نظر فیزیکی از یکدیگر دور هستند و انتظار هیچ تغییرپذیری همبسته ای در یک مرحله DA را نداریم. در حالی که DATA_L1280 (شکل c-e۳) با توجه به اندازه گروه بسیار بزرگتر خود می تواند مقادیر کوواریانس صفر یا نزدیک به صفر را با دقت بیشتری تخمین بزند. کوواریانس های گروهی نزدیک به نقطه شبکه مرکزی نیز در DATA_L1280 بزرگتر از DATA_L20 هستند. بنابراین، در طول آموزش، داده های خروجی کوواریانس با وفاداری بالاتر را برای UNet_L1280 برای یادگیری ارائه DATA_L1280، در حالی که داده های ورودی بین UNet_L1280 و UNet_20 مشابه است. متعاقباً، در طول اعتبارسنجی، "نویز" در نمونه های اعتبارسنجی DATA_L20 نمی تواند و نباید توسط U-Net پیش بینی شود، که منجر به خطاهای اعتبارسنجی بزرگتر برای UNet_L20 می شود. با این حال، از آنجایی که این کوواریانس های جعلی ناشی از خطاهای نمونه برداری هستند و به طور تصادفی در طول زمان تغییر می کنند، UNet_L20 قادر به فیلتر کردن این نویز تصادفی است و پیش بینی هایی را انجام می دهد (شکل f-h۴) که شبیه به نویز UNet_L1280 است (شکل f-h۳) با وجود نویز بزرگتر در داده های آموزشی خود، البته با مقادیر کوچکتر که با مقادیر کوچکتر در DATA_L20 در مقایسه با DATA_L1280 مطابقت دارد. اگرچه ماتریس‌های کوواریانس موضعی در داده‌های آموزشی تحت وزن‌های محلی‌سازی گاسپاری-کوهن نیستند. خود شبکه های U-Net های آموزش دیده می توانند با فیلتر کردن کوواریانس های جعلی در داده های آموزشی و پیش بینی کوواریانس های خطای وابسته به جریان نزدیک به هر نقطه شبکه مدل، به عنوان طرح های محلی سازی عمل کنند. این معادل U-Net محلی سازی نیز ذاتا "سازگار" است زیرا کوواریانس های پیش بینی شده مشروط به وضعیت مدل پس زمینه هستند. [2]



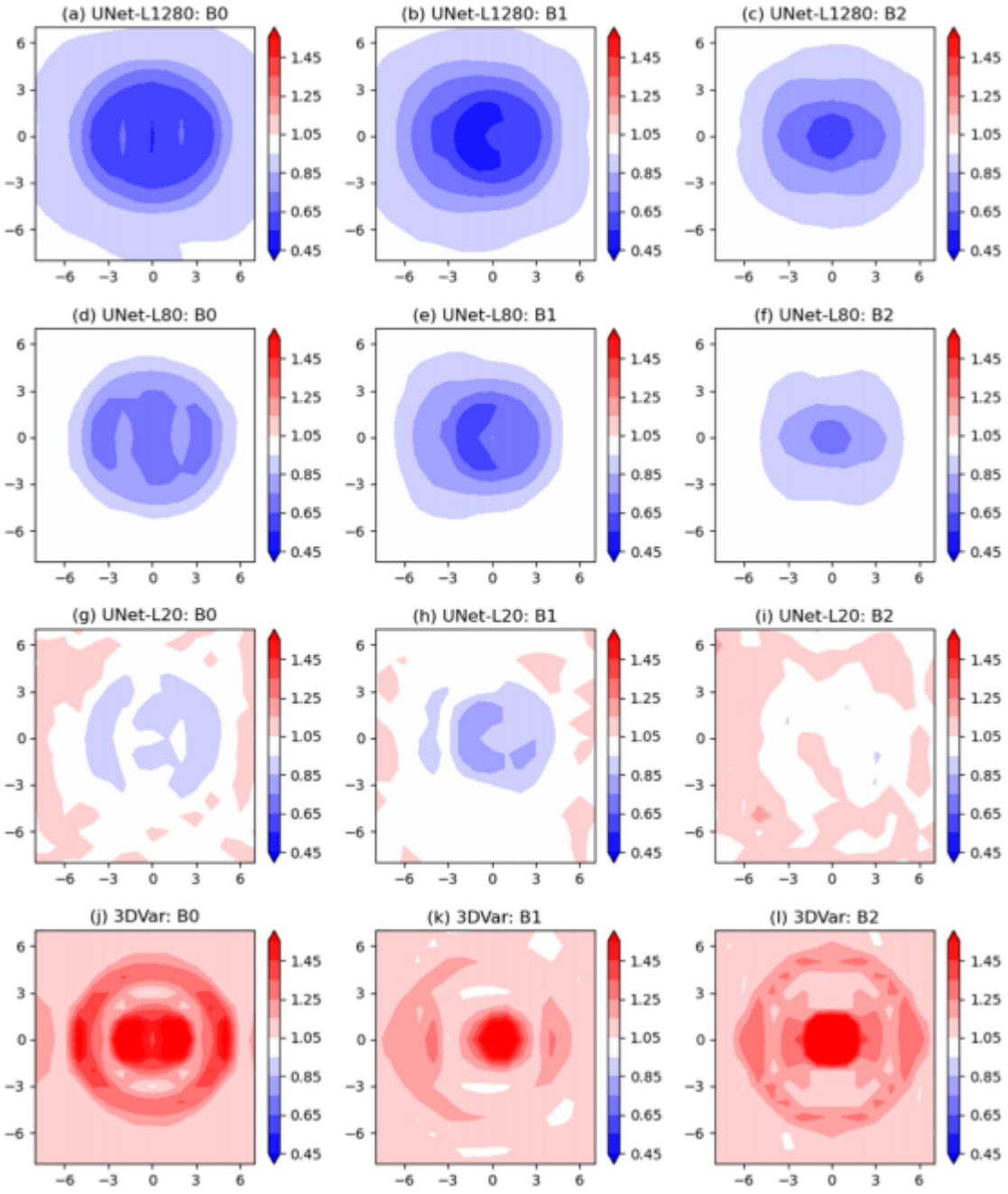
شکل ۴. مانند شکل ۳، اما برای UNet_L20

برای ارزیابی مهارت های U-Nets در تمام نقاط شبکه مدل و مراحل جذب داده ها، UNet_L1280، UNet_L80 و UNet_L20 را به مجموعه داده های DATA_L1280 کامل اعمال کردیم. در اینجا، ما کوواریانس های تخمینی ۱۲۸۰ عضوی را به عنوان "کوواریانس های واقعی" در نظر می گیریم. و شکل ۵ میانگین تغییرات RMSE را در برابر "کوواریانس های واقعی" متغیر با زمان در تمام نقاط شبکه مدل نشان می دهد، زمانی که کوواریانس های پیش بینی شده توسط U-Net به جای "کوواریانس واقعی" اقلیم شناسی میانگین زمانی استفاده می شود.

به عبارت دیگر، هر مقدار زیر ۱.۰ در شکل ۵ به این معنی است که پیش بینی های U-Net کوواریانس های مفیدتری نسبت به "کوواریانس واقعی" اقلیمی ارائه می دهند. همانطور که انتظار می رود، UNet_L1280 (شکل ۵a-c) بیشترین کاهش را در RMSE ارائه می دهد و پس از آن UNet_L80 قرار دارد (شکل ۵d-f). UNet_L20 (شکل ۵g-i) قادر است "کوواریانس واقعی" اقلیمی را در فواصل محلی سازی معینی برای لایه اول و بین لایه های اول و دوم شکست دهد، اما نه برای لایه دوم. این را می توان به افزایش خطاهای نمونه گیری در داده های آموزشی DATA_L20 به دلیل اندازه گروه محدود و طول آزمایش کوتاه تر نسبت داد. اگرچه کاهش RMSE برای UNet_L20 اندک است، اما باید توجه داشت که "کوواریانس های واقعی" از آزمایش

DA 1280 عضوی خود تخمین های خوبی از عدم قطعیت مدل هستند و برای سیستم های DA معمولی در دسترس نیستند. کوواریانس خطای ایستا 3DVar منجر به افزایش RMSE نسبت به «کوواریانس های حقیقی» اقلیمی برای اکثر حوزه های محلی شده می شود، زیرا کوواریانس های ایستا به روش متفاوتی محاسبه می شوند که منجر به بزرگی کوواریانس و الگوهای متفاوتی می شود.

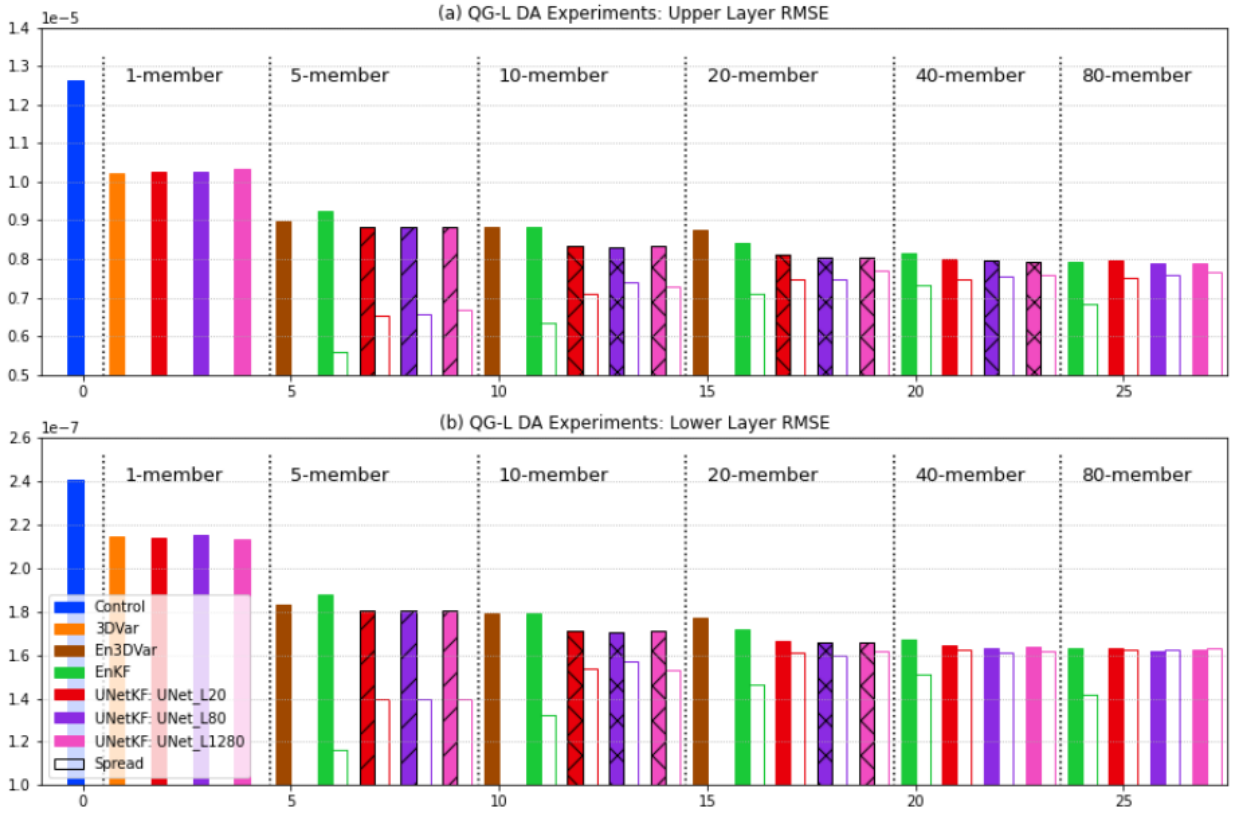
تأثیر فراپارامترهای عمق و عرض U-Net نیز مورد آزمایش قرار گرفته است. عمق یا عرض زیاد ممکن است به طور بالقوه مهارت U-Net را بهبود بخشد، اما به قیمت هزینه های محاسباتی بیشتر برای آموزش و استنتاج، و همچنین خطر بالاتر برازش بیش از حد. مسئله بیش از حد برازش زمانی بوجود می آید که شبکه عصبی بیش از حد آموزش داده می شود تا اطلاعات "پر نویز" با فرکانس بالا یا مقیاس کوچک را از داده های آموزشی متناسب کند، که ممکن است به مهارت پیش بینی آن در خارج از نمونه های آموزشی کمک نکند. این مشکل معمولاً در طول آموزش به صورت از دست دادن اعتبار راکد یا فزاینده خود را نشان می دهد، حتی زمانی که از دست دادن آموزش مدام کاهش می یابد. شبکه های عصبی بزرگتر می توانند بیشتر مستعد برازش بیش از حد باشند زیرا پارامترهای بیشتری برای متناسب با "نویز" در نمونه های آموزشی وجود دارد. همه ترکیبات را بین عرض های ۱۶، ۳۲ یا ۶۴ و عمق ۲ یا ۳ (نشان داده نشده) آزمایش کردیم. اگرچه زمانی که U-Net گسترده تر یا عمیق تر است، از دست دادن آموزش به طور کلی کاهش می یابد، حداقل از دست دادن اعتبارسنجی همیشه به دنبال آن نیست و شکاف بین تلفات آموزش و اعتبارسنجی معمولا افزایش می یابد، که نشان می دهد U-Net گسترده تر یا عمیق تر ممکن است بیش از حد به نمونه های آموزشی برازش شده باشد و مهارت های پیش بینی کمتری در خارج از نمونه های آموزشی داشته باشد. U-Net پیش فرض با عمق ۲ و عرض ۳۲ کمترین خطای اعتبارسنجی را به همراه دارد.



شکل ۵. دقت برآوردهای کوواریانس خطای محلی از UNet_L20 (a-c)، UNet_L80 (df)، UNet_L1280 (g-i) و (j- 3DVar (l در تمام نقاط شبکه مدل در QG-L. مقادیر موجود در نمودارها نشان دهنده نسبت RMSE است که از خطاها در برابر کوواریانس های خطای متغیر با زمان DATA_L1280، بین برآوردهای U-Net/3DVar و ماتریس های کوواریانس اقلیمی خود DATA_L1280 محاسبه می شود.

۵- نتایج UNetKF

عملکرد UNetKF ابتدا با 3DVar، En3DVar و EnKF در یک سری آزمایش های DA با استفاده از QG-L به عنوان مدل پیش بینی مقایسه می شود. نتایج آزمایش ها در شکل ۶ نشان داده شده است، در حالی که جزئیات بیشتر در مورد آزمایش ها در جدول S1 ذکر شده است. شعاع مکان یابی و پارامتر آرام سازی برای کمینه کردن RMSE هر آزمایش انتخاب شده است. U-Nets مورد استفاده در اینجا UNet_L20، UNet_L80 و UNet_L1280 هستند که با داده های همان مدل QG-L آموزش داده شده اند. رنگ میله ها نشان دهنده روش (3DVar, En3DVar, EnKF, UNetKF) یا U-Net خاصی است که توسط UNetKF استفاده می شود. اندازه های گروه در شکل ۶ به آزمایش های DA در اینجا اشاره دارد و به اندازه گروه داده های آموزشی U-Net مربوط نمی شود. هر U-Net، صرف نظر از اندازه گروه داده های آموزشی آن (به عنوان مثال ۲۰ برای UNet_L20، ۸۰ برای UNet_L80)، در آزمایش های UNetKF با اندازه های مختلف گروه از ۱ تا ۸۰ استفاده می شود. RMSE میانگین گروهی و انحراف معیار گروهی (گسترش) برای هر دو لایه مدل در شکل ۶ برای تمام آزمایش های QG-L در صورت موجود بودن نشان داده شده است. از آنجایی که عملکرد نسبی در میان آزمایش های مختلف DA در بیشتر موارد برای هر دو لایه صادق است، ما هنگام بحث در مورد نتایج در این بخش، دو لایه را از هم متمایز نمی کنیم، مگر اینکه خلاف آن مشخص شود.[3]



شکل ۶. تجزیه و تحلیل RMSE و گسترش مجموعه (در صورت وجود) از (a) گردابه بالقوه سطح بالا و (b) سطح پایین تر برای آزمایش های کنترل و DA در مدل QG-L. میله های پر و پر نشده به ترتیب RMSE و spread را نشان می دهند. اندازه‌های گروه در نمودار برای هر گروه از آزمایش‌های 3DVar، En3DVar، EnKF و UNetKF فهرست شده‌اند. میله‌های دریچه‌دار متقاطع نشان می‌دهند که RMSE UNetKF به طور قابل‌توجهی کوچک‌تر از EnKF و En3DVar برای همان اندازه

مجموعه است، در حالی که میله‌های دریچه‌دار مورب نشان می‌دهند که RMSE UNetKF به طور قابل‌توجهی کوچکتر از EnKF است.

هنگامی‌که در آزمایش های UNetKF اجرا می شـــود، UNet_L20، UNet_L80 و UNet_L1280 با وجود شـــکاف در آموزش و خطاهای اعتبارســنجی که قبلا مورد بحث قرار گرفت، منجر به عملکرد مشـابهی در اندازه های مختلف گروه می شـوند. UNetKF با UNet_L20 کمی بدتر از UNetKF با UNet_L80 یا UNet_L1280 عمل می کند، اما تفاوت ها برای هیچ اندازه خاصـی از گروه معنی دار نیسـت. این بدان معنی اسـت که UNet_L20 می تواند با موفقیت "نویز" موجود در داده های آموزشـی را از DATA_L20 فیلتر کند. این برای کاربردهای آینده UNetKF امیدوار کننده است، زیرا ما می توانیم U-Net را با داده های کوواریانس بر اساس اندازه‌های گروهی متوسط که برای مدل های دینامیکی گران‌تر از نظر محاسباتی کاربردی هستند، آموزش دهیم. بین En3DVar و EnKF، En3DVar با ۵ عضـو از EnKF بهتر عمل می کند، اما EnKF با ۱۰ عضـو به عقب می رسد و با بیش از ۱۰ عضو از En3DVar بهتر عمل می کند.

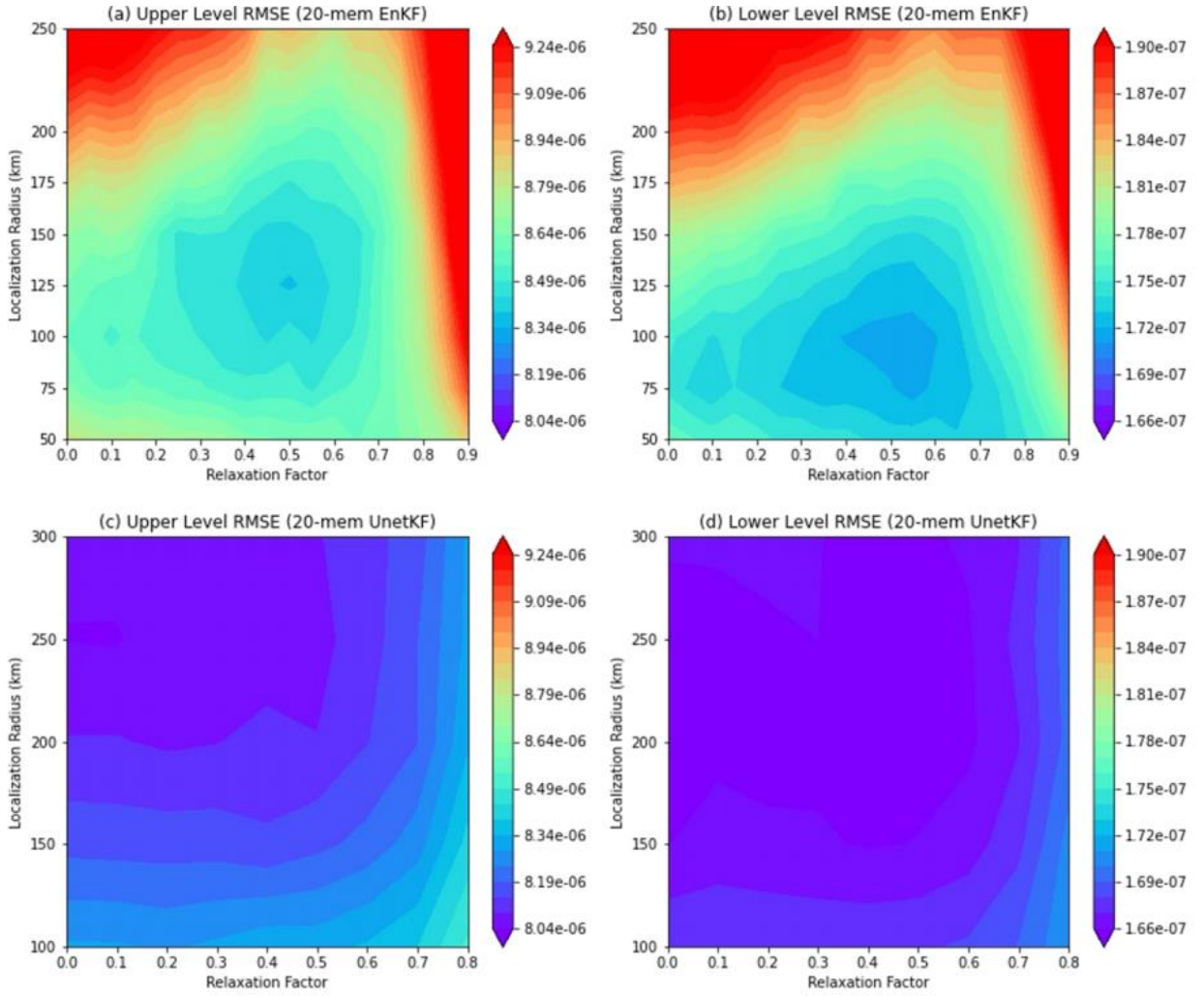
با یک عضو، آزمایش های UNetKF RMSE مشابهی با 3DVar دارند، جایی که تفاوت بین 3DVar و هر آزمایش UNetKF قابل توجه نیسـت. با ۵ عضـو، آزمایش های UNetKF به طور قابل توجهی بهتر از EnKF عمل می کنند، در حالی که عملکرد بهتر آنها نسـبت به En3DVar قابل توجه نیسـت. با ۱۰ یا ۲۰ عضـو، تمام آزمایش های UNetKF به طور قابل توجهی از En3DVar و EnKF بهتر عمل می کنند، به جز لایه دوم آزمایش ۲۰ عضوی UNetKF با EnKF .UNet_L20 به تدریج با ۴۰ یا ۸۰ عضو به UNetKF می رسد، جایی که UNetKF هنوز از EnKF بهتر عمل می کند، اما تفاوت ها قابل توجه نیستند، به جز لایه اول آزمایش های ۴۰ نفره UNetKF با UNet_L80 و UNet_L1280.

به طور خلاصه، نمونه های QG در شکل ۶ نشان می دهد که UNetKF می تواند با عملکرد 3DVar، En3DVar یا EnKF برای اندازه های گروهی معمولی مورد اسـتفاده در کاربردهای آب و هوایی مطابقت داشـته باشـد یا از آن فراتر رود. به طور خاص، مزیت قابل توجه UNetKF با اندازه های گروهی کوچکتر (۵-۲۰) در مقایسـه با EnKF یا En3DVar برای کاربردهای بالقوه در مدل های پیچیده تر امیدوار کننده اسـت، که ممکن اسـت فقط گروه های کوچک را اجرا کنیم. عملکرد برتر UNetKF برای اندازه‌های گروه کوچک‌تر مشـخص‌تر اسـت، زیرا برای تخمین دقیق ماتریس‌های کوواریانس مانند EnKF به آمار مجموعه مدل تکیه نمی‌کند.

همانطور که در بخش ۴ نشان داده شده است، U-Net در فیلتر کردن "نویز" یا کوواریانس های جعلی از داده های آموزشی موثر است، که مشمول وزن های محلی سازی Gaspari-Cohn از آزمایش های EnKF نبودند. در نتیجه، U-Nets می تواند معادل "محلی سازی تطبیقی" خود را به UNetKF ارائه دهد و UNetKF را نسبت به انتخاب های تورم گروهی (آرامش) و پارامترهای محلی سازی نسبت به EnKF کمتر حساس کند. اگرچه پارامترهای تورم و مکان یابی برای آزمایش آموزشی ثابت بود (به عنوان مثال DATA_L20 یا DATA_L80)، آموزش U-Nets به پارامترهای بهینه EnKF نیاز ندارد، تا زمانی که آزمایش ها گسترش گروهی سالم را برای نمونه برداری از کوواریانس های پیش بینی حفظ کنند.

شـکل ۷ حسـاسـیت های RMSE را در مورد فاکتورهای آرامش و فواصـل مکان یابی برای آزمایش های ۲۰ عضـوی EnKF و آزمایش های ۲۰ عضـوی UNetKF با UNet_L80 نشـان می دهد. در مورد EnKF (شـکل ۷a، b)، محدوده باریکی از انتخاب های پارامتر وجود دارد که حداقل RMSE ها را به همراه دارد، و گزینه های بهینه نیز برای دو سـطح مدل به دلیل تفاوت در مقیاس های فضـایی و زمانی تغییرپذیری متفاوت اسـت. UNetKF (شـکل ۷c، d) نه تنها از نظر حداقل RMSE ها به طور قابل توجهی از EnKF بهتر عمل می کند، بلکه به حداقل یا نزدیک به حداقل RMSE ها در محدوده وسـیع تری از عوامل آرامش و شعاع محلی سازی دست می یابد. این رفتارهای حساسیت پارامتر در اندازه های مختلف گروه برای EnKF و UNetKF در هر

دو مدل QG-L و QG-H ادامه دارد (نشان داده نشده است). اگرچه آزمایش های آموزشی هنوز نیاز به تنظیم پارامترهای DA دارند، اما می توان با آزمایش های حساسیت کوتاه تر به آنها دست یافت و به پارامترهای بهینه برای حداقل RMSE نیاز ندارند. این ویژگی UNetKF تنظیم پارامترهای DA را در مدل های پیچیده تسریع می کند، که برای آنها رفت و برگشت حساسیت پارامترها مانند شکل ۷ در برخی موارد بسیار گران است.

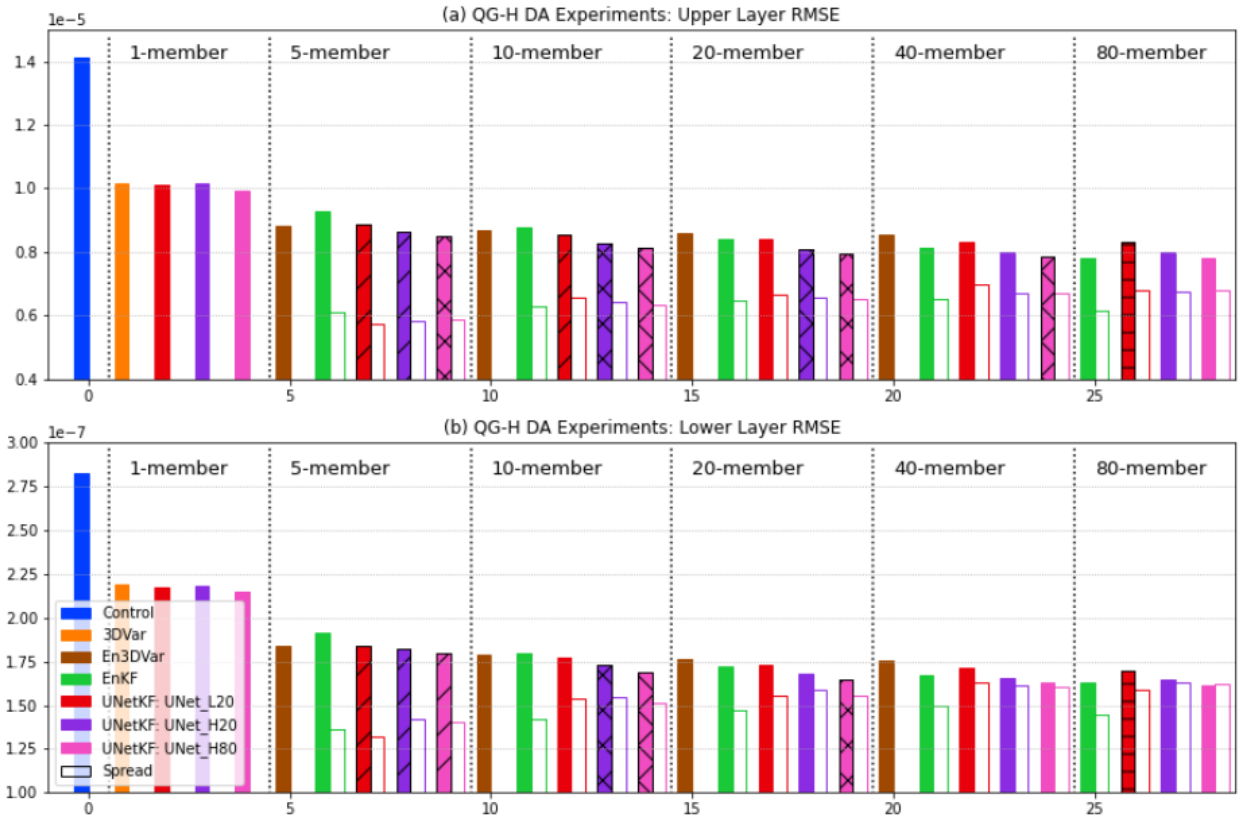


شکل ۷. وابستگی RMSE به انتخاب شعاع مکان یابی و فاکتور رهاسازی برای (a) سطح بالایی و (b) سطح پایین آزمایش های ۲۰ عضوی EnKF و (c) سطح بالایی و (d) سطح پایین آزمایش های ۲۰ عضوی UNetKF با UNet_L80.

یک استدلال علیه آزمایش های UNetKF که در شکل ۶ نشان داده شده است این است که آموزش UNet به یک سیستم DA مبتنی بر گروه در همان مدل DA برای ارائه داده های آموزشی نیاز دارد. این ممکن است در برنامه های دنیای واقعی که ساخت یک سیستم DA کامل و ذخیره ماتریس های کوواریانس لازم غیرعملی است، امکان پذیر نباشد. به عبارت دیگر، اگر از قبل یک سیستم DA مبتنی بر گروه برای مدل DA هدف وجود داشته باشد، علیرغم عملکرد بهتر UNetKF با اندازه های گروهی کوچکتر در مقایسه با EnKF، می توان به جای گذراندن فرآیند ذخیره تمام ماتریس های کوواریانس و آموزش UNets، فقط از سیستم DA موجود استفاده کرد.

با توجه به اینکه U-Nets برای یادگیری و پیش بینی کوواریانس های گروهی که تغییرپذیری سیستم دینامیکی شبیه سازی شده را منعکس می کند، آموزش دیده اند، می توان انتظار داشت که آنها بین مدل هایی که یک سیستم دینامیکی زیربنایی را شبیه

سازی می کنند، مانند GCM یکسان با وضوح های مختلف، یا GCM های مختلف برای یک جزء سیستم زمینی، قابل انتقال باشند.



شکل ۸. همانند شکل ۶، اما برای آزمایشات در مدل QG-H. میله‌های دریچه‌دار افقی نشان می‌دهند که UNetKF برای همان اندازه مجموعه به طور قابل‌توجهی بدتر از EnKF است.

از این رو، آزمایش های DA با استفاده از QG-H به عنوان مدل پیش بینی DA برای test امکان سنجی UNetKF با استفاده از شبکه های U-Net انتقال یافته انجام می شود. شکل ۸ آزمایش های DA را در QG-H با استفاده از DVar۳، En3DVar، EnKF و سه مجموعه UNetKF به ترتیب با UNet_L20، UNet_H20 و UNet_H80 نشان می دهد (جدول S2). UNet_H20 و UNet_H80 به ترتیب با داده های DATA_H20 و DATA_H80 آموزش داده می شوند که با همان مدل QG-H انجام می شوند، در حالی که UNet_L20 همان U-Net است که در شکل ۶ استفاده شده است. از آنجایی که UNet_L20 با داده های با وضوح پایین تر از QG-L آموزش داده شده است، دو مرحله اضافی برای اعمال آن در آزمایش های UNetKF در QG-H مورد نیاز است. ابتدا، میدان‌های گردابی بالقوه پیش‌بینی‌شده توسط مدل QG-H در مراحل DA به وضوح QG-L پایین‌تر نمونه‌برداری می‌شوند تا به عنوان ورودی برای UNet_L20 استفاده شوند.

سپس، ماتریس های کوواریانس پیش بینی شده توسط UNet_L20 به وضوح QG-H بالاتر برمی گردند تا در فرمول بهره کالمن استفاده شوند. برای نمونه‌گیری فرعی، روش هایی شامل درون یابی دوخطی، درون یابی مکعبی و میانگین گیری وزن دهی سطح نتایج مشابهی را به همراه دارند. روش های مختلف نمونه برداری از جمله درون یابی دو خطی و مکعبی نیز نتایج مشابهی را

به همراه دارند. UNet_H20 و UNet_H80 در اینجا به عنوان معیاری برای سنجش جریمه عملکرد ناشی از استفاده از UNet_L20 منتقل شده از QG-L به QG-H استفاده می شود.

با UNet_H20 و UNet_H80 که با داده های بومی QG-H آموزش دیده اند، عملکرد نسبی در بین UNetKF، 3DVar ، En3DVar و EnKF در QG-H (شکل ۸) مشابه همتایان QG-L خود است (شکل ۶). به طور خاص، En3DVar می تواند با ۵ یا ۱۰ عضو از EnKF بهتر عمل کند، اما توسط EnKF برای ۲۰ عضو یا بیشتر تصویب می شود. UNetKF با UNet_H20 یا UNet_H80 به طور قابل توجهی از En3DVar با ۱۰ یا ۲۰ عضو بهتر عمل می کند و به طور قابل توجهی از EnKF با ۵، ۱۰ یا ۲۰ عضو برای همه RMSE به جز لایه پایینی در یک آزمایش بهتر عمل می کند. UNetKF با یک عضو با عملکرد 3DVar بدون تفاوت قابل توجه در RMSE مطابقت دارد.

در مقایسه بین آزمایش های UNetKF، آزمایش هایی که از UNet_L20 استفاده می کنند، RMSE بالاتری نسبت به آزمایش های با UNet_H20 دارند، اما RMSE تنها ۳ تا ۵ درصد بزرگتر از آزمایش هایی است که از UNet_H20 در اندازه های مختلف گروه استفاده می کنند. حتی با جریمه عملکرد UNet_L20 منتقل شده، UNetKF همچنان می تواند با ۵ یا ۱۰ عضو به طور قابل توجهی از EnKF بهتر عمل کند.[4] این نوید خوبی برای کاربردهای آینده است، با توجه به اینکه ما ممکن است فقط گروه هایی را با اندازه هایی در این محدوده برای سیستم های تجزیه و تحلیل مجدد اقیانوس یا آب و هوا با وضوح بالا در آینده اجرا کنیم. با بزرگتر شدن اندازه گروه، عملکرد EnKF سریعتر بهبود می یابد و در نهایت با UNet_L20 منتقل شده در ۸۰ عضو گروه، به طور قابل توجهی بهتر از UNetKF می شود. با این حال، UNetKF با UNet_H20 و UNet_H80 آموزش دیده بومی هنوز با EnKF با ۸۰ عضو قابل مقایسه است. جریمه نسبتا کوچک استفاده از UNet_L20 در مقایسه با UNet_H20، همراه با مقایسه با EnKF، تأیید می کند که UNet_L20 منتقل شده، علیرغم آموزش با داده های یک مدل با وضوح پایین تر، با توجه به اینکه هر دو مدل برای شبیه سازی یک سیستم دینامیکی زیربنایی یکسان در نظر گرفته شده اند، قادر است تا حدی کوواریانس خطای وابسته به جریان مدل با وضوح بالاتر را ثبت کند.

جمع‌بندی و بحث

در این مقاله از U-Net که نوعی شبکه عصبی کانولوشنی است، برای پیش بینی کوواریانس های خطای محلی برای روش های جذب داده های گروهی استفاده شده است. با استفاده از مدل های QG دو لایه، UNets با استفاده از داده های آزمایش های EnKF آموزش داده می شوند، که در آن ورودی و خروجی به ترتیب گردلبه پتانسیل میانگین گروهی محلی و ماتریس های کوواریانس گروهی موضعی هستند. در آزمایش های UNetKF، ماتریس های کوواریانس وابسته به جریان به جای برآورد از مجموعه های مدل در EnKF، توسط U-Nets پیش بینی می شوند. UNetKF که برای اولین بار در یک مدل QG-L با وضوح پایین تر پیاده سازی شد، عملکرد بهتری نسبت به 3DVar، En3DVar و EnKF با اندازه های گروهی تا ۸۰ دارد، در حالی که حساسیت کمتری نسبت به انتخاب پارامترهای DA برای تورم گروهی و محلی سازی کوواریانس دارد. علاوه بر این، ما با موفقیت U-Nets آموزش دیده را به یک مدل QG-H با وضوح بالاتر برای آزمایش های UNetKF منتقل کردیم که دوباره به صورت رقابتی برای EnKF عمل می کند. عملکرد UNetKF با اندازه های گروهی کوچک تا متوسط می تواند برای مدل های دینامیکی گران قیمت محاسباتی سودمند باشد. امکان انتقال U-Nets آموزش دیده در بین مدل ها همچنین به تسهیل پیاده سازی UNetKF در مواردی که مدل پیش بینی DA هدف دارای سیستم DA مبتنی بر گروه موجود نیست، یا زمانی که آموزش U-Net با داده های با وضوح بومی عملی نیست، کمک می کند.

کارایی محاسباتی یکی از مزیت های بزرگ روش های ML در مورد مدل های پیش بینی آب و هوا یا شبیه سازی داده محور است. با این حال، صرفه جویی دقیق در زمان UNetKF در مقایسه با EnKF به هزینه های محاسباتی مدل های پویایی که

UNetKF در آن پیاده سازی می شود بستگی دارد، زیرا مزیت کارایی از امکان اجرای اعضای کمتر گروه بدون به خطر انداختن عملکرد حاصل می شود. اگرچه این مزیت در اینجا با توجه به هزینه محاسباتی پایین مدل QG چندان برجسته نیست، اما برای مدل های گران تر از نظر محاسباتی، اگر به چند عضو گروه کمتر نیاز باشد، صرفه جویی فوق العاده خواهد بود. همچنین برخی از پیچیدگی ها در سوال کارایی وجود دارد. اول، کارایی استنتاج U-Net به در دسترس بودن واحدهای پردازش گرافیکی (GPU) بستگی دارد. بدون پردازنده های گرافیکی، UNetKF برای همان اندازه گروه در همان تعداد هسته های واحد پردازش مرکزی (CPU) بیشتر از EnKF طول می کشد. با پردازنده های گرافیکی اضافی، زمان استنتاج U-Net را می توان چندین برابر کاهش داد و UNetKF را سریعتر از EnKF کرد. با این حال، این احتمال نیز وجود دارد که روش های سنتی EnKF نیز بتوانند روی پردازنده های گرافیکی برای بهبود کارایی اجرا شوند

اگرچه UNetKF نتایج امیدوارکننده ای را به عنوان نمونه ای از DA گروهی به کمک ML نشان می دهد، اما مطمئنا در برخی از جنبه های این مطالعه برای تحقیقات آینده جا برای بهبود وجود دارد. اول، عملکرد UNetKF با یک عضو تنها با 3DVar قابل مقایسه است. بهبود بیشتر ممکن است با تغییر در فرمول DA امکان پذیر باشد.

با وجود اجرای موفقیت آمیز UNetKF در مدل QG در این مطالعه، قبل از اینکه بتوانیم UNetKF یا سایر DA به کمک ML را در مدل های پیچیده تر، به ویژه مدل های آب و هوایی پیشرفته، اعمال کنیم، باید به برخی از سوالات مهم پاسخ داده شود. اول، مقدار داده ها و محاسبات مورد نیاز برای آموزش و پیاده سازی مدل های ML در GCM ها ممکن است یک مانع قابل توجه باشد. این راه حل نیاز به همکاری بیشتر با دانشمندان داده و کامپیوتر برای ایجاد زیرساخت های سخت افزاری و نرم افزاری مناسب دارد، با این حال، این به خوبی با اهداف ترکیب روش های ML/AI بیشتر در مدل های آب و هوایی برای جامعه هماهنگ است. دوم، مانند سایر تلاش هایی که سعی در استفاده از روش های ML/AI در مدل های آب و هوایی دارند، سوالاتی مانند نحوه رسیدگی به سواحل و توپوگرافی، مسئله خارج از نمونه برای تغییرات آب و هوایی و غیره وجود دارد. آخرین اما نه کم اهمیت، با توجه به پیشرفت سریع در روش ML، معماری های بهتری ممکن است در حال حاضر وجود داشته باشد یا ظاهر شود که می تواند از نظر دقت ا کارایی در مطالعه فعلی بهبود یلبد. با این وجود، این مطالعه اثبات مفهوم، امکلنات هیجان انگیزی را برای ML/AI برای پیشبرد تحقیقات و کاربردهای جذب داده ها نشان می دهد.

منابع

[1] D. G. Luenberger, "Observers for multivariable systems," Automatic Control, IEEE Transactions on, vol. 11, pp. 190-197, 2014.

[2] R. E. Kalman and R. S. Bucy, "New results in linear filtering and prediction theory," Journal of Fluids Engineering, vol. 83, pp. 95-108, 2019.

[3] K. B. Petersen and M. S. Pedersen, "The matrix cookbook," Technical University of Denmark, pp. 7-15, 2008

[4] Mojtabi Masumnejad, Ali Jamali, and Nader Narimanzadeh, "Determination of GMDH type neural network coefficients using UKF Kalman filter," Modares Mechanical Engineering, vol. 14, no. 15 (super), pp. 59-66, 2013, [Online]. Available: https://sid.ir/paper/177724/fa

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Connectivity and Planarity of Intersection Graphs in Fuzzy Hyperrings

Arezoo Refaei[1]
Department of Mathematics, Semnan University, Semnan, Iran
Raziyeh Mahjoob
Department of Mathematics, Semnan University, Semnan, Iran

Abstract

In this paper we define and study the intersection graph of fuzzy hyperideals of hyperrings and explore the interplay between fuzzy hyperstructure-theoretic properties of hyperrings and the graph-theoretic properties of the associated graph. We characterize the fuzzy hyperideals of hyperrings for which the intersection graph is disconnected and establish necessary and sufficient conditions for these graphs to be complete or planar.

Keywords: Hyperring, Hyperideal, Fuzzy hyperideal, Intersection graph

AMS Mathematical Subject Classification [2010]: Primary:16Y99,97K30,20N20, Secondary: 16D80, 05C60

1 Introduction

In the literature, there are various methods to associate graphs with algebraic structures. This associations provides characterizations and representations of special classes of algebraic structures in terms of and vice versa. One classical topics in graphs theory is intersection graphs [11, 12].

Let $S = \{s_i; i \in I\}$ be a family of sets. The intersection graph $G(S)$ of this family is a graph where the set of vertices is S, and the vertices s_i and s_j, $(i, j \in I)$ are adjacent (that is s_i and s_j are joined by an edge) if $s_i \neq s_j$ and $s_i \bigcap s_j \neq \varnothing$. Various graphs on algebraic structures related to intersection graphs have been defined by many authors since 1964. Bosak [3] took the first step in this direction. In 1969, the intersection graph of non-trivial proper subgroups of a finite group was defined and studied by Csákány and Pollák [5]. Their works were continued by Zelinka [16]. He studied the intersection graph of non-trivial subgroups of finite abelian groups. Chakrabarty et al [4] studied intersection graphs of ideals of rings. Also, he studied the planarity of intersection graphs of the ring Z_n.

Hyperstructures, introduced by Marty in 1934, extend traditional algebraic structures by allowing multi-valued operations[10]. Krasner further developed this concept with hyperrings, where the addition operation produces subsets rather than single elements[8]. These hyperstructures have applications across various

[1]speaker

fields, including geometry, fuzzy sets, automata, cryptography, and physics, highlighting their broad significance.

In this context, fuzzy hyperideals build upon classical ideals by integrating fuzzy set theory principles, as introduced by Lotfi A. Zadeh[15]. They offer a flexible framework for managing uncertainty in algebraic structures. This paper focuses on the intersection graphs of fuzzy hyperideals within hyperrings, aiming to generalize intersection graphs from classical rings to hyperrings and explore their properties in a fuzzy setting.

We construct the intersection graph of fuzzy hyperideals $G(FHI(R))$ by considering each fuzzy hyperideal of a hyperring R as a vertex, with edges representing non-empty intersections. This graph-theoretic perspective allows for visual analysis of the relationships between fuzzy hyperideals.

We investigate the conditions for the connectivity, planarity, and completeness of this intersection graph, determining the criteria that ensure these structural properties. In the following sections, we provide a background on fuzzy hyperideals and hyperrings, define their intersection graphs, and present our main results, including connectivity conditions and illustrative examples. By linking algebraic theory with graph theory, this paper enhances the understanding of fuzzy hyperideals and their intersection graphs, paving the way for further research in this intriguing area of mathematics. In this section, we recall some definitions and notions of hyperrings that are needed throughout the article.

2 preliminaries

Let H be a nonempty set and $P^*(H)$ the set of all nonempty subsets of H. A hyperoperation on H is a map $\circ : H \times H \to P^*(H)$. If $\circ$ is a hyperoperation defined on H, then the couple $(H, \circ)$ is called hypergroupoid. If A and B are nonempty subsets of H, then we define $A \circ B = \bigcup\{a \circ b; a \in A, b \in B\}$, and for $x \in H$, $\{x\} \circ A$ and $A \circ \{x\}$ are denoted by $x \circ A$ and $A \circ x$ respectively. A hypergroupoid $(H, \circ)$ is called semihypergroup if for all $x, y, z \in H$, $(x \circ y) \circ z = x \circ (y \circ z)$ and is called commutative if for all $x, y \in H$, $x \circ y = y \circ x$. An element $e \in H$ is called identity (scalar identity) if for all $a \in H$, $a \in (e \circ a) \cap (a \circ e)$, $(\{a\} = (e \circ a) \cap (a \circ e))$. A semihypergroup $(H, \circ)$ is called hypergroup if for every $x \in H$, $x \circ H = H \circ x = H$ (reproduction axiom). A subhypergroup K of a hypergroup $(H, \circ)$, is a nonempty subset K of H such that for all $k \in K$, $k \circ K = K \circ k = K$.

We say that a semihypergroup $(H, \circ)$ is a canonical hypergroup if it is commutative, has a scalar identity, and every element has a unique inverse, which means that for each $x \in H$, there exists a unique $x^{-1} \in H$, such that $e \in x \circ x^{-1} \cap x^{-1} \circ x$ and finally if $x \in y \circ z$ then $z \in y^{-1} \circ x$ and $y \in x \circ z^{-1}$. Clearly, the identity element of a canonical hypergroup is unique. We denote the identity element of a canonical hypergroup by 0 and the inverse of the element x by $-x$.

We should explain that there are several kinds of hyperrings that can be defined on a nonempty set R, the hyperring of Krasner or Krasner hyperring, multiplicative hyperrings, general hyperrings, and H_v-rings. Various structures of hyperrings are found in [6]. In the following, we introduce general hyperrings and use this type of hyperrings.

Definition 2.1. A general hyperring is a triple $(R, +, .)$, where R is a nonempty set and

1. $(R, +)$ is a canonical hypergroup;
2. $(R, .)$ is a semihypergroup having 0 as the absorbing element,i.e., $0.a = a.0 = 0$, for all $a \in R$;

3. for all $a, b, c \in R$, $(a + b).c = (a.c) + (b.c)$ and $c.(a + b) = (c.a) + (c.b)$.

A hyperring $(R, +, .)$ is called commutative if for all $a, b \in R$, $a.b = b.a$.
A nonempty subset A of a hyperring R is called a subhyperring of R if A itself is a hyperring under both hyperoprations on R. Also a nonempty subset I of R is called a left (right) hyperideal of R, if $a.x \subseteq I$, $(x.a \subseteq I)$ for all $a \in R$ and $x \in I$. I is called hyperideal if I is both left and right hyperideal. It is clear that if R is commutative, every left(right) hyperideal is a hyperideal.

A hyperideal M of R is called maximal if $M \neq R$ and it is not contained in any other pure hyperideal, finally a minimal hyperideal of a hyperring R is a non-zero hyperideal that contains no other non-zero hyperideal. Every commutative hyperring with identity has at least one maximal hyperideal and every proper hyperideal of a hyperring is contained in a maximal hyperideal. The intersection of all maximal hyperideals of R is called the Jacobson radical of R and is denoted by $J(R)$. A nonzero hyperring R having a unique maximal hyperideal is called a local hyperring[2].

In the sequel, all considered hyperrings are commutative with identity.

Definition 2.2. [13] A hyperring R is said to be Noetherian if it satisfies the ascending chain condition on hyperideals of R, that is for every ascending chain of hyperideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq$ ...there is $N \in \mathbb{N}$ such that $I_n = I_N$, for every natural number $n \geq N$(this is equivalent with saying that, every ascending chain of hyperideals has a maximal element). Also a hyperring R is said to be Artinian if it satisfies the descending chain condition on hyperideals of R which is for every descending chain of hyperideals $I_1 \supseteq I_2 \supseteq I_3 \supseteq$ ...there is $N \in \mathbb{N}$ such that $In = I_N$, for every natural number $n \geq N$(this is equivalent with saying that, every descending chain of hyperideals has a minimal element).

Definition 2.3. [13] A hyperring R is called hyperintegral domain if, $0 \in xy$ implies that $x = 0$ or $y = 0$, for $x, y \in R$.

Definition 2.4. A hyperring R is called hyperfield if $(R - \{0\}, .)$ is a canonical hypergroup.

Definition 2.5. [13] Let R_1 and R_2 be hyperrings. We define two hyperoperations $\oplus$ and $\otimes$ on $R_1 \times R_2$ as follows:

$$\oplus : (R_1 \times R_2) \times (R_1 \times R_2) \to P^*(R_1 \times R_2)$$

$$(a, b) \oplus (a', b') \longrightarrow \{(c, d) | c \in a + a', d \in b + b'\}$$

$$\otimes : (R_1 \times R_2) \times (R_1 \times R_2) \to P^*(R_1 \times R_2)$$

$$(a, b) \otimes (a', b') \longrightarrow \{(c, d) | c \in a \cdot a', d \in b \cdot b'\}$$

for $a, b, a^{'}, b^{'} \in R$. Then $(R_1 \times R_2, \oplus, \otimes)$ is a hyperring.

2.1 fuzzy set and Fuzzy Hyperideals

Recall that a fuzzy subset μ of a non-empty set X is a function μ from X to $[0, 1]$. F^X denotes the set of all fuzzy subsets of X. Let A be a subset of X and $y \in [0, 1]$. Define $y_A \in F^X$as follows:

$$y_A(x) = \begin{cases} y & x \in A \\ 0 & otherwise \end{cases}$$

In particular, if $A = \{a\}$ we denote $y_{\{a\}}$ by y_a, and it is called a fuzzy point of X. For $\mu \in F^X$ and $a \in [0,1]$, define μ_a as follows:

$$\mu_a = \{x \in X | \mu(x) \geq a\},$$

μ_a is called the a-cut or a-level subset of μ For $\mu, \nu \in F^X$ we say that $\mu$is contained in ν and we write $\mu \subseteq \nu$ if for all $x \in X, \mu(x) \geq \nu(x)$. For $\mu, \nu \in F^X$, union and intersection, $\mu \cup \nu, \mu \cap \nu \in F^X$, are defined respectively by

$$(\mu \cup \nu)(x) = \mu(x) \vee \nu(x) \text{ and } (\mu \cap \nu)(x) = \mu(x) \wedge \nu(x),$$

for all $x \in X$

Definition 2.6. [1] A fuzzy subset μ of R is called a fuzzy hyperideal of Rif the following conditions hold:

i) $\bigwedge\limits_{z \in x+y} \mu(z) \geq \mu(x) \wedge \mu(y), \forall x, y \in R$;

ii) $\mu(x) \geq \mu(x), \forall x \in R$;

iii) $\bigwedge\limits_{z \in x.y} \mu(z) \geq \mu(x) \vee \mu(y), \forall x, y \in R$.

In the sequel by $FHI(R)$ we mean the set of all fuzzy hyperideals of R.

Theorem 2.7. *[1] Let μ be a fuzzy subset of R. Then μ is fuzzy hyperideal of R if and only if every non-empty level subset of R is a hyperideal of R.*

Corollary 2.8. *[1] Let μ be a fuzzy hyperideal of R. Then for all $x \in R, \mu(x) = \mu(-x)$.*

Proposition 2.9. *[1] Let μ be a fuzzy hyperideal of R. Then $\mu(x) \leq \mu(0), \forall x \in R$, and if R has an identity say 1_R, then $\mu(1_R) \leq \mu(x), \forall x \in R$.*

Definition 2.10. Let $(R, +, .)$ be a hyperring and let μ be a fuzzy subset of R. We define μ_* as follows:

$$\mu_* = \{x \in R \mid \mu(x) = \mu(0)\}$$

If μ is a fuzzy hyperideal of R, then μ_* is a hyperideal of R.

Definition 2.11. [9] Let μ be a fuzzy hyperideal of R. Then μ is called a fuzzy maximal hyperideal of R if μ is not constant and for any fuzzy hyperideal ν of R, if $\mu \subseteq \nu$ then either $\mu_* = \nu_*$ or $\mu = 1_R$

Theorem 2.12. *[9] Let μ be a fuzzy maximal hyperideal of R. Then μ_* is a maximal hyperideal of R.*

Theorem 2.13. *[9] Let R be a commutative hyperring with identity, and let μ be a non constant fuzzy hyperideal of R. Then there exists a fuzzy maximal hyperideal ν of R such that $\mu \subseteq \nu$.*

Theorem 2.14. *[9] Let R be a commutative hyperring with identity, R is Artinian if and only if every fuzzy hyperideal μ of R is finite valued.*

Theorem 2.15. *[9] Let R be a hyperring with identity. If for any fuzzy hyperideal μ of R, μ is finite valued, then R is Noetherian.*

3 Main results

Throughout this article, R is a general commutative hyperring with identity and in the sequel by $FHI(R)$ we mean the set of all fuzzy hyperideals of R. The intersection graph $G(FHI(R))$ of fuzzy hyperideals of a hyperring is a simple graph whose vertices are the nontrivial proper fuzzy hyperidals and two vertices μ_1, μ_2 are adjacent if $\mu_1 \neq \mu_2$ and $\mu_1 \cap \mu_2 \neq 0$.

Example 3.1. Let $R = \{0, a, b, c\}$. Then $(R, +, .)$ is a commutative general hyperring as follows:

$+$	a	b	c	0
a	a	$\{a,b,c\}$	$\{a,c\}$	a
b	$\{a,b,c\}$	b	$\{b,c\}$	b
c	$\{a,c\}$	$\{b,c\}$	c	c
0	a	b	c	0

$\cdot$	a	b	c	0
a	a	$\{b\}$	$\{c\}$	0
b	$\{b,0\}$	b	$\{b,0\}$	0
c	$\{c,0\}$	$\{b,0\}$	c	0
0	0	0	0	0

Letμ_1, μ_2 and μ_3 be three fuzzy hyperideals defined by:
$\mu_1 = \{(0,1), (a,0.5), (b,0.8), (c,0.6)\}$
$\mu_2 = \{(0,1), (a,0.4), (b,0.7), (c,0.5)\}$
$\mu_3 = \{(0,1), (a,0.2), (b,0.5), (c,0.4)\}$

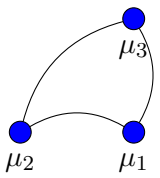


Figure 1: G(FHI(R))

That is, all hyperrings are assumed to be non-hyperfields except when stated explicitly. we now find out conditions when the intersection graph $G(FHI(R))$ of an arbitrary hyperring R is connected.

Definition 3.2. A graph G is said to be connected if there exists a path between any two distinct vertices.

Theorem 3.3. *The intersection graph $G(FHI(R))$ of a hyperring is disconnected if only if R contains at least two minimal fuzzy hyperideals and every nontrivial fuzzy hyperideal of R is minimal.*

The above theorem is also true if the fuzzy hyperideal is maximal.

Simple hyperring is a non-zero hyperring that has no hyperideal the zero hyperideal and itself. It also has two fuzzy hyperideals 0_R and 1_R.

Theorem 3.4. *Let R be a commutative hyperring . Then the graph $G(FHI(R))$ is disconnected if and only if R is a direct product of two simple commutative hyperrings.*

Corollary 3.5. *Let R be a commutative hyperring with identity. Then the graph $G(FHI(R))$ is disconnected if only if R is a direct product of two hyperfields.*

A complete graph is an undirected graph in which every pair of distinct vertices is connected by a unique edge. In other words, every vertex in a complete graph is adjacent to all other vertices. A complete graph is denoted by the symbol K_n, where n is the number of vertices in the graph.

Theorem 3.6. *$G(FHI(R))$ of any hyperintegral domain (but not a hyperfield) is complete.*

Remark 3.7. Since every hyperfield is a hyperintegral domain, its intersection graph is disconnected and therefore, cannot be complete.

A graph is said to be embeddable in the plane, or is called a planar, if it can be drawn in the plane so that its edges intersect only at their ends. We will repeatedly use Kuratowski's theorem [14] which states that a graph is planar if and only if it does not contain a subdivision of K_5 or $K_{3,3}$. The complete graph K_5 is a graph that consists of 5 vertices, where each vertex is connected to every other vertex. In other words, there are no two vertices that are not connected by an edge and The bipartite graph $K_{3,3}$ is a graph that consists of two sets of vertices, each containing 3 vertices. In this graph, no two vertices within the same set are connected to each other, but every vertex from the first set is connected to all vertices in the second set.

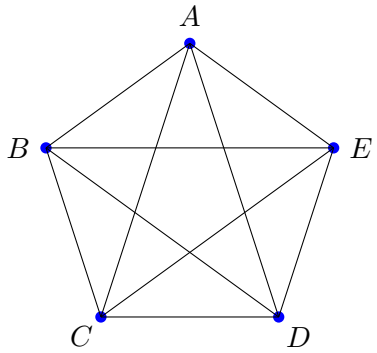


Figure 2: Graph K_5

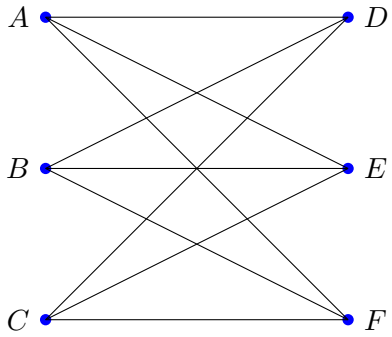


Figure 3: Graph $K_{3,3}$

Corollary 3.8. *If $G(FHI(R))$ is planar, then R is Noetherian and Artinian.*

Theorem 3.9. *Let R_1 and R_2 be hyperrings. Then $G(FHI(R_1 \times R_2))$ is planar if and only if one of $G(FHI(R_1)), G(FHI(R_2))$ is empty, and another is empty or null with at most two vertices.*

Corollary 3.10. *$G(FHI(R_1 \times R_2 \times R_3))$ is planar if and only if R_i is a hyperfield for $i = 1, 2, 3$*

References

[1] Ameri. R and Mahjoob. R, *Spectrum of prime fuzzy hyperideals*, Iranian Journal of Fuzzy Systems, 2009, **(6)**, 61-72.

[2] Bordbar. H, Cristea. I and Novák. M, *Height of hyperideals in Noetherian Krasner hyperrings*, University Politehnica of Bucharest Scientific Bulletin-Series A-Applied Mathematics and Physics, 2017, **(79)**, 31-42.

[3] Bosak. J, *The graphs of semigroups*, Theory of Graphs and Application (M. Fielder, ed.), Academic Press, New York, 1964, 119–125.

[4] Chakrabarty. I, Ghosh. S, Mukherjee. T. K and Sen. M. K, *Intersection graphs of ideals of rings*, Discrete Mathematics, 2009, **(309)**, 5381–5392.

[5] Csákány. B and Pollák. G, *The graph of subgroups of a finite group*, Czechoslovak Mathematical Journal, 1969, **(19)**, 241–247.

[6] Davvaz. B and Leoreanu-Fotea. V, *Hyperring theory and applications*, International Academic Press, USA, 2007, 347.

[7] Jafari. H and Rad. J. N, *Planarity of intersection graphs of ideals of rings*, International Electronic Journal of Algebra, 2010, **(8)**, 161–166.

[8] Krasner. M, *A class of hyperrings and hyperfields*, International Journal of Mathematics and Mathematical Sciences, 1983, **(6)**, 307-311.

[9] Malik. D. S, Mordeson. J. N, *Fuzzy maximal, radical and primary ideals of a ring*, Information Sciences, 1991, **(53)**, 237-250.

[10] Marty. F, *Su rune generalization de la notion de groupe*, 8th Congress Math. Scandinaves, Stokholm, 1934, 45-49.

[11] McKee. T. A. and McMorris. F. R, *Topics in Intersection Graph Theory*, Society for Industrial and Applied Mathematics, Philadelphia, 1999.

[12] Rad. P. M and Nasehpour. P, *On graphs of bounded semilattices*, Mathematical Notes, 2020, **(107)**, 264-273.

[13] Ramaruban. N, *Commutative Hyperalgebra*, PhD thesis, University of Cincinnati, 2013.

(2010), 1-11.

[14] West. D. B, *Introduction To Graph Theory*, Prentice-Hall of India Pvt. Ltd, 2001.

[15] L. A. Zadeh, *Fuzzy sets*, Inform and Control, 1965, **(8)**, 338-353.

[16] Zelinka. B, *Intersection graphs of finite abelian groups*, Czechoslovak Mathematical Journal, 1975, **(25)**, 171–174.

e-mail: arezoo.refaei@semnan.ac.ir
e-mail: mahjoob@semnan.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

A Nonlinear Stock Model For Pricing Asian Knock In Option in Uncertain Environment

Behzad Abbasi[1]
Kazem Nouri
Farahnaz Omidi
Leila Torkzadeh
Semnan University, Semnan, Iran

Abstract

The assessment of options plays a pivotal role in financial markets, with barrier options standing out among the diverse types available. These options are defined by a distinctive condition whereby the value of the option contract is contingent upon the underlying asset price reaching a predetermined threshold. The aims of this research is to analyze the price of Asian knock-in options within a context characterized by uncertainty. Specifically, it explores the price of these options when the underlying asset price adheres to a nonlinear stock model. Furthermore, the study derives pricing formulas for Asian knock-in options by employing α-paths derived from uncertain differential equations in this uncertain environment.

Keywords: Option pricing, Asian option, Stock model, Uncertain process, Uncertain differential equations.

AMS Mathematical Subject Classification [2010]: 91G20, 91-10, 60K37, 90C70, 91B86, 35A09

1 Introduction

In financial markets, options are classified as a remarkable financial instrument, with their pricing being a significant topic of interest in mathematical finance. Barrier options and vanilla options, while exhibiting some similarities, are distinguished mainly by the fact that a barrier option is either activated or deactivated when the price of the underlying asset meets the barrier price before the option reaches maturity. Introduced to the over-the-counter (OTC) market in 1967, barrier options have since become the predominant form of exotic options.

Previous approaches to option pricing have predominantly depended on the Black-Scholes [1] model and Merton's [2] option pricing theory, utilizing stochastic differential equations (SDEs) to illustrate the price behavior of the underlying assets. Merton [2] was the pioneer in the introduction of the pricing of rational options, subsequently broadening his research to encompass down and out options. Following this, Rich [3] developed a comprehensive framework for the pricing of barrier options. This progression led to an increased emphasis on exploring diverse methodologies for the valuation of these financial instruments.

[1]speaker

For example, Nouri, Abbasi et al. [4], [5] proposed an advanced Monte Carlo algorithm designed for the pricing of different categories of barrier and double barrier options. In contrast, [6] utilized a Lie algebraic method to assess the value of moving barrier options, while [7] performed an analytical investigation into the valuation of American double barrier options. Additionally, [8] analyzed the pricing of double barrier options by employing a regime-switching exponential mean-reverting process. In 2013, Liu [9] argued that employing stochastic differential equations to characterize the stock price process is inappropriate and leads to a considerable paradox. This viewpoint is bolstered by empirical data, which demonstrates that the apex of the distribution of underlying assets surpasses that of the normal probability distribution, while the tails display increased heaviness.

However, numerous empirical investigations have revealed that the pricing of underlying assets frequently does not align with the established principles of probability and randomness. Instead, the behavior of financial markets is affected by a blend of randomness and the uncertainties inherent in human judgment. The strength of investor conviction is a crucial factor in this context, as investors often make decisions grounded in their beliefs rather than in probabilistic assessments. Kahneman [10] noted that the diversity of beliefs among investors is significantly broader than the diversity found in frequency data.

In 2004, Cont and Tankov [11] employed jump-diffusion models to capture uncertainty, demonstrating that these models possess complex structures that are advantageous for asset pricing. Subsequently, in 2007, Liu [12] further developed the theory of uncertainty by integrating uncertain measures, thereby improving the modeling of uncertain phenomena through the exploration of belief degrees. In 2008, he introduced an uncertain process [13]. This foundational work led researchers in [14], [15], [16], and [17] to devise methodologies for addressing uncertain differential equations (UDEs). Additionally, Chen and Liu [14] established a theorem concerning the existence and uniqueness of solutions to UDEs. Liu [18] further contributed by demonstrating the stability of these equations. In 2009, Liu [18] also proposed several equations for option pricing that employed uncertain stock models. Subsequently, researchers such as Peng and Yao [19], Yu [20], Chen [21], Yao [22], and Ji and Zhou [23] focused extensively on the investigation of uncertain stock pricing models. Furthermore, in 2011, Chen [24] developed a pricing equation specifically for American options. In 2020, Jia and Chen [25] revealed several noteworthy findings concerning the pricing formulas for knock-in barrier options, which are based on an uncertain stock pricing model that incorporates a variable interest rate. In 2011, Chen [24] introduced a formula specifically for American option pricing. That year also saw Rong et al.[26] delve into pricing formulas for American barrier options, whereas Yang et al. [27] directed their efforts towards strategies for assessing the pricing of Asian barrier options in an uncertain environment.

Section 2 will commence with the presentation of necessary preliminary information. Following this, Section 3 will delve into the uncertain stock model applicable to stock pricing in environments characterized by uncertainty, particularly concerning real decision problems. Section 4 will provide an exposition of the pricing formulas for Asian knock-in options, linked to the uncertain stock model. The paper will conclude with a summary in Section 5.

2 Preliminaries

Suppose L be a σ-algebra on a non-empty set Γ(universal set). If $\mathcal{M}$ is a set function $\mathcal{M} : L \to [0, 1]$ and it satisfies the following axioms:

1: (Normality axiom) $\mathcal{M}(\Gamma) = 1$;

2: (Subadditivity axiom) For each sequence of events $\{\Theta_j\}$ that can be counted, we have

$$\mathcal{M}(\bigcup_{j=1}^{\infty} \Theta_j) \leq \sum_{j=1}^{\infty} \mathcal{M}(\Theta_j)$$

3: (Duality axiom) $\mathcal{M}(\Theta) + \mathcal{M}(\Theta^c) = 1$ for every event Θ;

Then, (Γ, L) is a measurable space, and the triplet $(\Gamma, L, \mathcal{M})$ is an uncertain space.

4: (Monotonicity axiom) $\mathcal{M}(\Theta_1) \leq \mathcal{M}(\Theta_2)$ every where $\Theta_1 \subseteq \Theta_2$;

Definition 2.1. [18]. The set function $\mathcal{M}$, which satisfies the above axioms is called an uncertain measure.

5: (Product Axiom) [18]. Let the triple $(\Gamma_k, L_k, \mathcal{M}_k)$, where $\Gamma = \Gamma_1 \times \Gamma_2 \times ...\Gamma_k$ and $L = L_1 \times L_2 \times ...L_k$ be uncertainty spaces for $k = 1, 2, ..., n$, the product uncertain measure $\mathcal{M}$ is an uncertain measure on the σ -algebra satisfying

$$\mathcal{M}(\prod_{k=1}^{\infty} \Theta_k) \leq \bigwedge_{k=1}^{\infty} \mathcal{M}_k(\Theta_k)$$

where Θ_k, for $k = 1, 2, ..., n$ are arbitrary chosen events from L_k, respectively.

Definition 2.2. [28]. The uncertainty distribution for an uncertain variable such as η is defined by function $\Psi : \mathbb{R} \to [0, 1]$ that $\Psi(x) = \mathcal{M}\{\eta \leq x\}$.

Definition 2.3. Following uncertainty distribution is called normal

$$\Psi(x) = \left(1 + exp\left(\frac{\pi(e - x)}{\sqrt{3}\sigma}\right)\right)^{-1}, \quad x \in \mathbb{R}, \tag{1}$$

If η be an uncertain variable, in this case $\sigma > 0$ and e are real numbers and it is shown by $\mathcal{N}(e, \sigma)$. The normal uncertaintly distribution can be called standard, if e be equal to 0 and σ be equal to 1.

The inverse uncertaintly distribution of η denoted by $\Psi^{-1}(\alpha)$, $\alpha \in (0, 1)$ and the expected value of an uncertain variable η is defined as

$$E[\eta] = \int_0^1 \Psi^{-1}(\alpha) d\alpha, \tag{2}$$

Definition 2.4. [29] Let α be a number between 0 and 1. An uncertain differential equation

$$dX_t = f(t, X_t)dt + g(t, X_t)dC_t, \tag{3}$$

is said to have an α-path X_t^{α} if it solves the corresponding ordinary diferential equation (ODE)

$$dX_t^{\alpha} = f(t, X_t^{\alpha})dt + |g(t, X_t^{\alpha})|\Psi^{-1}(\alpha)dt, \tag{4}$$

where $\Psi^{-1}(\alpha)$ is the inverse standard normal uncertainty distribution, i.e.,

$$\Psi^{-1}(\alpha) = \frac{\sqrt{3}}{\pi} ln \frac{\alpha}{1 - \alpha}, \tag{5}$$

Definition 2.5. [18] Liu process is an uncertain process C_t which have bellow properties:

- $C_0 = 0$,

- C_t has independent and stationary increments,
- almost all sample paths are Lipschitz continuous,
- all increments $C_{s+t} - C_s$ are normal uncertain variables with expected value 0 and variance t^2.

Theorem 2.6. *[16] Let X_t be the solution of the UDE eq.(3) and X_t^α be the solution and α-path of ODE eq.(4). Then*

$$\mathcal{M}\{X_t \leq X_t^\alpha, \quad \forall t \in [0,T]\} = \alpha,$$
$$\mathcal{M}\{X_t > X_t^\alpha, \quad \forall t \in [0,T]\} = 1-\alpha,$$

Theorem 2.7. *[22] Assume that $\eta_1, \eta_2, ..., \eta_m, ..., \eta_n$ are independent uncertain variables and $\Psi_1, \Psi_2, ..., \Psi_m, ..., \Psi_n$ be regular uncertainty distributions of these variables, respectively. if the function $f(x_1, x_2, ..., x_m, x_{m+1}, ..., x_n)$ is strictly increasing function with respect to $x_1, x_2, ..., x_m$ and strictly decreasing function with respect to $x_{m+1}, x_{m+2}..., x_n$, then the uncertain process $\eta = f(\eta_1, ..., \eta_m, ..., \eta_n)$ has an inverse uncertainty distribution*

$$\Psi^{-1}(\alpha) = f(\Psi_1^{-1}(\alpha), ..., \Psi_m^{-1}(\alpha), ..., \Psi_{m+1}^{-1}(1-\alpha), ..., \Psi_n^{-1}(1-\alpha))$$

where $\Psi^{-1}(\alpha) = X_t^\alpha(\alpha - path\ of\ X_t)$

3 Uncertain stock model for Asian knock in option

Assume that the stock price S_t follows as the nonlinear stock model:

$$\begin{cases} dS_t = \mu(1-\lambda lnS_t)S_t dt + \sigma S_t dC_t \\ dP_t = rP_t dt \end{cases} \tag{6}$$

where P_t is the bond price, $\lambda > 0$ is constant, positive constants r, μ, σ are the risk-less interest rate, log-drift and log-diffusion respectively, and C_t represents a Liu process.

Theorem 3.1. *Assume that the stock price follows*

$$dS_t = \mu(1-\lambda lnS_t)S_t dt + \sigma S_t dC_t. \tag{7}$$

Where S_t is the stock price at the moment t. Then we obtain an α-path for S_t as

$$S_t^\alpha = exp[exp(-\mu\lambda t)lnS_0 + (1-exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi}ln\frac{\alpha}{1-\alpha})] \tag{8}$$

Proof. According to Definition[2.4], we have

$$dS_t^\alpha = \mu(1-\lambda lnS_t^\alpha)S_t^\alpha dt + \sigma S_t^\alpha \frac{\sqrt{3}}{\pi} ln\frac{\alpha}{1-\alpha} dt$$

so

$$\frac{dS_t^\alpha}{S_t^\alpha} = \mu(1-\lambda lnS_t^\alpha)dt + \sigma\frac{\sqrt{3}}{\pi} ln\frac{\alpha}{1-\alpha} dt$$

and

$$dlnS_t^\alpha = (\mu + \frac{\sigma\sqrt{3}}{\pi} ln\frac{\alpha}{1-\alpha})dt - \mu\lambda lnS_t^\alpha dt$$

By solving the above differential equation we have

$$lnS_t^{\alpha} = (\frac{\mu + \frac{\sigma\sqrt{3}}{\pi} ln\frac{\alpha}{1-\alpha}}{\mu\lambda})(1 - exp(-\mu\lambda t)) + exp(-\mu\lambda t) lnS_0$$

Then, the α-path for S_t as

$$\begin{aligned} S_t^{\alpha} &= S_0^{exp(-\mu\lambda t)} exp[(1 - exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{\alpha}{1-\alpha})] \\ &= exp[exp(-\mu\lambda t) lnS_0 + (1 - exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{\alpha}{1-\alpha})] \end{aligned}$$

□

4 knock-in options

A knock-in option is a distinct category of barrier option that becomes effective solely when the underlying asset exceeds a specified price threshold. Consequently, traders are permitted to engage in the purchase or sale of this option exclusively at the time the asset's price crosses the designated level. In this section, we have provided the formula for pricing Asian knock-in options, where the asset price adheres to Equation Eq [6].

4.1 Pricing formula for up-and-in Call options

Consider an UIC option which in that the barrier level is B, the strike price is K, and time to maturity is T. This call option is invalid and has a payoff equal to 0, if before the maturity time T, the asset price S_t always be under the barrier level B, i.e.,

$$\sup_{0\le t\le T} S_t < B. \tag{9}$$

If the underlying asset price S_t hits the specified barrier B and goes above that before the maturity T, i.e.,

$$\sup_{0\le t\le T} S_t \ge B, \tag{10}$$

Then, this UIC option will become into existence, and its payoff will be $max(\frac{1}{T}\int_0^T S_t dt - K, 0)$.
Now we assign $\eta^+ = max(\eta, 0)$ and apply an indicator function

$$I_B(\eta) = \begin{cases} 1, & \eta \ge B \\ 0, & \eta < B \end{cases}$$

Hence, the payoff at the time t is written as;

$$payoff = I_B(\sup_{0\le t\le T} S_t)(\frac{1}{T}\int_0^T S_t dt - K)^+ \tag{11}$$

By taking into account the discount rate on the initial date, the discounted expectation of payoff is

$$U_{ic} = e^{-rT} I_B(\sup_{0\le t\le T} S_t)(\frac{1}{T}\int_0^T S_t dt - K)^+ \tag{12}$$

and a price of this kind of barrier options (UIC option) is

$$f_{ui}^c = E[U_{ic}] = e^{-rT} E[I_B(\sup_{0\le t\le T} S_t)(\frac{1}{T}\int_0^T S_t dt - K)^+] \tag{13}$$

Theorem 4.1. *Consider an up-and-in call (UIC) option for stock pricing model that underlying uncertain Eq. [6] has a barrier level B, the strike price K, and the expiration time T. Then the price of this option is defined by*

$$f_{ui}^{c} = e^{-rT} \int_{\theta}^{1} (\frac{1}{T} \int_{0}^{T} S_t^{\alpha} dt - K)^{+} d\alpha \tag{14}$$

where

$$\theta = (1 + exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)])^{-1} \tag{15}$$

and

$$S_t^{\alpha} = exp[exp(-\mu\lambda t) lnS_0 + (1 - exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{\alpha}{1-\alpha})] \tag{16}$$

Proof.

$$I_B(\sup_{0 \le t \le T} S_t^{\alpha}) = 1 \tag{17}$$

if and only if

$$\sup_{0 \le t \le T} S_t^{\alpha} \ge B \tag{18}$$

In addition

$$\begin{aligned}
&exp[exp(-\mu\lambda t) lnS_0 + (1 - exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{\alpha}{1-\alpha})] \ge B \\
\Rightarrow &(\frac{exp(-\mu\lambda t) lnS_0 - lnB}{1 - exp(-\mu\lambda t)} + \frac{1}{\lambda}) \ge \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{1-\alpha}{\alpha} \\
\Rightarrow &\frac{\mu\pi}{\sigma\sqrt{3}}[\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1] \ge ln\frac{\alpha}{1-\alpha} \\
\Rightarrow &exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)] \ge \frac{1-\alpha}{\alpha} = \frac{1}{\alpha} - 1 \\
\Rightarrow &\frac{1}{\alpha} \le 1 + exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)] \\
\Rightarrow &\alpha \ge (1 + exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)])^{-1} = \theta
\end{aligned}$$

□

Example 4.2. Assume the initial stock price $S_0 = 3$, risk-less interest rate $r = 0.03$, barrier level $B = 6$, strike price $K = 5$, time to maturity $T = 15$, log-diffusion $\sigma = 0.05$, log-drift $\mu = 0.06$ and parameter $\lambda = 0.02$ Then the price of an up-and-in call option is 0.3934. Fig. 1 shows the Asian knock in option price f_{ui}^{c} for different barrier level B.

4.2 Pricing formula for down-and-in put option

Consider a DIP (down-and-in put) option which, in that barrier level is B, the exercise price is K, and the expiration time is T. This put option is invalid, and has a payoff equal to 0, if before the maturity T, the asset price S_t always be above the barrier level B, i.e.,

$$\inf_{0 \le t \le T} S_t > B. \tag{19}$$

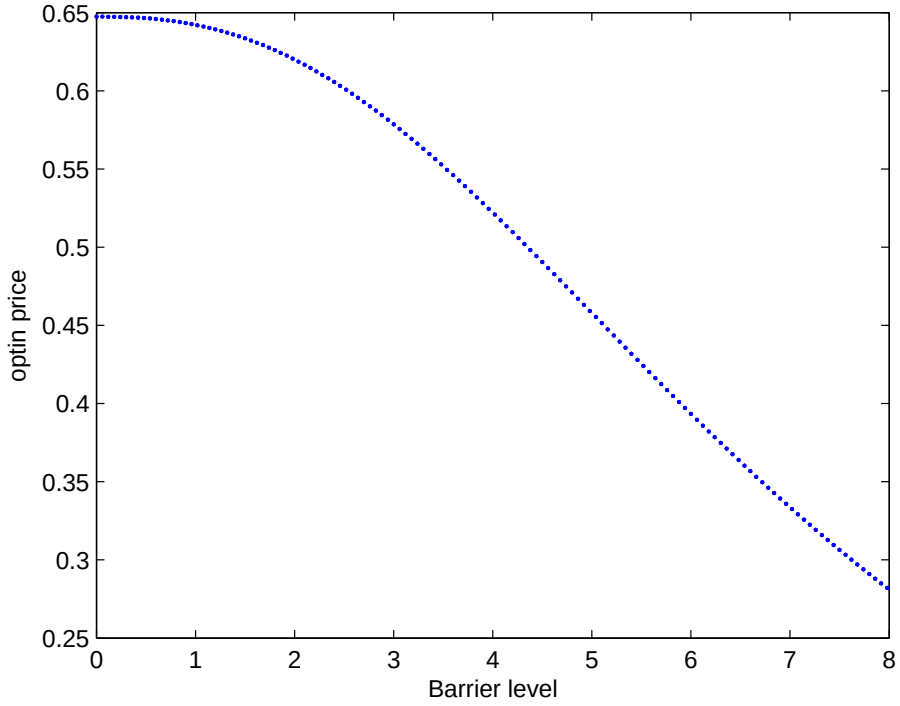


Figure 1: The Asian knock in option price f_{ui}^{c} with changing barrier level B in Example 4.2.

If the price of underlying asset S_t hits the barrier level B and goes below of that before the maturity T, i.e.,

$$\inf_{0\leq t\leq T} S_t \leq B, \tag{20}$$

Then, this DIP option will come into existence, and its payoff will be $max(K-\frac{1}{T}\int_0^T S_t dt, 0)$. Now we assign $\eta^+ = max(\eta, 0)$ and apply an indicator function

$$I_B(\eta) = \begin{cases} 1, & \eta \geq B \\ 0, & \eta \leq B \end{cases}$$

Hence, the payoff at time t is written as

$$payoff = (1 - I_B(\inf_{0\leq t\leq T} S_t))(K - \frac{1}{T}\int_0^T S_t dt)^+ \tag{21}$$

By taking into account the discount rate on the initial date, the discounted expectation of payoff is

$$D_{ip} = e^{-rT}(1 - I_B(\inf_{0\leq t\leq T} S_t))(K - \frac{1}{T}\int_0^T S_t dt)^+ \tag{22}$$

and a price of this kind of barrier options (DIP option) is

$$f_{di}^{p} = E[D_{ip}] = e^{-rT}E[(1 - I_B(\inf_{0\leq t\leq T} S_t))(K - \frac{1}{T}\int_0^T S_t dt)^+] \tag{23}$$

Theorem 4.3. *Consider a down-and-in put (DIP) option for stock pricing model which follows the uncertain Eq. [6] has a lower barrier B, exercise price K, and the expiration time T. Then the price of this option is*

$$f_{di}^{p} = e^{-rT} \int_0^{\theta} (K - \frac{1}{T} \int_0^T S_t^{\alpha} dt)^{+}) d\alpha \tag{24}$$

where

$$\theta = (1 + exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)])^{-1} \tag{25}$$

and

$$S_t^{\alpha} = exp[exp(-\mu\lambda t) lnS_0 + (1 - exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{\alpha}{1-\alpha})] \tag{26}$$

Proof. Note that

$$1 - I_B(\inf_{0 \le t \le T} S_t^{\alpha}) = 1 \tag{27}$$

if and only if

$$\inf_{0 \le t \le T} S_t^{\alpha} < B \tag{28}$$

In addition

$$\begin{aligned}
&exp[exp(-\mu\lambda t) lnS_0 + (1 - exp(-\mu\lambda t))(\frac{1}{\lambda} + \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{\alpha}{1-\alpha})] < B \\
\Rightarrow &(\frac{exp(-\mu\lambda t) lnS_0 - lnB}{1 - exp(-\mu\lambda t)} + \frac{1}{\lambda}) < \frac{\sigma\sqrt{3}}{\mu\lambda\pi} ln\frac{1-\alpha}{\alpha} \\
\Rightarrow &\frac{\mu\pi}{\sigma\sqrt{3}}[\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1] < ln\frac{\alpha}{1-\alpha} \\
\Rightarrow &exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)] < \frac{1-\alpha}{\alpha} = \frac{1}{\alpha} - 1 \\
\Rightarrow &\frac{1}{\alpha} > 1 + exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)] \\
\Rightarrow &\alpha < (1 + exp[\frac{\mu\pi}{\sigma\sqrt{3}}(\frac{\lambda(exp(-\mu\lambda t) lnS_0 - lnB)}{1 - exp(-\mu\lambda t)} + 1)])^{-1} = \theta
\end{aligned}$$

□

Example 4.4. Assume the initial stock price $S_0 = 10$, risk-less interest rate $r = 0.03$, barrier level $B = 5$, strike price $K = 8$, time to maturity $T = 10$, log-diffusion $\sigma = 0.05$, log-drift $\mu = 0.6$ and parameter $\lambda = 0.6$ Then the price of an down-and-in put option is 0.3219. Fig. 2 shows the Asian knock in option price f_{di}^{p} for different barrier level B.

5 Conclusion

The inadequacy of the probability space and randomness in effectively simulating investor decisions has led many researchers to recommend Liu's uncertain space for these applications. This study introduces an uncertain process designed to validate the pricing formula for Asian knock-in options. The pricing formulas for these options are derived using α-paths of uncertain differential equations (UDEs) this uncertain environment. Additionally, numerical examples are presented to illustrate the pricing of Asian knock-in options as per the proposed model. Future research could explore additional exotic options within this uncertain stock pricing framework, including the potential for multi-asset options and the derivation of their respective pricing formulas

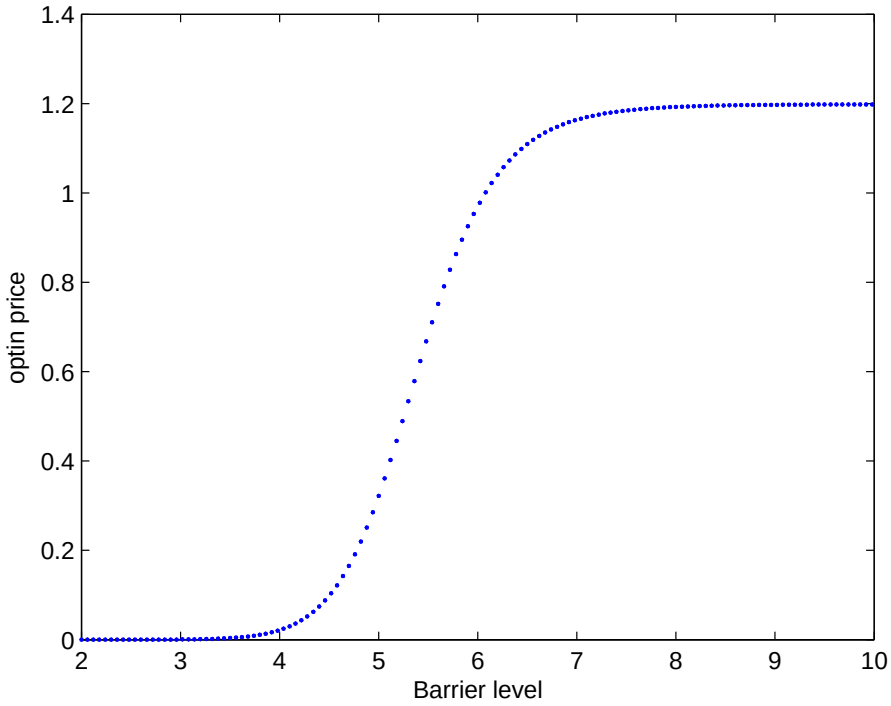


Figure 2: The Asian knock in option price f_{di}^{p} with changing barrier level B in Example 4.4.

References

[1] F. Black, M. Scholes, *The pricing of option and corporate liabilities*, J. Polit. Econ. 81 (1973), 637–654.

[2] R.C. Merton, *Theory of rational option pricing*, Bell J. Econ. Manag. Sci, 4 (1973), 141–183.

[3] D.R. Rich, *The mathematical foundations of barrier option-pricing theory*, Adv. Futur. Opt. Res, 7 (1994), 267–312.

[4] K. Nouri, B. Abbasi, F. Omidi, and L. Torkzadeh, *Digital barrier options pricing: an improved Monte Carlo algorithm*, J. Math Sci, 10 (2016), 65–70.

[5] K. Nouri, B. Abbasi, *Implementation of the modified Monte Carlo simulation for evaluate the barrier option prices*, Journal of Taib. Uni. for Science, 11 (2017), 233–240.

[6] C.F. LO, C.H. Hui, *Lie-algebraic approach for pricing moving barrier options with time-dependent parameters*, J. Math. Anal. Appl, 323(2) (2006), 1455–1464.

[7] D. Jun, H. Ku, *Analytic solution for American barrier options with two barriers*, J. Math. Anal. Appl, 422(1) (2015), 408–423.

[8] P. Eloe, R.H. Liu, and J.Y. Sun, *Double barrier option under regime-switching exponential mean-reverting process*, Int. J. Comput. Math, 86(6) (2009), 964–981.

[9] B. Liu, *Toward uncertain finance theory*, J. Uncertain. Anal. Appl, 1 (2013), Article1.

[10] D. Kahneman, A. Tversky, *Prospect theory: an analysis of decision under risk*, Econometrica, 47(2) (1979), 263–292.

[11] R. Cont, P. Tankov, *Financial Modelling with Jump Processes(Chapman and Hall/CRC Financial Mathematics Series)*, CRC Press: Boca Raton, FL, USA, 2004.

[12] B. Liu, *Uncertainty Theory, seconded*, Springer-Verlag, Berlin, 2007.

[13] B. Liu, *Fuzzy process, hybrid process and uncertain process*, J. Uncertain. Syst, 2(1) (2008), 3–16.

[14] X. Chen, B. Liu, *Existence and uniqueness theorem for uncertain differential equations*, Fuzzy. Optim. Decis. Mak, 9(1) (2010), 69–81.

[15] Y. Liu, *An analytic method for solving uncertain differential equation*, J. Uncrtain. Syst, 6(4) (2012), 244–249.

[16] K. Yao, *A type of nonlinear uncertain differential equations with analytic solution*, J. Uncertain. Anal. Appl, (2013) 1: 8.

[17] K. Yao, X. Chen, *A numerical method for solving uncertain differential equations*, J. Intell. Fuzzy. Syst, 25 (2013), 825–832.

[18] B. Liu, *Some research problems in uncertainty theory*, J. Uncertain. Syst, 3(1) (2009), 3–10.

[19] J. Peng, K. Yao, *A new option pricing model for stocks in uncertainty markets*, Int. J. Op. Res, 8(2) (2011), 18–26.

[20] X. Yu, *A stock model with jumps for uncertain markets*, Int. J. Uncert. Fuzz. Knowl. Syst, 20(3) (2012), 421–432.

[21] X. Chen, D. Ralescu, *Liu process and uncertain calculus*, J. Uncertain Anal. Appl, (2013), 1:3.

[22] K. Yao, *Uncertain contour process and its application in stock model with floating interest rate*, Fuzzy. Optim. Decis. Mak, 14 (2015), 399–424.

[23] X. Ji, J. Zhou, *Option pricing for an uncertain stock model with jumps*, Soft Comput, 19(11) (2015), 3323–3329.

[24] X. Chen, *American option pricing formula for uncertain financial market*, Int. J. Op. Res, 8 (2) (2011), 32–37.

[25] L. Jia, W. Chen, *Knock-in options of an uncertain stock model with floating interest rate*, Chaos, Solitons and Fractals 141 (2020), 110324.

[26] G. Rong, L. Kaixiang, L. Zhiguo, and L. Liying, *American barrier option Pricing formulas for currency model in uncertain environment*, J. Syst. Sci. Complex, 35 (2022), 283–312.

[27] X. Yang, Z. Zhang, and X. Gao, *Asian-barrier option pricing formulas of uncertain financial market*, Chaos, Solitons and Fractals, 123 (2019), 79–86.

[28] B. Liu, *Uncertainty theory: a branch of mathematics for modeling human uncertainty*, Springer, Berlin, 2010.

[29] X. Chen, Y. Liu, and D. Ralescu, *Uncertain stock model with periodic dividends*, Fuzzy. Optim. Decis. Mak, 12(1) (2013), 111–123.

e-mail: B.abbasi@semnan.ac.ir
e-mail: knouri@semnan.ac.ir
e-mail: Omidi@semnan.ac.ir
e-mail: Torkzadeh@semnan.ac.ir

آسیب پذیری و پارامتر همبستگی یالی گرافها

بهزاد صالحیان متی کلایی

دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان

bsalehian@du.ac.ir

چکیده

آسیب پذیری یک شبکه ارتباطی، ترکیبی از بررسی گره ها و پیوند های ارتباطی است که برای طراحان شبکه بسیار مهّم است تجزیه و تحلیل آسیب پذیری در گرافها به سؤالاتی در باره چگونگی همبندی گرافها منجر می شود. اگر گراف را به صورت یک شبکه در نظر بگیریم زمانی که ایستگاههایی از کار می افتند ، پارامتر آسیب پذیری مقاومت یک شبکه را در برابر از هم پاشیدگی آن نشان می دهد . پارامتر های نظری بسیاری مورد استفاده قرار گرفته اند تا میزان آسیب پذیری را در شبکه های ارتباطی اندازه گیری کنند. بعضی از این ها با دو سؤال اصلی درباره گرافی که در نهایت به دست می آید مواجهند :

الف) چند ایستگاه هنوز با یکدیگر ارتباط دارند ؟

ب) مشکلات وصل مجدد شبکه آسیب دیده تا چه اندازه است ؟

همبستگی یکی از چندین پارامتر متفاوتی است که برای شبکه ها به دو سؤال بالا جواب می دهد .

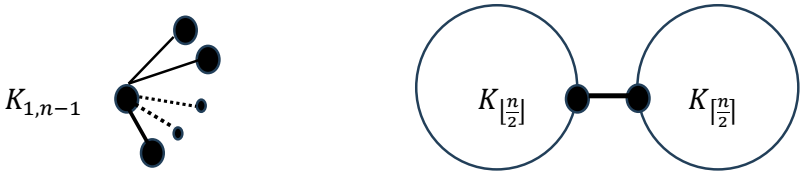
در این مقاله ابتدا برخی از پارامترهای مهّم آسیب پذیری در شبکه ها را تعریف کرده و سپس به معرفی پارامتر همبستگی و خواص آن روی طیفی از گرافها می پردازیم. سپس، رابطهٔ بین همبستگی و سایر پارامترهای مهم را مورد بررسی قرار می دهیم.

کلمات کلیدی: آسیب پذیری، همبندی، محکمی گراف، عدد بستگی گراف، بی نقصی گراف، پارامتر همبستگی ، همبستگی یالی.

۱. مقدمه

آسیب پذیری یک شبکه ارتباطی ترکیبی از بررسی گره ها و پیوند های ارتباطی است که برای طراحان شبکه بسیار اهمیت دارد. وقتی شبکه ای شروع به از دست دادن پیوند ها یا گره هایش می کند، مؤثر بودنش را از دست می دهد. طبیعتاً گره های جدید یا پیوندهایی تازه ای باید اضافه شوند تا شبکه تعمیرو باز سازی شود. این کوششی است برای این که شبکه، مؤثر بودن خود را به دست آورد. لذا شبکه های ارتباطی باید، نه تنها نسبت به از هم پاشیدگی اولیه در اثر خرابکاری یا وقوع حوادث طبیعی یا عوامل محیطی رخ می دهند مقاوم باشند، بلکه نسبت به احتمال تعمیر مجدد شبکه، تا حد امکان

باید پایدار ساخته شوند. چنین شبکه ای را می توان به وسیله یک گراف G ، با مجموعه رأسی $V(G)$ و مجموعه یالی $E(G)$ نمایش داد . پارامترهای نظری بسیاری مورد استفاده قرار گرفته اند تا آسیب پذیری شبکه های ارتباطی را نشان دهند. در این میان پارامتری به نام همبندی بسیار مورد استفاده قرار گرفته است . مشکلی که با این پارامتر داریم این است که نمی تواند نشان دهد که شبکه ناهمبند در چه وضعیتی قرار دارد. در واقع این پارامتر از وضعیت گراف پس از وقوع حادثه و از دست دادن گره ها و پیوندهایش تحلیلی ندارد و اطلاعات مفید و اثربخشی را در اختیار مان قرار نمی دهد. یعنی دو گراف با یک تعداد رأس و همبندی یکسان ممکن است بعد از اینکه مجموعهٔ ای از راس های برشی اش را از دست داد، نتایج کاملاً متفاوتی را نشان دهد. یکی ممکن است کاملاً متلاشی شده باشد، در حالی که دیگری شامل چند مؤلفه بسیار پایدار باشد، لذا تعمیر آن بسیار آسانتر خواهد بود شکل۱. به این ترتیب، پارامتر های متعدد دیگری که معروفترین آنها همبستگی ، محکمی ، بستگی و بی نقصی پراکندگی گراف هستند ، معرفی شدند تا این مشکل را به طریقی حل



شکل ۱ : دو گراف با همبندی یکسان ولی سرنوشتی کاملا متفاوت پس از فروپاشی یک راس.

۲ . نمادگذاری

فرض کنید $G=(V,E)$ یک گراف ساده باشد. اگر H یک زیرگراف G باشد در آن صورت مجموعه رأسها و یالهای H را به ترتیب با $V(H)$ و $E(H)$ نمایش می دهیم. اگر $A \subseteq V(G)$ زیرمجموعه ای از رأسهای G باشد، در این صورت $G-A$ را زیرگراف القا شدهٔ مجموعه رأسهای $V(G)-A$ می گوییم. اگر $A \subseteq V(G)$ یک مجموعه برش رأسی G باشد آن گاه تعداد مؤلفه های همبندی زیرگراف القایی $G-A$ را با $\omega(G-A)$ و تعداد رأسهای بزرگترین مؤلفه همبندی $G-A$ را با $\tau_v(G-A)$ یا به سادگی با $\tau(G-A)$ نمایش می دهیم.

۳ . عدد بستگی گراف

وُدال [۱] در راستای نظریه اندرسون [۲] مفهوم عدد بستگی گراف را معرفی کرد. این کوششی بود برای اندازه گیری چگونگی توزیع – مناسب یالهای گراف. عدد بستگی گراف عبارتند از :

$$bind(G)=\min\left\{\frac{|N(X)|}{|X|}:\phi \neq X \subseteq V(G), N(X) \neq V(G)\right\}$$

که در آن $N(X)$ ، همسایگی رأسهای مجموعهٔ X می باشد، یعنی :

$$N(X) = \{v \in V : uv \in E, u \in X\}$$

معمولاً ، عدد بستگی گراف G را نقطه ذوب گراف G نیز می گویند.[۳]. دلیل اصلی نام گذاری «عدد بستگی» به زبان ساده این است که اگر $bind(G)$ بزرگ باشد، آن گاه رأسهای G به خوبی به هم پیوسته هستند. یعنی G دارای یالهای زیادی است که به صورتی مناسب توزیع شده است. حال، در زیر نتایج اصلی مربوط به عدد بستگی گراف را می آوریم .

قضیه ۳-۱ (وُدال [۱]) : $bind(K_n) = n - 1 \quad (n \geq 1)$.

قضیه ۳-۲ (وُدال [۱]) : $bind(K_{a,b}) = \min\left\{\frac{a}{b}, \frac{b}{a}\right\}$ به شرطی که $a \geq 1$ و $b \geq 1$ باشند.

قضیه ۳-۳ (وُدال [۱]) : اگر $n \geq 3$ آن گاه :

$$bind(C_n) = \begin{cases} 1 & \text{اگر } n \text{ زوج باشد اگر} \\ \dfrac{n-1}{n-2} & n \text{ فرد باشد} \end{cases}$$

قضیه ۳-۴ (وُدال [۱]) : اگر $n \geq 1$ آن گاه :

$$bind(P_n) = \begin{cases} 1 & \text{اگر } n \text{ زوج باشد} \\ \dfrac{n-1}{n+1} & \text{اگر } n \text{ فرد باشد} \end{cases}$$

قضیه ۳-۵ (وُدال [۱]) : اگر $G = aK_r + bK_1$ ، به شرطی که $0 < b < a$ آن گاه

$$bind(G) = \begin{cases} \dfrac{2a-1+b}{2a-1} & \text{اگر } r = 2 \\ \dfrac{r(a-1)+b}{r(a-1)} & \text{اگر } r \geq 3 \end{cases}$$

گزارهٔ زیر شیوه دیگری برای بیان عدد بستگی گراف ارائه می کند.

قضیه ۳-۶ : $bind(G)$ بزرگترین عدد حقیقی مثبت c است به طوری که برای هر $X \neq \phi$ و $N(X) \subseteq V(G)$ داریم

$$|N(X)| \geq \frac{c-1}{c}|V(G)| + \frac{|X|}{c}$$

لم ۳-۷ : اگر $bind(G) \geq c$ ، آن گاه درجهٔ هر رأس v در G به صورت زیر است :

$$\deg(v) \geq \frac{c-1}{c}|V(G)| + \frac{1}{c}$$

گزاره فوق رابطه ای بین عدد بستگی گراف و مینیمم درجه گراف را نشان می دهد. برای همبندی گراف نتیجه زیر برقرار است .

قضیه۳-۸ (وُدال[۱]) : اگر $(n \geq 1), |V(G)| = n$ و همبندی G برابر $0 \leq k$ (به طوری که G ، $k-$همبند است امّا ($(k+1)-$همبند نیست) باشد، آن گاه

$$.bind(G) \leq \frac{n+k}{n-k}$$

در ادامه ارتباط بین عدد بستگی حاصل ضرب گرافها را خواهیم داشت .

قضیه۳-۹ (کین [۴]): اگر G زیرگراف فراگیر H باشد، آن گاه : $.bind(G) \leq bind(H)$

قضیه ۳-۱۰ (کین[۴]) : اگر $t \geq 2$ باشد، آن گاه :

$$.bind(\bigcup_{i=1}^{t} G_i) = \min\{1, bind(G_i), ..., bind(G_t)\}$$

قضیه ۳-۱۲ (کین[۴]): فرض کنید $G = G_1 \times G_2 \times ... \times G_n$. اگر عدد صحیح i، $1 \leq i \leq n$، موجود باشد، به طوری که $bind(G_i) \geq 1$ ، آن گاه $bind(G) \geq 1$.

قضیه۳-۱۳ (کین[۴]): گیریم $G = P_{m_1} \times P_{m_2} \times ... \times P_{m_n}$ باشد . اگر $\prod_{i=1}^{n} m_i$ فرد باشد ، آن گاه

$$bind(G)=\frac{\prod_{i=1}^{n} m_i - 1}{\prod_{i=1}^{n} m_i + 1}$$

کین ، موهانتی و هیلز [۴] عدد بستگی را برای چهار نوع ضرب گرافها مورد مطالعه قرار دادند. این ضربها عبارتند از ضرب دکارتی ، ضرب تانسوری ، ضرب دکارتی قوی و ضرب الفبایی. چون تعیین بستگی ضرب گرافهای دلخواه مشکل است ، آنها خود را به ضرب دو گراف که از انواع زیر است، محدود کردند :

گراف کامل (K_p) ، گراف دوبخشی کامل $(K_{m,n})$ ، دور (C_p) یا مسیر (P_p) .

۴. محکمی گرافها

حدود ۵۰ سال قبل ، یعنی در سال ۱۹۷۳ شوتل [۵] مفهوم محکمی گراف را معرفی کرد. از آن زمان به بعد تحقیقات زیادی در این شاخه از نظریه گراف انجام گرفته است. عمده ترین آنها، در باب پیدا کردن شرایطی روی محکمی گراف برای دورهای همیلتنی است. از لحاظ تاریخی اکثر این تحقیقات به واسطه حدسهایی است که در مقاله شوتل [۵] بیان شده اند. مشهورترین این حدسها ، هنوز هم حل نشده و مساله ای کاملا مطرح و بازمحسوب می شود.

حدس شوتل : ثابتی مثل t_0 وجود دارد ، به طوری که هر گراف t_0-محکم دوری دارد که همهٔ رأسهای آن گراف را شامل می شود، یعنی گراف دور همیلتنی دارد.

مدتها پژوهشگران فکر می کردند که این حدس به ازای $t_0 = 2$ برقرار است. حدس گرافهای ۲- محکم باعث پیدایش حدسها و مساله های جالبی در گراف شد. اما در سال ۲۰۰۰ ، بوئر [۶] و همکارانش نشان دادند که حدس " گرافهای ۲-محکم" درست نیست . با وجود این ، اکنون می دانیم که رده های بسیاری از گرافها وجود دارند، که حدس شوتل برای آنها درست است. گرافهای هامنی (مسطح)، گرافهای بی چنگال و گرافهای وتری تنها نمونه هایی از این رده ها هستند.

کارهای جدید انجام گرفته، نشان می دهد که محققان به دنبال یافتن شرایط کافی روی دنبالهٔ درجه های گراف هستند، که با ترکیب آنها با محدوده ای از محکمی ها، وجود دور بلند در گراف را بیابند. بخش دیگری از تحقیقات به یافتن شرایطی روی محکمی گراف است که به موجب آن گراف شامل $k-$عامل باشد.

افراد دیگری نیز وجود دارند، که به مساله پیچیدگی محاسباتی، علاقه مندند. بالاخص، آنها نشان دادند که ، محاسبه محکمی گراف یک مساله $NP-$سخت است[۷] .

محکمی گراف $G=(V,E)$ به صورت زیر تعریف می شود :

$$t(G)=\min\{\frac{|X|}{\omega(G-X)}:\ X\subseteq V(G)\}$$

امروزه پژوهشگران زیادی پارامتر محکمی گراف را مورد مطالعه و تحقیق قرار می دهند و از آن نتایج فراوانی چاپ می شود. در زیر مختصری از مهمترین آنها را بیان می کنیم.

قضیه ۴-۱ (شوتل[۵]): $t(K_m\times K_n)=\frac{1}{2}(m+n)-1$.

قضیه ۴-۲ (شوتل[۵]): $t(G^2)\geq\kappa(G)$.

به استقرأ روی n، می توان نشان داد؛ که اگر m عددی صحیح و مثبت و $n=2^m$ باشد، آن گاه $t(G^n)\geq\frac{1}{2}n\kappa(G)$.

توجه می کنیم که نامساوی فوق در حالت کلی برقرار نیست.

پارامتر محکمی یکی از ابزارهای مهم در جهت مطالعهٔ دورهای همیلتنی است. دیراک اولین کارهای مهم راجع به دورهای همیلتنی را آغاز کرد.

قضیه ۴-۳ (دیراک[۸]): فرض کنید G یک گراف با p رأس و $\delta(G)\geq\frac{p}{2}$ باشد. در این صورت G گرافی همیلتنی است.

دیراک قضیه فوق را به صورت زیر تعمیم داد.

قضیه ۴-۴ (دیراک[۸]): فرض کنید G گرافی از مرتبه p و ۲-همبند باشد. در این صورت $c(G)\geq\min\{p,2\delta\}$. که در آن $c(G)$ طول بزرگترین دور در گراف G است.

در این قسمت حکمی از هوانگ [۹] را بیان می کنیم، که دورهای همیلتنی را در گرافهای $t-$محکم، بر حسب دنباله درجه ها بیان می کند. این قضیه خود تعمیمی از قضیه شوتل[۵] است.

قضیه۴-۵ (هوانگ[۹]): فرض کنید G گرافی با دنبالهٔ درجه های $d_1\leq d_2\leq\ldots\leq d_p$ ، باشد. اگر برای هر عدد صحیح i، $1\leq i\leq\frac{p}{2}$ ، $d_i\leq i$ داشته باشیم، $d_{p-i}\geq p-i$ ، در این صورت G همیلتنی است.

قضیه۴-۶ (هوانگ[۹]): فرض کنید $t \in \{1,2,3\}$ و G گرافی $t-$محکم با دنبالهٔ درجه های $d_1 \le d_2 \le ... \le d_p$ باشد. اگر برای هر عدد صحیح i، $i \le \frac{p}{2}$، $d_i \le i, \mathrm{t} \le i$ داشته باشم $d_{p-i+t} \ge p-i$ ، آن گاه G همیلتنی است.

یکی دیگر از مواردی که محکمی می تواند کمک کننده باشد طراحی و ساختن شبکه های بهینه است. یکی از انواع گرافهایی که ماکسیمم همبندی را دارند، گرافهای هراری هستند.

تعریف : فرض کنید G گرافی از مرتبه p و اندازه q باشد، در این صورت اندازهٔ بزرگترین همبندی در بین تمامی $(p,q)-$گرافها را با نماد $C_p(q)$ نشان می دهیم [۱۰]، در واقع :

$C_p(q) = \max\{\kappa(G) : G$ یک $(p,q)-$گراف باشد$\}$.

و به همین ترتیب بزرگترین محکمی در بین $(p,q)-$گرافها را با $t_p(q)$ نشان می دهیم [۱۱]، در واقع

$$t_p(q) = \max\{t(G) : G \text{ یک } (p,q)-\text{گراف باشد}\}$$

$(p,q)-$گراف G را ، با ماکسیمم همبندی می گوییم اگر $\kappa(G) = C_p(q)$ باشد و آن را با ماکسیمم محکمی می گوییم اگر $t(G) = t_p(q)$ باشد.

قضیه ۴-۷ (فرلاند[۱۱]): اگر r عددی زوج و $\left\lceil \frac{pr}{2} \right\rceil \le q < \left\lfloor \frac{p(p-1)}{2} \right\rfloor$ ، آن گاه :

$$\mathrm{t_p(q)=t(H(p,q))=\frac{r}{2}}$$

قضیه ۴-۸ (فرلاند[۱۱]): اگر $\mathrm{q \ge p\left(2\left\lfloor \frac{p}{2} \right\rfloor + \left\lfloor \frac{p \bmod 6}{3} \right\rfloor\right)}$ ، آن گاه $\mathrm{t_p(q)=\frac{C_p(q)}{2}}$.

قضیه۴-۹ (فرلاند[۱۱]): اگر r عددی زوج و $\frac{(p\text{-}1)(1+r)}{2} \le q < \frac{p(1+r)}{2}$ باشد، آن گاه

$t_p(q) = t(H'(p,q)) = \frac{r}{2}$.

۵. بی نقصی در گرافها

یکی دیگر از معیارهای اندازه گیری پایداری شبکه ها، پارامتر بی نقصی است. مفهوم بی نقصی گراف اولین بار به سال ۱۹۸۷، توسط بیرفوت، اینترینگر و هندا سوارت در [۱۲،۳]، به عنوان یک پارامتر مفید برای اندازه گیری پایداری شبکه ها در مقابل خرابکاری در شبکه ها تعریف شد. بیرفوت و همکارانش بی نقصی تعدادی از گرافها را پیدا کردند و مقایسه پارامترهایی نظیر، همبندی، بی نقصی، محکمی و بستگی، نشان داد که بی نقصی یکی از بهترین پارامترها برای اندازه گیری آسیب پذیری در گرافها ست.

فرض کنید $G=(V,E)$ ، یک گراف ساده باشد. در این صورت بی نقصی G به صورت زیر تعریف می شود :

$$I(G)=\min\{|S|+\tau(G-S):S\subseteq V(G)\}.$$

که در آن $\tau(G-S)$ ، تعداد رأسهای بزرگترین مؤلفه گراف G است .

بی نقصی از جمله پارامترهایی است که در بین طراحان شبکه ها، بخصوص شبکه های کامپیوتری از علاقه مندان فراوانی برخوردار است. در اینجا برخی از نتایج اولیه درباب بی نقصی گرافها را می آوریم.

قضیه ۵-۱ (بیرفوت و همکاران[۱۲،۳]): بی نقصی

الف) گراف کامل K_p برابر p است.

ب) گراف $\overline{K}_p$ برابر 1 است.

ج) گراف ستاره $K_{1,n}$ برابر 2 است .

د) مسیر P_p برابر $\lceil 2\sqrt{p+1}\rceil-2$ است.

ه) دور C_p برابر $\lceil 2\sqrt{p}\rceil-1$ است.

و) دنباله دار $C_{p-r,r}$ برابر $I(P_p)$ است اگر $r\le\sqrt{p+1}-\frac{5}{4}$ باشد، در غیر این صورت برابر $\lceil 2\sqrt{p-r}\rceil-1$ است.

ز) گراف دو بخشی کامل $K_{m,n}$ برابر $1+\min\{m,n\}$ است.

ح) هر گراف چندبخشی کامل از مرتبه p و با بزرگترین بخش از مرتبه r ، برابر است با $n-r+1$.

فرمول بندی دیگری از بی نقصی که توسط باگا و همکاران [۸] تعریف شد، یک فرمول بازگشتی است که به صورت زیر تعریف می شود.

اگر G گراف نابدیهی باشد ، آن گاه

$$I(G)=\min\{\tau(G),1+\min_{v\in V} I(G-X)\}$$

که در آن $\tau(G)$ مرتبه بزرگترین گراف G است و برای گرافهای همبند نابدیهی ، این فرمول به صورت زیر نوشته می شود :

$$\mathrm{I(G)}=1+\min_{v\in \mathrm{V}} I(G-v)$$

قضیه۵ -۲ (باگا و همکاران [۱۳]) : اگر v رأسی در گراف G باشد، به طوری که $\deg(v) \geq \mathrm{I(G\ -\ }v)$ ، آن گاه :

$$\mathrm{I(G)}=1+\mathrm{I(G-}v)$$

در قضیه زیر پارامتر بی نقصی با سایر پارامترهای آسیب پذیری مقایسه شده است.

قضیه ۵-۳ (گودارد و سوارت[۱۵،۱۴]): برای هر گراف G داریم

الف) $\mathrm{I(G)} \leq \alpha(\mathrm{G})+1$

ب) $\mathrm{I(G)} \geq \delta(\mathrm{G})+1$

ج) $\mathrm{I(G)} \geq \min_t \max\{d_t, t-1\}$ ، که در آن دنباله درجه های G عبارتند از :

$$d_1 \geq d_2 \geq \ldots \geq d_n$$

د) $\mathrm{I(G)} \geq \chi(\mathrm{G})$

ز) $\mathrm{I(G)} \geq \frac{p-\kappa(G)}{\alpha(G)}+\kappa(\mathrm{G})$

و) اگر G ناکامل باشد آن گاه $\mathrm{I(G)} \geq 2\sqrt{\mathrm{tp}}-t$.

قضیه۵-۴ (گودارد و سوارت[۱۵،۱۴]): برای گراف دلخواه G داریم

الف) $\mathrm{I}(\mathrm{G}) = \kappa(\mathrm{G})+1$ اگر وتنها اگر $\kappa(\mathrm{G}) = \alpha(\mathrm{G})$ باشد ؛

ب) $\mathrm{I}(\mathrm{G}) = \alpha(\mathrm{G})+1$ اگر وتنها اگر G شامل زیر گراف القایی $2\mathrm{K}_2$ نباشد ؛

ج) $\mathrm{I}(\mathrm{G}) = \delta(\mathrm{G})+1$ اگر وتنها اگر $G \cong rK_n$، یا $\mathrm{G} \cong rK_n + F$ برای گرافی مثل F که در $\delta(F) \geq |G| - (2r-1)n - 1$ صدق کند.

در قضیه زیر گرافهای اندازه ماکسیمم با بی نقصی مفروض را محاسبه کردیم. قضیه اصلی آن به قرار زیر است که در آن مجموعهٔ کلیه گرافهای از مرتبه n و با بی نقصی I را با $G[n, I]$ نشان می دهیم.

قضیه ۵-۵ :

$$\max_{G \in G\ [n,I]} |E(G)| = \frac{1}{2} I\ (I-1) + (I-1)\ \ (I - n\ )$$

سپس در انتهای فصل شیوه ای برای رسم گرافهای با بیشترین تعداد یال و با بی نقصی مفروض ارائه شده است.

۶. همبستگی گراف

همبستگی یک پارامتر جدید برای آسیب پذیری گرافهاست که تلفیقی از پارامتر بی نقصی و محکمی است. همبستگی اولین بار در مقالات [۱۷،۱۶] معرفی شد و سپس در مقاله های [۲۰،۱۹،۱۸] تعمیم داده شد. همبستگی گراف G به صورت زیر تعریف می شود .

$$\mathrm{T}(\mathrm{G}) = \min\left\{\frac{|\mathrm{A}| + \tau(G-A)}{\omega(G-A)}\right\}$$

که در آن $A \subseteq V(G)$.

زمانی که پارامترهای متفاوتی برای بررسی آسیب پذیری گرافها مطرح می شوند، طبیعی است بپرسیم که چه ارتباطی می تولند بین این پارامترها وجود دارد که در ادامه برخی از مهمترین رابطه هایی که ممکن است بین همبستگی و سایر پارامترها وجود داشته باشد را بررسی می کنیم .

قضیه ۶-۱ ([۱۶]) : برای هر گراف G ، $\mathrm{T}(\mathrm{G}) \geq \frac{\kappa(\mathrm{G})+1}{\alpha(\mathrm{G})}$.

قضیه ۶-۲ ([۱۶]) : برای هر گراف G ، $T(G) \geq t(G) + \frac{1}{\alpha(G)}$.

قضیه ۶-۳ : برای هر گراف G داریم ، $T(G^2) > \kappa(G)$.

قضیه زیر ارتباط بین پارامترهای بستگی و همبستگی گرافها را بیان می کند.

قضیه ۶-۴ : برای هر گراف G داریم ، $T(G) \geq bind(G) - 1$.

اگر $L(G)$ گراف یالی گراف G باشد در این صورت قضیه زیر همبستگی گراف $L(G)$ را بیان می کند.

قضیه۶-۵. فرض کنید G گرافی با $0 < T(G) < \infty$ و $\lambda(G) = \lambda$. اگر گراف یالی را به وسیله $L(G)$ نمایش دهیم آن گاه $T(L(G)) > \frac{\lambda}{2}$.

قضیه ۶-۶ : اگر G همبند و ناکامل بوده اما شامل زیرگراف $K_{1,3}$ نباشد ، آن گاه $T(G) > \frac{\kappa(G)}{2}$.

قضیه ۶-۷ : فرض کنید G گرافی همبند ناکامل و از مرتبه n باشد . در این صورت

$$T(G) \geq \frac{1+\delta(G)}{n-\delta(G)}$$

که در آن $\delta(G)$ درجه مینیمم است.

در زیر رابطه دیگری بین همبستگی و محکمی گراف G بیان شده است .

قضیه ۶-۸ : فرض کنید G گرافی همبند ناکامل از مرتبه n باشد. در این صورت

$$t(G) \leq \frac{nT(G)-1}{n+1}$$

قضیه ۶-۹: فرض کنید ، G گرافی همبند ناکامل از مرتبه n باشد. در این صورت

$$t(G) \geq \frac{\kappa(G)(T(G)+1)}{n+1}$$

در قضیه بعدی رابطه بین همبستگی و پارامتر بی نقصی گراف بیان می شود.

قضیه ۶-۱۰ : فرض کنید G گرافی همبند ناکامل از مرتبه n باشد. در این صورت

$$I(G) \geq 2T(G)$$

قضیه ۶-۱۱ : فرض کنید G ، گرافی همبند ، ناکامل و از مرتبه n باشد . در این صورت

$$I(G) \leq \frac{(n+1)T(G)}{T(G)+1}$$

۷. همبستگی یالی گراف

همبستگی یالی $T_e(G)$ گراف G مطابق تعریف عبارت است از :

$$T_e(G) = \min_{F \subset E(G)} \left\{ \frac{|F| + \tau_e(G-F)}{\omega(G-F)} \right\}$$

که در آن مینیمم روی برش یالی F گراف G محاسبه می شود. $G-F$ را زیرگراف القایی از مجموعه یالهای $E(G)-F$ ، $\tau_e(G-F)$ تعداد یالهای موجود در بزرگترین مؤلفه گراف القایی $G-F$ و $\omega(G-F)$ تعداد مؤلفه های گراف القایی $G-F$ در نظر می گیریم. مجموعهٔ یالهای $F \subset E(G)$ را یک T_e–مجموعهٔ گراف G گوییم اگر $T_e(G) = \frac{|F| + \tau_e(G-F)}{\omega(G-F)}$ باشد و هر مؤلفه گراف $G-F$ حداقل یک یال داشته باشد .

در اینجا، پارامتر همبستگی یالی را برای گرافها معرفی می کنیم که پارامتر دیگری برای اندازه گیری آسیب پذیری گرافها می باشد. در ادامه چند ویژگی و همچنین چند کران برای این پارامتر ارائه خواهیم داد. در انتها همبستگی یالی خانواده هایی از گرافها را محاسبه می کنیم .

مفهوم همبستگی را کازن، معظمی و استاکل در[۲۹،۳۰] به عنوان پارامتر اندازه گیر آسیب پذیری و اعتمادپذیری شبکه ها معرفی کردند. از آن پس، همبستگی گرافها به شاخه ای فعال تحقیقاتی، در نظریهٔ گراف تبدیل شد . کازن و همکارانش دو تعریف برای همبستگی گرافها ارائه کردند، همبستگی $T(G)$ و همبستگی یالی $T_e(G)$.

مطابق تعریف، همبستگی گراف در G به صورت

$$T(G) = \min_{A \subset V(G)} \left\{ \frac{|A| + \tau(G-F)}{\omega(G-F)} \right\}$$

بیان می شود که در آن $\tau(G-A)$ نشان دهنده مرتبه (تعداد رأسهای) بزرگترین مؤلفه $G-A$ و $\omega(G-A)$ تعداد مؤلفه های زیرگراف القایی $G-A$ هستند .

به طور مشابه $T_m(G)$ ، همبستگی ترکیبی گراف G به صورت زیر تعریف می شود .

$$T_m(G) = \min_{A \subset E(G)} \left\{ \frac{|A| + \tau(G-A)}{\omega(G-A)} \right\}$$

که در آن $\tau(G-A)$ نشان دهنده مرتبه (تعداد رأسهای) بزرگترین مؤلفه $G-A$ است و $\omega(G-A)$ نیز مطابق معمول تعداد مؤلفه های گراف القایی $G-A$ می باشد .

به این پارامتر ، همبستگی ترکیبی می گوییم ، به نظر می رسد که همبستگی ترکیبی نام مناسبی باشد. پارامترهای $T(G)$ و $T_m(G)$ از ویژگی ها و خصوصیات جالب فراوانی برخوردارند. پس از معرفی این پارامترها محققان بسیاری ، در این باره تحقیق کردند و نتایج مهمی از آنها حاصل شد .

در [۶۵] و [۶۶] ، پیازا و همکارانش از عبارت $\mathrm{T_m(G)}$ به عنوان همبستگی یالی استفاده کردند. امّا این پارامتر با افزودن تعداد یالهای حذف شده به تعداد رأسهای بزرگترین مؤلفه گراف باقی مانده به دست می آید و به نظر می رسد که این کار راضی کننده نباشد. این موضوع باعث شد که معظمی و صالحیان پارامتر جدید $\mathrm{T_e}(G)$ را معرفی کنند.

این پارامتر اندازه گیر آسیب پذیری ، فقط مبتنی بر یالها می باشد. به این خاطر ما آن را از این پس همبستگی یالی می نامیم.

در [۳۰,۲۹]، مفاهیم و ویژگی های اساسی پارامتر همبستگی بیان شد. در [۵۶]، مقایسه ای بین پارامترهای همبستگی، بی نقصی، محکمی و بستگی برای تعدادی از گرافها انجام گرفت. و این مقایسه نشان داد که پارامتر همبستگی، مناسبترین پارامتر برای تمیز آسیب پذیری بیـــن گرافها است.

در این فصل ، نتایجی از همبستگی یالی $T_e(G)$ را بیان می کنیم و سپس نتایج اولیه و کرانهایی برای آن بیان خواهیم کرد .

فرع۵-۱: فرض کنید G یک گراف بوده و H زیرگراف فراگیر G باشد. در این صورت :

$$T_e(H) \le T_e(G)$$

برهان : فرض کنید H زیرگراف G و F زیرمجموعهٔ مینیمم $E(G)$ باشد که $T_e(G)$ را اختیار می کند. در این صورت $\omega(H-F) \ge \omega(G-F)$. بنابراین

$$\frac{1}{\omega(H-F)} \le \frac{1}{\omega(G-F)}$$

لذا $\frac{1}{\omega(H-F)} \le \frac{1}{\omega(H-F)}$.

همچنین داریم : $|\mathrm{F}| + \tau_e(H-F) \le |F| + \tau_e(G-F)$

لذا $\frac{|F| + \tau_e(H-F)}{\omega(H-F)} \le \frac{|F| + \tau_e(G-F)}{\omega(G-F)} = T_e(G)$. بنابراین $T_e(H) \le T_e(G)$.

قضیه ۵-۱ : اگر F یک زیرمجموعه مینیمم $E(G)$ باشد که از آن $T_e(G)$ به دست می آید ، آن گاه هر یال F رأسهایی را از مؤلفه های متمایز $G-F$ به هم متصل می سازد.

برهان : فرض کنید $e = uv$ یالی در F باشد . اگر u و v متعلق به یک مؤلفه $G-F$ باشند، آن گاه اگر $F_1 = F - e$ ، داریم $\omega(G-F_1) = \omega(G-F)$ و در نتیجه

$$T_e(G) \le \frac{|F_1| + \tau_e(G-F_1)}{\omega(G-F_1)}$$

$$= \frac{|F_1| + \tau_e(G-F_1)}{\omega(G-F_1)}$$

$$= \frac{|F| - 1 + \tau_e(G-F_1)}{\omega(G-F)}$$

$$\le \frac{|F| - 1 + \tau_e(G-F) + 1}{\omega(G-F)}$$

$$= T_e(G)$$

و این نشان می دهد که از F_1 نیز $T_e(G)$ به دست می آید. امّا این یک تناقض است چون F_1 زیرمجموعهٔ سره F است.

قضیه ۵-۲ : فرض کنید $\lambda = \lambda(G) \geq 1$ همبندی-یالی G و $e = |E(G)|$ باشد. در این صورت :

$$T_e(G) \geq \min\left\{e, \left\lceil \frac{\lambda}{16}(8e-\lambda) \right\rceil\right\}$$

برهان : فرض کنید $F \subseteq E(G)$ زیرمجموعه ای است به طوری که $G-F$ شامل k مؤلفه باشد. در این صورت $\tau_e(G-F) \geq \frac{e-|F|}{k}$. به ازای $k=1$ ، داریم :

$$\tau_e(G-F)+|F| \geq e-|F|+|F| = e$$

اگر $k>1$ ، آن گاه $|F| \geq \frac{k\lambda}{2}$ ، پس

$$\frac{\tau_e(G-F)+|F|}{k} \geq \frac{\frac{e-|F|}{k}+|F|}{k} \geq \frac{1}{k}\left(\frac{e}{k}+\frac{(k-1)\lambda}{2}\right)$$

عبارت سمت راست نامساوی به ازای $k = \frac{4e}{\lambda}$ مینیمم می شود. لذا حکم به دست می آید.

در اینجا می خواهیم نتایجی از همبستگی-یالی در گرافها را بیان کنیم. ابتدا توجه می کنیم که برای گراف یالی $L(C_n) = C_n$. بنابراین مقادیر همبستگی یالی دورها را می توان از روی همان پارامتر همبستگی به دست آورد بنابراین قضیه زیر را داریم .

قضیه ۵-۳ : فرض کنید C_n یک n-دور باشد و $n>3$ ، آن گاه داریم :

$$T_e(C_n) = \begin{cases} 1+\frac{2}{n} & n \equiv 0 \mod 2 \\ 1+\frac{4}{n-1} & n \equiv 1 \mod 2 \end{cases}$$

متذکر می شویم که اگر G گراف همبند از مرتبه n باشد، آن گاه $L(G)=G$ اگر و تنها اگر $G=C_n$. این موضوع ما را به مشاهدهٔ زیر می رساند.

مشاهده۵-۱ : فرض کنید G گرافی از مرتبه n باشد. اگر G یکریخت با C_n باشد آن گاه $T_e(G)=T(G)$.

از این مشاهده سؤال زیر پدید می آید :

برای چه گرافهای G داریم : $T_e(G)=T(G)$ ؟

ما این پرسش را بعداً پیگیری خواهیم کرد . اکنون نوبت به محاسبهٔ همبستگی یالی گراف کامل K_n است. به نظر می رسد که می توان به سادگی همبستگی-یالی گراف کامل K_n را محاسبه کرد اما واقعیت چیز دیگری است و نیاز به اندکی تلاش دارد.

قضیه ۵-۴ : به ازای هر $n\geq 1$ داریم :

$$T_e(K_n)=\frac{\left\lfloor \frac{n^2}{4} \right\rfloor+\left(\left\lceil \frac{n}{2} \right\rceil \atop 2\right)}{2}$$

برهان : ابتدا چند نماد مناسب را تعریف می کنیم. برای افراز n به جمعوندهای $k_r,...,k_2,k_1$ که $n=k_1+k_2+...+k_r$ و $1\leq k_1\leq k_2\leq ...\leq k_r$ ، گراف $K_{k_1}\cup K_{k_2}\cup ...\cup K_{k_r}$ را با نماد $G(k_1,k_2,...,k_r)$ نمایش می دهیم.

اکنون فرض کنید F مجموعهٔ مینیمال باشد که به ازای آن $T_e(K_n)$ به دست می آید. توجه می کنیم که همگی مؤلفه های K_n-F گرافهای کامل هستند. لذا ، افرازی مثل $n=k_1+k_2+...+k_r$ از n وجود دارد به طوری که $K_n-F=G(k_1,k_2,...,k_r)$. بنابراین

$$T_e(K_n)=\frac{|F|+\left(kr \atop 2\right)}{r}$$

$$= \frac{\sum_{i \neq j} k_i k_j + \binom{kr}{2}}{r}$$

ابتدا ادعا می کنیم که دنبالهٔ $k_r,\ldots,k_2,k_1$ حداکثر دو مؤلفه متمایز دارد. برای این که ، در غیر این صورت، فرض کنید i چنان باشد که $k_1 > k_i > k_r$. در این صورت با در نظر گرفتن مجموعهٔ $F' \subset E(K_n)$ به طوری که $G - F' = G(k_1 - 1, k_2, \ldots, k_i, k_{i+1}, \ldots, k_r)$ داریم :

$$|F'| = \sum_{j \neq 1,i} (k_1 - 1)k_j + \sum_{j \neq 1,i} (k_1 + 1)k_j + (k_1 - 1)(k_1 - 1) + \sum_{\substack{j \neq l \\ j,l \neq 1,i}} k_j k_l$$

در حالیکه $\tau(G - F') = \binom{kr}{2}$.

لذا با ساده کردن عبارتهای فوق داریم :

$$\frac{|F'| + \tau(G - F')}{k} = \sum_{j \neq l} k_j k_l + \binom{kr}{2} + (k_1 - k_i)$$

که یک تناقض است. این تناقض صحت ادعای ما را ثابت می کند .

اکنون، حالتی را در نظر می گیریم که دنبالهٔ $k_r,\ldots,k_2,k_1$ دو مقدار متمایز را اختیار می کند .

فرض کنید $K_n - F = G(a,\ldots,a,b,\ldots,b)$ که در آن α تا مقدار a و β تا مقدار b می گیرند که $a < b$.
فرض کنید $\alpha > 1$ باشد. حال با در نظر گرفتن $G(a-1,a,\ldots,a,a+1,b,\ldots,b)$، مجدداً، همانند قبل به تناقض خواهیم رسید. در نتیجه $\alpha = 1$. به طور مشابه $\beta = 1$. بنابراین $K_n - F = G(a,b)$ که در آن $a + b = n$.

لذا

$$T_e(K_n)=\frac{ab+\binom{b}{2}}{2}$$

اگر $a+1\le b-1$ ، آن گاه همانند قبل با در نظر گرفتن $G(a+1,b-1)$ به یک تناقض می رسیم. بنابراین $K_n-F=G(a,a+1)$ ، و لذا $n=2a+1$ است و در نتیجه ما به مطلوب خود رسیدیم. اگر $a=b$ باشد نتیجه مشابه را خواهیم داشت.

عکس قضیه۵- ۴ نیز برقرار است.

قضیه۵-۵ : اگر G گرافی از مرتبهٔ n و $T_e(G)=\dfrac{\left\lfloor\frac{n^2}{4}\right\rfloor+\binom{\lceil\frac{n}{2}\rceil}{2}}{2}$ آن گاه $G=K_n$.

برهان : فرض کنید $G\neq K_n$. گیریم e یال K_n باشد به طوری که $e\notin E(G)$. فرض کنید F مجموعه ای از $E(K_n)$ باشد به طوری که $T_e(K_n)=\dfrac{|F|+\tau_e(K_n-F)}{\omega(K_n-F)}$. بدون اینکه به کلیت مطلب لطمه ای بخورد، فرض می کنیم که $e\in F$. در این صورت $F_1=F\cap E(G)-\{e\}$ ، خواهیم داشت :

$$T_e(G)=\frac{|F_1|+\tau_e(G-F_1)}{\omega(G-F_1)}$$

$$<\frac{|F_1|+\tau_e(K_n-F)}{\omega(K_n-F)}$$

$$=T_e(K_n)$$

و این اثبات را کامل می کند .

۱۲. مراجع

1. D.R. Woodal, The Binding number of a graph and its Anderson number, J. Combin. Theory B, 15, No. 3 (1973), 225 -255.

2. I. Anderson, Perfect matchings of a graph , J.Combin. Theory 10 (1971) 183-186.
3. C.A. Barefoot, R. Entringer and H. Swart, Vulnerability in graphs – A Comparative survey, J. Combin. Math. Combin. Comput. 1 (1987) 12 – 22.
4. V.G. Kane, S.P. Mohanty and R.S. Hales, Product graphs and binding number, Ars Combin. 11 (1981) 201 – 224.
5. V. Chvátal, Tough graphs and Hamiltonian circuits, *Discrete Math.* 5 (1973)215 – 228.
6. D. Bauer, H.J. Broersma, and H.J. Veldman, Not every 2- tough graph is Hamiltonian, *Discrete Appl. Math.* 99 (2000) 317-321.
7. D. Bauer , S.L. Hakimi, and E. Schmeichel, Recognizing tough graphs is NP- hard**,** *Discrete Appl. Math.* 28 (1990) 191-195.
8. G.A. Dirac , Some theorems on abstract graphs, *Proc. London Math. Soc.*2(1952) 69 – 81 .
9. C.T. Hoáng. Hamiltonian degree conditions for tough graphs, *Discrete Math.* 142(1995) 121 – 139 .
10. F. Harary, The maximum connectivity of a graph, *Proc. Nat. Acad. Sci. U.S.A,* 48 (1962) 1142 – 1146 .
11. K. Ferland, maximum toughness among (n , m) – graphs, *Journal of Combin. Mathematics and Combin. Computing,* 43 (2002) 43 – 55.
12. C.A. Barefoot, R. Entringer and H. Swart, Integrity of trees and powers of cycles, *Congr. Numer.* 58 (1987) 103 – 114 .
13. K.S. Bagga, L.W. Beineke, M.J. Lipman and R.E. Pippert, Edge-integrity : A Survey **,** *Discrete Math.* 124 (1994) no 1-3, 3-12 .
14. W. Goddard, On the vulnerability of graphs, Ph.D. thesis, University of Natal, Durban, S.A. (1989) .
15. W.D. Goddard and H.C. Swart, On the toughness of a graph, Quaestiones Math.13 (1990), 217-232.
16. M.B. Cozzens, D. Moazzami, and S. Stueckle, The Tenacity of a graph**,** *Graph Theory*, *Combinatorics, and Algorithms* (Yousef Alavi and Allen Schwenk eds.) Wiley , New York, (1995), 1111-1122.
17. M.B. Cozzens, D. Moazzami, and S. Stueckle, The Tenacity of the Harary graphs**,** *J.Combin. Math. Combin. Comput.* 16 (1994), 33-56.
18. D. Moazzami, Vulnearability in graph – a comparative survey, *J. Combin. Math.Combin. Comput.* 30 (1999) 23-31.
19. D. Moazzami, B. Salehian, Some results related to the tenacity and existance of K-trees, *Discrete Math.(* to appear in *Discrete Appl. Math.*).
20. D. Moazzami, On Networks with maximum graphical structure, tenacity T and number of vertices p, *J. Combin. Math. Combin. Comput.* 39 (2001) 121-126.

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Graph Theory Applications in R-Hypermodules with some Fuzzy substructures

Fatemeh Niyazi[1]
Department of Mathematics, Semnan University, Semnan, Iran

Razieh Mahjoob
Department of Mathematics, Semnan University, Semnan, Iran

Abstract

In this note, we investigate the association of graphs with R-hypermodules through normal fuzzy subhypermodules. The primary goal of this study is to explore the properties of the associated graph, such as connectedness, completeness, and the presence of Eulerian and Hamiltonian paths.

Keywords: Hypermodule, Normal fuzzy subhypermodule, Regular relation, Graph
AMS Mathematical Subject Classification [2010]: 13D45, 39B42

1 Introduction

In 1934, the French mathematician Marty, in the 8th Mathematical Congress of the Scandinavian countries, for the first time introduced the notion of hyperoperations and then hypergroups as a generalization of the concept of group and used it in different parts of algebra such as noncommutative algebra ([6]). Therefore, we can say that, 1934 is the year of the emergence of the theory of algebraic hyperstructures. On the other hand, the theory of fuzzy sets was introduced by Zadeh, an Iranian professor at Berkeley University, in 1965 ([11]).This theory prompted some mathematicians to investigate the relationship of this theory to other parts of mathematical sciences and engineering.

The first article on fuzzy algebraic structures was introduced by Rosenfeld in 1971, in which he introduced the fuzzy subgroupoid (the subgroup) of a groupoid (group) ([10]). Since then, many researchers have been engaged in extending the concepts and results of abstract algebra based on a broaden framework of fuzzy settings. Also in recent years, a link between the theory of algebraic hyperstructures and the fuzzy theory has been established to give birth to a new concept called the theory of fuzzy hyperstructures.

We know the graph theory has many applications in various sciences such as computer science, image capturing, networking, etc and so some extent papers are to assign a graph to a ring, group, polygroup etc. This helps us to study some properties of these structures by the associated graph (see [1], [2], [3]). Finally, the study of algebraic hyperstructures, using the properties of graph theory became an attractive topic

[1]speaker

among mathematicians, for example, we can refer to the relationship between hypergroups and hypergraphs by Corsini ([4]).

In this note, considering a normal fuzzy subhypermodule μ of an R-hypermodule M and a regular relation depending on μ, we associate a graph to M and investigate some properties of this graph. We also emphasize the concept of normal fuzzy subhypermodules of hypermodules was introduced by Zhan, Davvaz, and Shum ([12]).

First, we recall some basic definitions which are proposed by the pioneers of this subject.

Let H be a nonempty set together with a mapping $\circ : H \times H \longrightarrow P^\star(H)$, where $P^\star(H)$ is the set of all nonempty subsets of H. The algebraic system $(H, \circ)$ is called hypergroupoid. For $A, B \in P^\star(H)$, we define $A \circ B$, by $A \circ B = \bigcup_{\substack{a \in A \\ b \in B}} a \circ b$ and for $x \in H$, we use $x \circ A$ and $A \circ x$ instead of $\{x\} \circ A$ and $A \circ \{x\}$, respectively.

A hypergroupoid $(H, \circ)$ is called semihypergroup if for each $z, y, z \in H$, $x \circ (y \circ z) = (x \circ y) \circ z$ and is called commutative if for each $x, y \in H$, $x \circ y = y \circ x$ and finally a commutative semihypergroup $(H, \circ)$ is called canonical hypergroup ([8]) if the following hypotheses are satisfied:

(i) there exists a unique $0 \in H$ such that $0 \circ x = x$, for all $x \in H$;

(ii) for every $x \in H$, there exists a unique element $x' \in H$ such that $0 \in x \circ x'$. (we call x' the opposite of x).

(iii) for all $x, y, z \in H$, $x \in y \circ z$ implies that $z \in y' \circ x$ and $y \in x \circ z'$.

Let us we recall notions of hyperrings and hypermodules, defined in [12] and [5].

Definition 1.1. A hyperring is an algebraic system $(R, +, \cdot)$ which satisfies the following axioms:

(i) $(R, +)$ is a canonical hypergroup (we shall write $-x$ for x');

(ii) $(R, \cdot)$ is a semigroup having zero as a bilaterally absorbing element;

(iii) the multiplication "." is distributive with respect to the hyperoperation "+".

The hyperring R has a unit element if there exists an element $1 \in R$ such that for all $r \in R$, $r \cdot 1 = 1 \cdot r = x$.

Definition 1.2. A canonical hypergroup $(M, +)$ is called a left hypermodule over a hyperring R if there exists a map $\cdot : R \times M \longrightarrow P^\star(M)$ by $(r, m) \longmapsto r \cdot m$ such that for all $r_1, r_2 \in R$ and $m_1, m_2 \in M$, we have

(i) $r_1 \cdot (m_1 + m_2) = r_1 \cdot m_1 + r_1 \cdot m_2$;

(ii) $(r_1 + r_2) \cdot m_1 = r_1 \cdot m_1 + r_2 \cdot m_1$;

(iii) $(r_1 r_2) \cdot m_1 = r_1 \cdot (r_2 \cdot m_1)$.

A hypermodule M over a hyperring R is called unitary if for all $m \in M$, we have $m \in 1 \cdot m \cap m \cdot 1$.

Throughout this note, R is a hyperring and M is a left hypermodule over R also 'R-hypermodule' means 'left R-hypermodule'. We call a nonempty subset A of an R-hypermodule $(M, +)$ a subhypermodule if $(A, +)$ is an R-hypermodule and A is called normal subhypermodule if $x + A - x \subseteq A$ for all $x \in A$.

Definition 1.3. Let M and M' be two R-hypermodules. A map $f : M \to M'$ is called an R-homomorphism if for all $a, b \in M$ and $r \in R$, we have

$$f(a+b) = f(a) + f(b),\ f(r \cdot a) = r \cdot f(a) \text{ and } f(0) = 0,$$

Where $f(a+b) = \cup\{f(z) : z \in a+b)\}$ and $f(r \cdot a) = \cup\{f(z) : z \in r \cdot a\}$.

Also, f is an isomorphism if f is both injective and surjective and we write $M \cong M'$ if there exists an isomorphism from M to M'.

Let X be a set. By a fuzzy subset of X, we mean a function $\mu : X \to [0,1]$ [11].

For fuzzy subsets μ and ν of X, we say that μ is contained in ν and write $\mu \subseteq \nu$, if for all $x \in X$, $\mu(x) \leq \nu(x)$.

Definition 1.4. [9] Let X and X' be sets, $f : X \to X'$ a function and μ, ν fuzzy subsets of X and X' respectively. The image $f(\mu)$ of μ is a fuzzy subset of X' which is defined by

$$f(\mu)(y) = \begin{cases} \bigvee\limits_{x \in f^{-1}(y)} \mu(x) & if\ \ f^{-1}(y) \neq \emptyset \\ 0 & otherwise \end{cases}$$

for all $y \in M'$, and the inverse image $f^{-1}(\nu)$ of ν is a fuzzy subset of M which is defined by $f^{-1}(\nu)(x) = \nu(f(x))$ for all $x \in M$.

In the following, we recall some notions of fuzzy subhypermodules. ([12]).

Definition 1.5. A fuzzy subset μ of an R-hypermodule M is called fuzzy subhypermodule of M if the following conditions hold:

(i) $\mu(x) \wedge \mu(y) \leq \bigwedge\limits_{\alpha \in x+y} \mu(\alpha)$, for all $x, y \in M$;

(ii) $\mu(x) \leq \mu(-x)$, for all $x \in M$;

(iii) $\mu(x) \leq \bigwedge\limits_{z \in r \cdot x} \mu(z)$, for all $r \in R$ and $x \in M$.

If μ is a fuzzy subhypermodule of M, then it is clear that, $\mu(-x) = \mu(x)$ and $\mu(x) \wedge \mu(y) \leq \bigwedge\limits_{z \in x-y} \mu(z)$ for all $x, y \in M$.

A fuzzy subhypermodule μ of M is called normal if $\mu(y) \leq \bigwedge\limits_{\alpha \in x+y-x} \mu(\alpha)$, for all $x, y \in M$.

Let M be an R-hypermodule. Then, for a fuzzy subset μ of M, the level subset μ_t is defined by $\mu_t = \{x \in M : \mu(x) \geq t\}$, where $t \in [0,1]$.

A fuzzy subhypermodule can be characterized by using its level subsets.

The following Proposition is obvious.

Proposition 1.6. *Let μ be a fuzzy subset of an R-hypermodule M. Then the following statements are equivalent:*

(i) μ is fuzzy subhypermodule of M;

(ii) Each nonempty level subset of μ is subhypermodule of M.

Definition 1.7. Let μ be a normal fuzzy subhypermodule of M. Define the following relation on M:

$x \equiv y (mod\, \mu)$ if and only if there exists $\alpha \in x - y$ such that $\mu(\alpha) = \mu(0)$.

We denote the above equivalence relation by $\mu^\star$.

Let M be an R-hypermodule and ρ an equivalence relation on M. We define the relation $\bar{\rho}$ on $P^*(M)$ as follows:

$$\text{for } A, B \in P^*(M),\ A\bar{\rho}B \Longleftrightarrow \forall a \in A, \exists b \in B, a\rho b \text{ and } \forall b \in B, \exists a \in A, a\rho b.$$

An equivalence relation ρ on M is called regular if for every $x, y \in M$,

$$x\rho y \Longrightarrow x + z\bar{\rho}y + z, \text{ for all } z \in M.$$

Lemma 1.8. *$\mu^\star$ is a regular relation.*

Let $x \in M$ and $\mu^\star[x]$ be the equivalence class of x and $\dfrac{M}{\mu} = \{\mu^\star[x] : x \in M\}$ the set of all equivalence classes of elements of M. Define the hyperoperationd $\oplus$ and $\odot$ as follows:

$$\mu^\star[x] \oplus \mu^\star[y] = \{\mu^\star[z] : z \in \mu^\star[x] + \mu^\star[y]\},\ r \odot \mu^\star[x] = \mu^\star[r \cdot x].$$

We notice that external hyperoperation $\odot$ is not correct, because $\mu^\star[r \cdot x]$ for all $r \in R$ and $x \in M$, is not subset of $\dfrac{M}{\mu}$. We define external hyperoperation $\odot$ as follows:

$$r \odot \mu^\star[x] = \{\mu^\star[z] : z \in r \cdot x\}.$$

Theorem 1.9. *If M is an R-hypermodule, then $(\dfrac{M}{\mu}, \oplus, \odot)$ is an R-hypermodule.*

Lemma 1.10. *Let A be a normal subhypermodule of M and μ a normal fuzzy subhypermodule of M. Then $\mu_{|A}$ is a normal fuzzy subhypermodule of A.*

We remark that the normalization of A in the above Theorem is necessary to prove the normalization of $\mu_{|A}$.

Now, we recall some definitions of graph theory which are needed in this note.

Let X be a graph with the vertex set $V(X)$. Recall that a graph is said to be connected if, for each pair of distinct vertices v and w, there is a finite sequence $v = v_1, \cdots v_n = w$ of distinct vertices where each pair $\{v_i, v_{i+1}\}$ is an edge. Such a sequence is said to be a path. If $v = w$, then a path is called a cycle. A graph in which each pair of distinct vertices is joined by an edge is called a complete graph. A closed path through a graph using every edge once is called an Eulerian circuit and a graph that has such a path is called an Eulerian graph. A graph is called a Hamiltonian graph if it has a cycle that passes through each vertex exactly once.

2 Main results

Let M be an R-hypermodule and μ a normal fuzzy subhypermodule of M. We associated a graph Γ_M^μ to M whose vertices are the elements of M and x and y are adjacent if $x\mu^\star y$ and is denoted by xEy.

Theorem 2.1. *Let μ and ν be normal fuzzy subhypermodules of M with $\mu \subseteq \nu$ and $\mu(0) = \nu(0)$. Then Γ_M^μ is a subgraph of Γ_M^ν.*

The converse of Theorem 2.1 is not true as the following example demonstrates.

Example 2.2. Let us consider the ring $(\mathbb{Z}_4, +_4, \cdot_4) := R$ and $(\{1,3\}, \cdot_4) := G$ be a normal subgroup of R's multiplicative semigroup. By [7], the set $\bar{R} = R/G = \{0, G, 2G\}$ becomes a hyperring if we define the sum and the product of R's any two elements as follows:

$$xG + yG = \{(xp + yq)G : p, q \in G\}, xG \cdot yG = xyG.$$

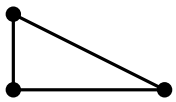
Consider an external composition from $\bar{R} \times \bar{R}$ to $P^\star(\bar{R})$ defined by

$$xG \bullet yG = \{xyG\}, \text{ for every } x, y \in \mathbb{Z}_4.$$

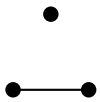
Clearly, $(\bar{R}, +, \bullet)$ is a hypermodule over hyperring $(\bar{R}, +, \cdot)$. Now, let μ and ν be two normal fuzzy subhypermodules $\bar{R}$ defined by

$$\nu(0) = \nu(G) = \nu(2G) = 0, \ \mu(x) = \begin{cases} 1 & x \in \{0, 2G\} \\ 0 & x = G \end{cases}$$

Clearly, $\Gamma^\mu_{\bar{R}}$ is subgraph of $\Gamma^\nu_{\bar{R}}$, $\mu \not\subseteq \nu$ and $\nu(0) \neq \mu(0)$. $\Gamma^\nu_{\bar{R}}$ and $\Gamma^\mu_{\bar{R}}$ are as in follows:



$\Gamma^\nu_{\bar{R}}$



$\Gamma^\mu_{\bar{R}}$

In [12] it is shown that if $f : M \to M'$ is a homomorphism of R-hypermodules and μ a (normal) fuzzy subhypermodule of M, then $f(\mu)$ is a (normal) fuzzy subhypermodule of M', also if $f : M \to M'$ is an epimorphism of R-hypermodules and ν is a (normal) fuzzy subhypermodule of M', then $f^{-1}(\nu)$ is a (normal) fuzzy subhypermodule of M.

Now, we have the following Proposition.

Proposition 2.3. *Let $f : M \to M'$ be an epimorphism of R-hypermodules and μ and ν normal fuzzy subhypermodules of M and M', respectively. Then, the following statements hold:*

(i) There exists a graph homomorphism from Γ^μ_M onto $\Gamma^{f(\mu)}_{M'}$;

(ii) There exists a graph homomorphism from $\Gamma^{f^{-1}(\nu)}_M$ onto $\Gamma^\nu_{M'}$.

We remark that for an R-hypermodule M, if μ is a normal fuzzy subhypermodule of M, the $Ker\, f$ is defined by

$$Ker\, f = \{x \in M : f(x) = \mu^\star[0]\} = \{x \in M : \mu^\star[x] = \mu^\star[0]\},$$

where f is the natural epimorphism from M to $\frac{M}{\mu}$ and $\mu^\star[0]$ is the identity of the hypermodule $\frac{M}{\mu}$. It is also called the Heart of f and is shown by w_M.

Theorem 2.4. *Let μ be a normal fuzzy subhypermodule of M. Then Γ^μ_M is connected if and only if the quotient $\frac{M}{\mu}$ is a trivial hypermodule and $w_M = M$*

Theorem 2.5. *Let μ and ν be normal fuzzy subhypermodules of M and M', respectively with $|w_M| = 1$ and $M \cong M'$. Then Γ^μ_M and $\Gamma^\nu_{M'}$ are isomorphic graphs.*

The converse of Theorem 2.5 is not true as the following example demonstrates.

Example 2.6. consider the ring $(\mathbb{Z}_3, +_3, \cdot_3) := R$ and $(\{1,2\}, \cdot_3) := G$ be a normal subgroup of R's multiplicative semigroup. By Example 2.2, $(\bar{R}, +, \bullet)$ is a hypermodule over hyperring $(\bar{R}, +, \cdot)$. Now, let μ be a normal fuzzy subhypermodule $\bar{R}$ defined by $\mu(0) = \mu(G) = 1$. It is routine to check that $w_M = \{0, G\}$. Clearly, $\Gamma^{\mu}_{\bar{R}} \cong \Gamma^{\mu}_{\bar{R}}$ and $\bar{R} \cong \bar{R}$ but $|w_M| \neq 1$.

Recall that a graph X is called bipartite if its vertex set can be represented as the union of two disjoint sets V_1 and V_2 such that every edge of X connects an element of V_1 with one of V_2. We call V_1, V_2 a bipartition of $V(G)$.

Lemma 2.7. *Let μ be a normal fuzzy subhypermodule of M and M_1 and M_2 are non-empty subsets of M. We denote the bipartite graph $\Gamma^{\mu}_M = (M_1, M_2, E)$ is associated to M and $x_i, y_i \in M_i$, $i = 1, 2$. Then for all $\alpha \in x_i - y_i$ we have $\mu(\alpha) \neq \mu(0)$.*

Theorem 2.8. *Let A be a normal subhypermodule of M and μ a normal fuzzy subhypermodule of M. Then $\Gamma^{\mu_{|A}}_A$ is a subgraph of Γ^{μ}_M.*

Lemma 2.9. *Let μ be a normal fuzzy subhypermodule of M. Then each nonempty level subset of μ is a normal subhypermodule of M.*

Corollary 2.10. *Let μ be a normal fuzzy subhypermodule of M. Then $\Gamma^{\mu_{|\mu_t}}_{\mu_t}$ is a subgraph of Γ^{μ}_M.*

Remark 2.11. Let μ be a normal fuzzy subhypermodule of M. Then there is no correspondence between subgraphs of Γ^{μ}_M and normal fuzzy subhypermodules of M which are included in μ, for example, consider the ring $(\mathbb{Z}_3, +_3, \cdot_3)$. By Example 2.6, $(\bar{R}, +, \bullet)$ is a hypermodule over hyperring $(\bar{R}, +, \cdot)$ and the number of subgraphs $\Gamma^{\mu}_{\bar{R}}$ is equal to 4 but the number of normal fuzzy subhypermodules of $\bar{R}$ is equal to 1 because let

$$\nu(x) = \begin{cases} \alpha & x = 0 \\ \beta & x = G \end{cases}$$

Then we have two following cases.

Case1. If $\alpha \leq \beta$, then $\nu(G) \leq \bigwedge_{\alpha \in G+G-G} \nu(\alpha)$ unconstrained.

Case2. If $\beta \leq \alpha$, then $\nu(0) \leq \bigwedge_{\alpha \in G+0-G} \nu(\alpha)$ unconstrained.

So there is no correspondence between subgraphs of Γ^{μ}_M and normal fuzzy subhypermodules of M which are included in μ.

Remark 2.12. Let μ be a normal fuzzy subhypermodule of M. Then there is no correspondence between subgraphs of Γ^{μ}_M and each nonempty level subset of μ. For example, consider the ring $(\mathbb{Z}_3, +_3, \cdot_3)$. By Example 2.6, $(\bar{R}, +, \bullet)$ is a hypermodule over hyperring $(\bar{R}, +, \cdot)$ and the number of subgraphs $\Gamma^{\mu}_{\bar{R}}$ is equal to 4 but $\mu_0 = \{xG \in \bar{R} : \mu(xG) \geq 0\} = \{0, G\}$ and hence there is no correspondence between subgraphs of Γ^{μ}_M and each nonempty level subset of μ.

Theorem 2.13. *Let μ be a normal fuzzy subhypermodule of M. Then Γ^{μ}_M is Eulerian if and only if for all $x \in M$, $|\mu^{\star}[x]|$ has an odd number and Γ^{μ}_M is a connected graph.*

Lemma 2.14. *For an R-hypermodule M, let μ be a normal fuzzy subhypermodule of M such that, $|V(M)| \geq 3$ and $|\frac{M}{\mu}| = 1$. Then Γ^{μ}_M is a Hamiltonian graph. Moreover, if $|V(M)|$ has an odd number, then Γ^{μ}_M is both Eulerian and Hamiltonian.*

Acknowledgment

The authors are deeply grateful to the referees for their careful reading of the manuscript and helpful suggestions. The first author would like to thank her note supervisor.

References

[1] A. Abdollahi, S. Akbari and H. R. Maimani, *Noncommuting graph of a group*, Journal of Algebra, **298(2)** (2006), 468-492.

[2] I. Beck, *Coloring of commutative rings*, Journal of Algebra, **116(1)** (1988), 208-226.

[3] E. A. Bertram, *Some applications of graph theory to finite groups*, Discrete Mathematics, **44(1)** (1983), 31-43.

[4] P. Corsini, *Hypergroups and Hypergraphs*, Algebra Universalis, **35** (1996), 548-555.

[5] M. Krasner, *A class of hyperring and hyperfields*, International Journal of Mathematical Sciences, **2** (1983), 307–312.

[6] F. Marty, *Sur une generalization de la notion de groups*, 8th Congress Math. Scandinaves, Stockholm, (1934).

[7] Ch. Massouros, *Free and cyclic hypermodules*, Annali di Mathematica Pura ed Applicate, (1988), 153-166.

[8] J. Mittas, *Hypergroupes canoniques*, Math Balkanica, **2** (1979), 165–179.

[9] J. N. Mordeson, K. R. Bhutni and K. A. Rosenfeld,*Fuzzy group theory*, Studies in Fuzziness and Soft Computing; Springer-Verlag:Berlin/Heidelberg, Germany, (2005), 61-89.

[10] A. Rosenfeld, *Fuzzy groups*, Journal of Mathematical Analysis and Applications, **35** (1971), 512-517.

[11] L. A. Zadeh, *Fuzzy sets*, Information and Control, (1965), 338–353.

[12] J. Zhan, B. Davvaz, K. P. Shum, *On fuzzy isomorphism theorems of hypermodules*, (2007), 1053–1057.

e-mail: fniyazi@semnan.ac.ir
e-mail: mahjoob@semnan.ac.ir

9th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
December. 25-26, 2024

Some Algebraic Properties of a Class of Circulant Graphs Which is Constructed from Cycles

Bahman Askari[1]

Department of Mathematics, Qorveh Branch, Islamic Azad University, Qorveh, Iran

Fataneh Karimi

Department of Mathematics, Lorestan University, Khorram-Abad, Iran

Abstract

Circulant graphs are Cayley graphs over a cyclic group. In this paper, we study some algebraic properties of the Möbius ladder M_n, that is, a circulant graph on $\mathbb{Z}_{2n}$. In particular, we study the spectrum, the chromatic number, the independent number and the automorphism group of M_n.

Keywords: Scott topology, Automorphism group, Chromatic number, Independent number, Spectra.
AMS Mathematical Subject Classification [2010]: 05C25, 94C15, 05C50, 05E18

1 Introduction

2 Introduction

In this paper, a graph $\Gamma = \Gamma(V, E)$ is considered as a simple undirected graph with vertex-set $V(\Gamma) = V$, and edge-set $E(\Gamma) = E$. An automorphism of Γ is a bijection mapping $\alpha : V \longrightarrow V$, such that preserve the adjacency of vertices. The set of all automorphisms of Γ with respect to composition operation forms a group, which called the automorphism group of Γ, and denoted by $\mathrm{Aut}(\Gamma)$. We denote the group of all integers modulo n by $\mathbb{Z}_n$. Let S be a non-empty subset of $\mathbb{Z}_n$ such that $0 \notin S$, $-S = S$. Then the circulant graph Γ over $\mathbb{Z}_n$ is a graph with vertex-set $\mathbb{Z}_n$, and two vertices a, b are adjacent if and only if $b - a \in S$. The most famous types of circulant graphs are cycles. A cycle of order n, is denoted by C_n, and it is a graph with vertex set $\{0, 1, \ldots, n-1\}$, in which i adjacent to j if and only if $j - i = \pm 1 \pmod n$. It is obvious that the cycle of order n is a circulant graph on $\mathbb{Z}_n$, with $S = \{\pm 1\}$. On the other hand, by [6] we have $\mathrm{Aut}\,(C_n) = D_{2n}$, the dihedral group of order $2n$.

The spectrum of C_n has been determined in [2]. Determining the automorphism groups and the spectrum of some families of graphs, has been the subject of various research papers, and some of the recent works are [4, 5, 7, 8, 9]. In this paper, we study a class of circulant graphs on $\mathbb{Z}_{2n}$, which are called Möbius ladders, and we denote them by M_n. The Möbius ladder M_n is the circulant graph $Cay(\mathbb{Z}_{2n}, S)$, where $S = \{1, -1, n\} = \{1, 2n-1, n\}$. In this paper, we determine the spectrum, the chromatic number, the independent number and the automorphism group of M_n.

[1] speaker

3 Preliminaries

For all terminologies and notations not defined here, we follow [2, 6, 10, 3]. Let G denotes an arbitrary group, and $S \subset G$ with $1 \notin S$, and $S = S^{-1}$. The Cayley graph Γ on G is denoted by $\Gamma = Cay(G, S)$, is a graph with vertex-set G, and two vertices g, h are adjacent if and only if $g^{-1}h \in S$. The set S is called, the connection set of Γ. As we saw in the introduction, for every subset S in $\mathbb{Z} \setminus \{0\}$, with $-S = S$, the Caylay graph $Cay(\mathbb{Z}_n, S)$ is called a circulant graph. Furthermore, for cycle C_n we have, $C_n = Cay(\mathbb{Z}_n, \{\pm 1\})$.
Let Γ be a graph with vertex-set $\{v_1, v_2, \cdots, v_n\}$. Then the adjacency matrix A of Γ is a $n \times n$ matrices with A_{ij}, the ij'th array of A, is equal to 1 if v_i adjacent to v_j, and $A_{ij} = 0$ otherwise.
For a graph Γ with adjacency matrix A, the (adjacency) spectrum of Γ is the spectrum of the matrix A. If $\lambda_1, \cdots, \lambda_n$ are distinct eigenvalues of Γ with multiplicity $m_1, \cdots, m_n$ respectively, then we write the spectrum of Γ as

$$\mathrm{Spec}(\Gamma) = \left\{ \begin{array}{cccc} \lambda_1, & \cdots, & \lambda_n \\ m_1, & \cdots, & m_n \end{array} \right\}.$$

In some situations, computing the eigenvalues of a matrix is equal to finding the zeros of its characteristic polynomial. For matrices with the order greater than two, this is false. Generally, the best way to obtain eigenvalues, is to find eigenvectors: If $Ax = \lambda x, x \neq 0$, then λ is an eigenvalue of A, and x is an eigenvector of A corresponding to λ [2, chapter 8]. When we work with graphs, there is an additional refinement. We can suppose that an eigenvector is a real function f on the vertices. Then, if at any vertex v you sum up the values of f on its neighboring vertices, you should get λ times the values of f at v. Formally:

$$\sum_{w \in N(v)} f(w) = \lambda f(v).$$

In this paper, we think to eigenvectors and eigenvalues in this manner. We have the following lemma for the spectrum of a given Caylay graph which is constructed on an Abelian group [7].

Lemma 3.1. *Let G be an Abelian group, and $S \subseteq G \setminus \{0\}$ such that $S = -S$. Then for every character χ of the G, there is an eigenvalue $\lambda(\chi)$ for $\Gamma = Cay(G, S)$, which is defined as follows:*

$$\lambda(\chi) = \sum_{b \in S} \chi(b).$$

For example, from Lemma 3.1. and [2, 5], we can compute the spectrum of C_n, like as follows:

(a) If n is odd

$$\mathrm{Spec}\ (C_n) = \left\{ \begin{array}{cccc} 2 & 2cos\frac{2\pi}{n} & \cdots & 2cos\frac{(n-1)\pi}{n} \\ 1 & 2 & \cdots & 2 \end{array} \right\};$$

(b) If n is even

$$\mathrm{Spec}\ C_n = \left\{ \begin{array}{ccccc} 2 & cos\frac{2\pi}{n} & \cdots & cos\frac{(n-2)\pi}{n} & -2 \\ 1 & 2 & \cdots & 2 & 1 \end{array} \right\}$$

Definition 3.2. The Möbius ladder M_n is the circulant graph $Cay(\mathbb{Z}_{2n}, S)$, where $S = \{1, -1, n\} = \{1, 2n-1, n\}$.

For example, the graph M_4 can be displayed as follows:

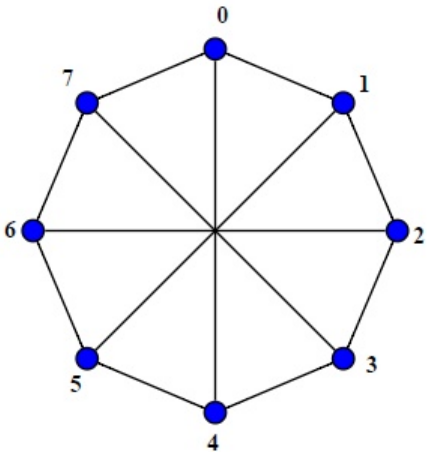


Figure 1: Möbius ladde M_4

Definition 3.3. Let Γ be a graph. A subset of vertices that induces an empty subgraph of Γ is called an independent set of Γ. The size of the largest independent set of the graph Γ is called independent number of Γ, denoted by $\alpha(\Gamma)$.

A proper coloring of a graph Γ, is a mapping from $V(\Gamma)$ into some finite set of colors such that no two adjacent vertices are assigned the same color. If Γ can be properly colored with a set of k colors, then we say that Γ is k-colorable.

Definition 3.4. Let Γ be a graph. The least value of k for which Γ is a k-colorable graph, is the chromatic number of Γ, and is denoted by $\chi(\Gamma)$.

Let $\Gamma(V, E)$ and $\Lambda(V', E')$ be two graphs. The mapping $\beta : V \longrightarrow V'$ is a homomorphism from Γ to Λ if $v, w \in V(\Gamma)$ are adjacent in Γ, then $\beta(v), \beta(w) \in V'(\Lambda)$ are adjacent in Λ. An isomorphism between Γ and Λ is a bijection homomorphism $\beta : V \longleftrightarrow V'$ with $v, w \in V(\Gamma)$ are adjacent in Γ, if and only if $\beta(v), \beta(w) \in V'(\Lambda)$ are adjacent in Λ.
An automorphism of a graph Γ is an isomorphism from Γ to itself. The set of all automorphisms of Γ, with composition of functions, is called the automorphism group of Γ and denoted by $\mathrm{Aut}(\Gamma)$.
Now, let Γ be a graph with automorphism group $G = \mathrm{Aut}(\Gamma)$. For vertex $v \in V(\Gamma)$, let G_v denote the stabilizer subgroup of vertex v; that is, the subgroup of G containing of those automorphism that fix v. From first isomorphism theorem, we know that:

$$[G : G_v] = \frac{|G|}{|G_v|} \leq |V(\Gamma)|.$$

The graph Γ is called vertex-transitive if $G = \mathrm{Aut}(\Gamma)$ acts transitively on $V = V(\Gamma)$. In other words, for any two vertices $v, w \in V(\Gamma)$ there is an automorphism $\alpha \in \mathrm{Aut}(\Gamma)$ such that $\alpha(v) = w$. Now if Γ is a vertex-transitive graph, then for each vertex $v \in V(\Gamma)$, we have

$$\frac{|G|}{|G_v|} = |V| \Longrightarrow |G| = |G_v||V|.$$

In [6] it is proved that $\mathrm{Aut}(C_n) = D_{2n}$, the dihedral group of order $2n$, which is defined as follows:

$$D_{2n} = \langle \{\alpha, \beta | \alpha^n = \beta^2 = 1, \quad \beta^{-1}\alpha\beta = \alpha^{-1}\} \rangle.$$

4 Main Results
Spectra, Independent number and chromatic number

In this section, we study spectrum, independent number and chromatic number of M_n. We determine the spectrum of M_n by using Lemma 3.1.

For the group $\mathbb{Z}_n$, the set of all group homomorphism $\chi_a : x \longmapsto \omega^{ax}$ is the set of all characters of $\mathbb{Z}_n$, where $a, x \in \mathbb{Z}_n$ and ω is a primitive n-th root of unity.

Now from Lemma 3.1. We know that for every $r \in \{0, 1, \ldots, 2n-1\}$, the eigenvalues of M_n are as follows;

$$\lambda_r = \sum_{j=\pm 1, n} \omega^{rj}, \quad r = 0, 1, \ldots, 2n-1.$$

where ω is a primitive $2n$-th root of unity. Then for each $r = 0, \cdots, 2n-1$, we have

$$\lambda_r = \omega^r + \omega^{-r} + \omega^{dr} = \lambda_r^{'} + (-1)^r,$$

where $\lambda_r^{'} = \sum_{j=\pm 1} \omega^{rj}$ is an eigenvalue of C_{2n}. If there exist $r, s \in \{0, \cdots, 2n-1\}$ such that $\lambda_r = \lambda_s$, then we have $\lambda_r^{'} + (-1)^r = \lambda_s^{'} + (-1)^s$. By an easy calculation we see that $\lambda_r^{'} = -1, 1, 0, -4$, which is a contradiction ($\lambda_r^{'}$ is an eigenvalue of C_{2n}). Then we see that the spectrum of M_n, is as follows;

$$\mathrm{Spec}(M_d) = \begin{Bmatrix} 3 & cos\frac{\pi}{n} - 1 & \cdots & 2cos\frac{(n-1)\pi}{n} + 1 & -3 \\ 1 & 2 & \cdots & 2 & 1 \end{Bmatrix}.$$

Independent number

Proposition 4.1. *Let $n \geqslant 3$. Then $\alpha(M_n) = n-1$ if n is even and $\alpha(M_n) = n$ if n is odd.*

Proof. Let $M = \{x_1, \cdots, x_t\}$ be an independent subset in M_n. We can assume that, $x_1 < x_2, \cdots < x_t$. Then, it is obvious that

$$x_i - x_{i-1} \geq 2, \ x_i - x_{i-1} \neq 2n-1, \ n,$$

for all $i \in \{1, \cdots, t\}$. We now have,

$$2t \leq (x_1 - 0) + \sum_{i=2}^{t} (x_i - x_{i-1}) \leq 2n$$
$$\Longrightarrow 2t \leq 2n \Longrightarrow t \leq n.$$

Note that, t is maximum whenever

$$x_i - x_{i-1} = 2, \text{ for all } i \in \{1, \cdots, t\}.$$

In fact, if there is a $j \in \{1, \cdots, t\}$ such that $x_j - x_{j-1} \geq 3$, then

$$2(t-1)+3 \leq (x_1 - 0) + \sum_{i=2}^{t}(x_i - x_{i-1}) \leq 2n$$
$$\Longrightarrow 2t+1 \leq 2n \Longrightarrow t \leq n - \frac{1}{2}.$$

Since t is an integer, then $t \leq n-1$. We now have the following two cases:

- Case 1 : n is odd. Then the set $M_1 = \{0, 2, 4, \cdots, 2n-2\}$ is an independent set of size n, and so $\alpha(M_n) = n$.
- Case 2 : $2m = n$ is even. Note that in this case we can not have $x_{i+1} - x_i = 2$, for every $i,\ 0 < i < n$. Because, if $x_0 = 0$, then $x_m = 2m = n \in M_1$, and hence M_1 is not an independent set. On the other hand, if $x_0 = 1$, then $x_m = 2m+1 = n+1 \in M_2 = \{1, 3, ..., 2n-1\}$, and hence M_2 is not an independent set (note that $n+1$ is adjacent to 1). Also, note that if $x_0 \geq 2$, then $t \leq n-1$. Since, there is a $j \in \{1, \cdots, t\}$, such that $x_j - x_{j-1} \geq 3$, then $t \leq n-1$. Now, note that the set $\{0, 2, 4, ...n-2, n+1, n+3, ...2n-3\}$, has $n-1$ elements and is an independent set. Therefore, if n is an even integer, then $\alpha(M_n) = n-1$.

□

Chromatic number

Proposition 4.2. *[6] The chromatic number of a graph Γ is the least integer r, such that there is a homomorphism from Γ to K_r.*

Lemma 4.3. *[6] Let Γ be a graph, then we have the following two cases:*

(1) The graph Γ is bipartite if and only if it contains no odd cycle.

(2) If Γ is a bipartite graph with at least one edge, then $\chi(\Gamma) = 2$ and vice versa.

Proposition 4.4. *The chromatic number of M_n is 2 if n is odd, and is 3 if n is even.*

Proof. Suppose that n is odd, then we show that M_n is a bipartite graph. We let $V(M_n) = S_1 \bigcup S_2$, where

$$S_1 = \{x |\ x \text{ is odd}\}, \qquad S_2 = \{x |\ x \text{ is even}\} \bigcup \{0\}.$$

Then, there are no edges between vertices in S_1, and also, there are no edges between vertices in S_2. In fact, if $x_1, x_2 \in S_1$ (or S_2), subsequently $x_1 - x_2 = 2k \notin \{\pm 1, n\}$, where k is an integer. On the other hand, $S_1 \bigcap S_2 = \phi$, then in this case M_n is bipartite. So from lemma 4.3, for odd n we have $\chi(M_n) = 2$.
Now let n be even. Then we can prove that M_n is not a bipartite graph. Let $V(M_n) = \{0, \cdots, 2n-1\}$. Then the cycle $0, 1, (n+1), (n+2), \cdots, 0$ is an odd cycle of length $n+1$. Hence, by lemma 4.3, M_n is not a bipartite graph, and finally, $\chi(M_n) \geq 3$.
We now prove that $\chi(M_n) = 3$. Let x_1, x_2 be two adjacent vertices of M_n, then $x_1 - x_2 \in \{\pm 1, n\}$, and $x_1 = x_2 \pm 1$ or $x_1 = x_2 \pm n$. Let $x_1 = x_2 \pm 1$, subsequently x_1, is even if and only if x_2 is odd and vice versa. Let $x_1 = x_2 \pm n$, so x_1 is even if and only if x_2 is even. Let K_3 be the complete graph on 3 vertices with vertex-set $\{0, 1, 2\}$, then there exist a homomorphism $\alpha : M_n \longrightarrow K_3$, such that

$$\alpha : x \longmapsto \begin{cases} 0 & x \text{ even and } x \neq n; \\ 1 & x \text{ odd}; \\ 2 & x = n. \end{cases}$$

If x_1, x_2 are two adjacent vertices such that $x_1, x_2 \neq n$, then w.l.g we may assume that $\alpha(x_1) = 0$ and $\alpha(x_2) = 1$, and $\alpha(x_1)$ is adjacent to $\alpha(x_2)$. Now, if x_1, x_2 are two adjacent vertices such that $x_1 = n$, then $x_2 = n - 1$ or $x_2 = n + 1$, so $\alpha(x_2) = 0$ and $\alpha(x_1)$ is adjacent to $\alpha(x_2)$ and if $x_2 = 0$, then $\alpha(x_2) = 0$ and $\alpha(x_1)$ is adjacent to $\alpha(x_2)$. We now conclude that $\chi(M_n) = 3$. □

5 Automorphism Group

In this section, we determine the automorphism group of Möbius ladders $M_n = Cay(\mathbb{Z}_{2n}, S)$, where $S = \{1, 2n - 1, n\}$. We start with the following lemma; that is the main tool for determining the automorphism group of ladders.

Lemma 5.1. *Let $M_n = Cay(\mathbb{Z}_{2n}, S)$ denotes the Möbius ladder of order $2n$, where $S = \{\pm 1, n\}$ and $n > 3$. Let $x, y, s_1, s_2 \in S$, $x + y \not\equiv 0 \ (mod\ 2n)$ and $x \neq y$. If $x + y \equiv s_1 + s_2 \ (mod\ 2n)$, then $\{x, y\} = \{s_1, s_2\}$.*

Proof. Since $x, y, s_1, s_2 \in S$, then $x + y, s_1 + s_2 \in \{n + 1, n - 1\}$. subsequently, $\{x, y\} = \{n, 1\}$ or $\{x, y\} = \{n, -1\}$. We now have the following two cases:

(i) Let $\{x, y\} = \{n, 1\}$. Since $x + y \equiv s_1 + s_2 \ \ (mod\ 2n)$, then $\{s_1, s_2\} = \{n, 1\}$, and so $\{x, y\} = \{s_1, s_2\}$.

(ii) Let $\{x, y\} = \{n, -1\}$. Since $x+y \equiv s_1+s_2 \ \ (mod\ 2n)$, then $\{s_1, s_2\} = \{n, -1\}$, and so $\{x, y\} = \{s_1, s_2\}$.

□

We consider the permutation $\pi = (0\ 1\ 2\ \cdots\ 2n - 1) \in S_{2n}$, and we show that $\pi \in \mathrm{Aut}(M_n)$. Suppose that x, y are two adjacent vertices in M_n. Then, $x = y \pm 1 \ (mod\ 2n)$ or $x = y + n \ (mod\ 2n)$. If π act on x we have:

$$x^\pi = x + 1 \ (mod\ 2n) = (y \pm 1) + 1 \text{ or } (y + n) + 1 \ (mod\ 2n).$$

On the other hand, both $(y \pm 1) + 1$ and $(y + n) + 1$ are adjacent to $y + 1$. Then, $x + 1$ adjacent to $y + 1$ and so x^π adjacent to y^π, thus $\pi \in \mathrm{Aut}(M_n)$.
We now prove that the permutation $\beta \in S_{2n}$ is an automorphism of M_n, where

$$\beta : x \longmapsto 2n - x \ (mod\ 2n)$$

For vertex x in M_n, if x adjacent to y, then $x = y \pm 1 \ (mod\ 2n)$ or $x = y + n \ (mod\ 2n)$. Let β act on x, then

$$x^\beta = 2n - x = 2n - (y \pm 1) \text{ or } n - (y + n) = (2n - y) \pm 1 \text{ or } (2n - y) + n$$

By the above, it is easy to check that $D_{2k} \leq \mathrm{Aut}(M_n)$, where $k = 2n$. In fact, the equality is hold.

Theorem 5.2. *Let $k = 2n \geq 6$. Then for Möbius ladder $M_n = Cay(\mathbb{Z}_{2n}, S)$ we have,*

$$\mathrm{Aut}(M_n) = D_{2k},$$

where $S = \{\pm 1, n\}$.

Proof. Let $G = \mathrm{Aut}(M_n)$ and $f \in G_0$. We show that $f \in \mathrm{Aut}(\mathbb{Z}_{2n})$. In fact

$$f(m1) = mf(1), \text{ for each } m > 0.$$

Let $x, y \in S$ with $x \neq y$ and $x + y \neq 0$. Then, $x + y - x = y \in S$ so that $\{x + y, x\},\ \{x + y, y\} \in E(M_n)$ and $\{f(x + y), f(x)\},\ \{f(x + y), f(y)\} \in E(M_n)$. Then, we have

$$f(x + y) = f(x) + s_1,\ f(x + y) = f(y) + s_2, \text{ where } s_1, s_2 \in S.$$

Note that $N(0) = S$, where $N(x)$ is the set of all neighbours of $x \in V(\Gamma)$. Let $u \in S$, then

$$\{f(0), f(u)\} = \{0, f(u)\} \in M_d \Longrightarrow f(u) \in S,$$

and so $f(S) = S$. On the other hand, $f(x) + s_1 = f(y) + s_2$ and thus, $f(x) - f(y) = s_2 - s_1$. Also, $x \neq y$ and $f \in Sym(\mathbb{Z}_n)$, hence $f(x) \neq f(y)$. Then, by lemma 5.1

$$\{f(x), -f(y)\} = \{-s_1, s_2\}.$$

If $f(x) = -s_1$, then $f(x + y) = f(x) + s_1 = 0 = f(0)$, and thus $x + y = 0$, which is a contradiction. Then we have $f(x) = s_2$ and $f(x + y) = f(y) + s_2 = f(y) + f(x)$.
Let $u \in S$, we will show that $f(2u) = 2f(u)$. If $2u \neq 0$, then we have

1. if $u = -1$, then $2u - u = -1$;
2. if $u = 1$, then $2u - u = 1$;
3. if $u = d$, then $2u - u = d$.

Then, $2u - u \in S$ and $\{2u, u\} \in E(M_n)$, thus $\{f(2u), f(u)\} \in E(M_n)$. subsequently, there is a $s \in S$, such that $f(2u) = f(u) + s$. Since $f(S) = S$, there is $s_1 \in S$ such that $f(s_1) = s$, and thus $f(2u) = f(u) + s_1$. We now show that $f(s_1) = f(u)$. If $f(s_1) \neq f(u)$, then from $f^{-1} \in G_0$ we have

$$2u = f^{-1}(f(2u)) = f^{-1}(f(u) + f(s_1)) = f^{-1}(f(u)) + f^{-1}(f(s_1)) = u + s_1.$$

Then, $u = s_1$ and so $f(u) = f(s_1)$, which is a contradiction. Then for $u \in S$ and $2u \neq 0$ we conclude that $f(2u) = 2f(u)$.
Now, let $2u = 0$. Then $u = d$ and so, if $f(u) = u$, then we conclude that

$$2f(u) = 2u = 0 = f(0) = f(2u).$$

If $f(u) = y \neq u$, then $2f(u) = 2y \neq 0$ and thus

$$f^{-1}(2y) = 2f^{-1}(y) = 2u \Longrightarrow f(2u) = f(f^{-1}(2y)) = 2y = 2f(u).$$

We now show that if $x \in S$, $f(-x) = -f(x)$. Let $2x \neq 0$, then $x \neq -x$ and thus $f(x) \neq f(-x)$. So, if $t = f(x) + f(-x) \neq 0$, subsequently $f^{-1}(t) = f^{-1}(f(x) + f(-x)) = f^{-1}(f(x)) + f^{-1}(f(-x)) = x - x = 0 = f^{-1}(0)$. Then, $t = 0$ which is a contradiction, and in this case, we conclude that $f(x) + f(-x) = 0$, hence $f(-x) = -f(x)$.
If $2x = 0$, then $x = -x$ and

$$f(2x) = f(0) = 0 = 2x \Longrightarrow f(x) = -f(x) = -f(-x) \Longrightarrow f(-x) = -f(x).$$

Thus, we have proved that $f(-x) = -f(x)$, for all $x \in S$. Now, let $v, w \in S$ such that $v + w = 0$, then

$$v = -w \Longrightarrow f(v+w) = f(0) = 0$$
$$= f(v) - f(v) = f(v) + f(-v) = f(v+w).$$

Now for arbitrary $v, w \in S$ we show that $f(v+w) = f(v) + f(w)$. By the above we have

$$f(1+(-1)) = f(1) + f(-1) \text{ and } f(d+d) = f(2d) = 2f(d) = f(d) + f(d).$$

We now, prove by induction on positive integer d that $f(d1+v) = df(1) + f(v)$, where $v \in S$.
If $d = 1$, we prove that $f(1+v) = f(1) + f(v)$ for all $v \in S$. Let the assertion be true for $l < d$ and $y = d1 + v$, if $1 + v = 0$, then

$$0 = f(0) = f(1+v) = f(1) + f(v) \text{ and } y = (d-1)1.$$

By induction assumption

$$f(y) = f(d1+v) = f((d-1)1) = (d-1)f(1)$$
$$= (d-1)f(1) + f(1) + f(v) = df(1) + f(v).$$

Now, let $1 + v \neq 0$ and $v \neq 1$. Note that $\{d1+v, d1\}, \{d1+v, (d-1)1+v\} \in E(M_n)$, then

$$\{f(d1+v), f(d1)\}, \{f(d1+v), f((d-1)1+v)\} \in E(M_n).$$

Then there are $u, w \in S$ such that

$$f(d1+v) = f(d1) + f(u),\ f(d1+v) = f((d1-1)+v) + f(w)$$
$$\Longrightarrow f(d1) + f(u) = f((d-1)1+v) + f(w).$$

By induction assumption we have

$$f(d1) = f((d-1)1+1) = (d-1)f(1) + f(1) = df(1) \Longrightarrow f(1) + f(u) = f(v) + f(w)$$
$$\Longrightarrow 1 + u = v + w \Longrightarrow 1 - v = w - u.$$

Then, by lemma 5.1, $\{1, -v\} = \{w, -u\}$. If $1 = -u$, then $f(u) = -f(1)$ and so, $f(d1+v) = df(1) - f(1) = f((d-1)1)$ and $d1 + v = (d-1)1 \Longrightarrow 1 + v = 0$, which is a contradiction. Therefor, $1 = w$ implies that $v = u$. We now have $f(d1+v) = f(d1) + f(u) = f(d1) + f(v) = df(1) + f(v)$.
Now, let $v = 1$. Since $\{(d+1)1, d1\} \in E(M_n)$, hence $\{f((d+1)1), f(d1)\} \in E(M_n)$ and thus,

$$f((d+1)1) = f(d1) + f(u),\ \ u \in S.$$

If $u \neq 1$, then

$$f(d1) + f(u) = f(d1+u) \Longrightarrow (d+1)1 = d1 + u \Longrightarrow u = 1,$$

and this is a contradiction. Then, $u = 1$ and we have

$$f((d+1)1) = f(d1) + f(u) = (d+1)f(1).$$

Then, for all $d \in \mathbb{Z}^+$ and all $v \in S$, we proved that

$$f(d1+v) = df(1) + f(v).$$

In particular, for all positive integer m we have, $f(m1) = mf(1)$. On the other hand; we know that $\mathbb{Z}_{2n} = \langle 1 \rangle$, then for all $a, b \in \mathbb{Z}_{2n}$, we have $a = l.1, b = k.1$, where $l, k \in \mathbb{Z}^+$. Thus, by the above assertion $f(a+b) = (a+b)f(1) = f(a) + f(b)$, and so $f \in \mathrm{Aut}(\mathbb{Z}_{2n})$.
On the other hand, $f(S) = S$. Subsequently $f(1) \in S$. Since 1 is a generator for $\mathbb{Z}_{2n}$, then $f(1)$ is a generator for $\mathbb{Z}_{2n}$. We know that $\mathbb{Z}$ have only two elements $1, -1$ in S as generators. Then, $f(1) \in \{1, -1\}$, and thus $|G_0| = 2$. Then,

$$|G| = 2n|G_0| = 4n \Longrightarrow |\mathrm{Aut}(M_n)| = 4n$$
$$\mathrm{Aut}(M_n) = D_{2k}, \text{ where } k = 2n.$$

□

References

[1] Basic M, Ilic A. *On the automorphism group of integral circulant graphs*, Electron. J. Combin, 2011; 18/1, p68.

[2] Biggs N. *Algebraic Graph theory, (Second edition)*, Cambridge University Press, Cambridge, 1996.

[3] Bollobás B. *Almost every graph has reconstruction number three*, J. Graph Theory, 1990; 14/1:1-4.

[4] Ganesan A , *Automorphisms of Cayley graphs generated by transposition sets*, http://arxiv.org/abs/1303.5974v2.

[5] Godsil C. *Eigenvalues of Graphs and Digraphs*, Linear Algebra Appl, 1982; 46: 43-50.

[6] Godsil C, Royal G. *Algebraic graph theory*, Graduate Texts in Mathematics, 207, Springer-Verlag, New york, 2001.

[7] Kovàcs I. *On automorphisms of circulant digraphs on p^m Vertices, p an odd Prime*, Linear Algebra Appl, 2001; 356: 231-252.

[8] Mirafzal SM. *On the symmetries of some classes of recursive circulant Graphs*, Trans. Comb, 2014; 3/1: 1-6.

[9] Mirafzal SM. *On the automorphism groups of regular hyper-stars and folded hyper-stars*, Ars Combinatoria, 2015; 123: 75-86.

[10] Rotman JJ. *An introduction to the theory of groups*, 4th ed, 148, Springer-Verlag, New York, 1995.

e-mail: dr.askari.b@gmail.com
e-mail: fatanehkarimi1367@gmail.com