Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.47974/JIOS-1941

A useful encryption of discrete graphs on symmetric groups

Sufyan Asif *
Department of Mathematics
University of the Punjab
Lahore 54590
Pakistan

and

Department of Mathematics
The Islamia University of Bahawalpur
Bahawalpur 63100
Pakistan

M. Khalid Mahmood †
Department of Mathematics
University of the Punjab
Lahore 54590
Pakistan

Abstract

In recent years, graph theory has become much more popular due to its wide range of applications in almost every field of interest. Especially, it plays an integral role in cryptography and coding theory to develop new security systems. In this article, we introduce and investigate novel discrete graphs arising from symmetric groups and incorporate these graphs to communicate confidential messages via an interesting encryption. These newly defined discrete graphs are termed as Order Incongruent Simple Graphs (OISG). The vertices of these graphs are the permutations of the symmetric groups, and edges are defined via

* *ORCID-ID:* **0009-0002-2940-495X**
† *ORCID-ID:* **0000-0002-1071-2808**

* *E-mail:* **sufyan.asif@iub.edu.pk (Corresponding Author)**
† *E-mail:* **khalid.math@pu.edu.pk**

modular arithmetic. Many fascinating structures and characterizations of these graphs are proposed and proved using congruences from number theory.

Subject Classification (2020): *05C25, 05C75, 05C50.*

Keywords: *Symmetry groups, Order incongruent graph, Modular arithmetic, Cryptography.*

1. Introduction

Graph theory plays a dynamic role in the field of mathematics as well as in other fields of science. To analyze and visualize the data, graphs play a primary role. The complex data sets can be visualized to observe trends and relationships among certain data sets with the assistance of graphs. The complex interconnected systems enable the analysis of connectivity of different entries. Graphs provide a visual display to study the dependencies between the data points. Graphical models help to solve the linear programming-based problems. Graphs are versatile and effective in nature regarding the analysis of the complex networks. It provides the basis for many significant algorithms, including those for sorting, searching, and optimization. Adjacency matrices, heaps, and trees are a few examples of data structures that rely on graphs for effective data organization and retrieval. It is crucial for analyzing networks, such as the internet, social networks, and computer networks.

Symmetric groups are of great importance in algebra as well as in other fields of mathematics like combinatorics, algebraic topology, and mathematical physics. For examining the symmetry and structures of different mathematical systems, the symmetry of groups provides a powerful framework. In chemistry, group theory is used to understand the symmetry and bonding of molecules. Group theory can be used to study a crystal's structure and characteristics. It is also used in cryptography and coding theory. Cryptographic algorithms use symmetric groups, especially when examining ciphers that rely on permutations. Error-correcting and error-detecting codes can be designed using symmetric groups. Researchers are also employing pure mathematics to construct graphs, especially in rings, groups, and number theory [1, 4-6]. The solutions of the cubic congruences of the form $y^3 \equiv b(mod\ p)$, where p is a rational prime, are examined in [7]. New classes of graphs based on power functions over moduli were described by Mahmood et al. [8]. Using these graphs, the solutions of congruences of p^{th} power over various residue classes have been suggested where p is an odd prime, and for any positive integer n, the number of components are also enumerated. Sufyan et al. introduced and investigated a novel class of graphs by using congruence over a set of moduli and explored several characteristics of moduli-based graphs [9, 10]. Al-Kaseasbeh and Erfanian investigated several characteristics of graphs arising from the coset of groups. The diameter, girth, planarity, and outer planarity of these graphs are explored in [11]. Aneela et al. introduced and investigated novel graphs based on

cyclic groups of order p [12]. For dihedral groups D_{2n} of order $2n$, commuting and non-commuting graphs are discussed in [13]. In [2, 3], graph theory has been employed to introduce interesting applications in cryptography.

This paper is organized in the following manner: Section 1 provides the fundamentals of algebraic graphs and graphs based on the concepts of number theory. Section 2 comprises the basic definitions and results used in this article. In Section 3, we proposed novel graphs, namely order-incongruent simple graphs, and discussed their structural characterization. These novel graphs are introduced over the symmetric group S_n. Finally, as an application of newly defined graphs, we incorporate our proposed graphs in cryptography.

2. Preliminaries And Basic Definitions

A graph is a pair $G(V,E)$, V is the set of nodes or vertices, while E represents the edge set. The number of the nodes in the graph is termed the order of the graph. The total number of edges associated with the vertex is called the degree of the vertex. The number of edges involved in the graph is called the size of the graph. The graph is said to be connected if there is always a path between each pair of vertices. A graph is termed the regular graph if each vertex of the graph is of the same degree. The maximum distance between the vertex v and any other vertex of the graph is defined as the eccentricity of the vertex v. The minimum eccentricity is called the radius of the graph, while the maximum eccentricity is termed the diameter of the graph. The subset of vertices of the graph whose eccentricity is equal to the radius of the graph is called the center of the graph. The subset of vertices of the graph is called the periphery if the eccentricity of each vertex is equal to the radius of the graph. A subset of the vertices of the graph is termed the independent set if no pair of the vertices in the subset is adjacent. A subset D of vertices of the graph is called the dominating set if each vertex in the complement of D is adjacent to at least one vertex of the D. The number of vertices in the smallest dominating set of the graph is termed the domination number of the graph. For the graph of order n, the closure graph $C(G)$ is a graph that is obtained by joining those vertices of G whose degree sum is at least n. A Hamiltonian graph has a cycle that visits each vertex exactly once without making any repetition. An open neighborhood of a vertex includes those vertices that are directly connected through an edge to the given vertex. It's the same as the immediate friends of a vertex. In graph theory, a closed neighborhood of a vertex means a subset of the vertex set that consists of that vertex and all those vertices that are linked to that vertex. It's similar to a group of friends that involves the vertex and all its immediate neighbors. The average distance of the graph of order n, which is denoted by $\mu(G)$, is $\frac{1}{\binom{n!}{2}}\sum_{u,v\in G)} d(u,v)$.

3. Order Incongruent Simple Graphs of S_n

The groups defined on symmetries are an important topic in algebra. These groups provide a structure to narrate and understand symmetries in certain shapes, objects, and parameters. In this section, we define graphs arising from symmetric groups and investigate their various properties and characteristics.

Definition 3.1: Let S_n be a symmetric group of order $n!$. The order incongruent simple graph(OICSG) $\Gamma_i^o(S_n)$ of S_n is a simple graph in which elements of S_n are the vertices. And an arbitrary pair of vertices α and β is adjacent if and only if $n!\,||\alpha| - |\beta|$. Figure *1* depicts the idea of order incongruent simple graph defined on S_3.

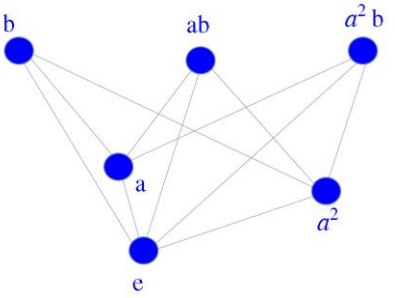

Figure 1
Order incongruent simple graph of S_3.

The following observations directly followed from the definition of an order incongruent simple graph of S_n.

Remarks 3.2:

(a) The identity permutation is always adjacent to non identity permutations of the symmetric group. That is, the degree of identity permutation is $n! - 1$.

(b) If α and β are two distinct permutations of S_n such that $\alpha\beta = e$, e is the identity permutation, then there is no edge between α and β.

Theorem 3.3: *For $n \geq 3$, $\Gamma_i^o(S_n)$ can never be a regular graph.*

Proof: Let S_n be a non-abelian symmetric group of order $n!$ where $n \geq 3$. Since there is only one identity permutation of unique order, there must be an element $e \neq \alpha \in S_n$ such that $\alpha\beta = e$ for some $\beta \in S_n$ and $\alpha \neq \beta$. Thus, α and β lose at least one edge in $\Gamma_i^o(S_n)$. Therefore, $deg(e) > deg(\alpha) = deg(\beta), \forall \alpha, \beta \in S_n$. This leads to the fact that $\Gamma_i^o(S_n)$ can never be a regular graph.

Proposition 3.4: $\Gamma_i^o(S_n)$ is always a connected graph.

Proof: Since $deg(e) = n! - 1$, it has no isolated vertex. Therefore, $\Gamma_i^o(S_n)$ is always a connected graph.

Next, Theorem 3.5 tells about the degree of an arbitrary cycle in S_n.

Theorem 3.5: *If $\gamma = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ is an arbitrary cycle of length k in S_n and k divides $n!$. Then in $\Gamma_i^o(S_n)$,*

$$deg(\gamma) = |S_n| - \frac{n!}{k(n-k)!} - n_k$$

where n_k denotes the number of the permutations as the products of cycles having order k.

Proof: Let S_n be a finite group of symmetries defined on a set of n elements. All of its elements are permutations including cyclic permutations and products of cyclic permutations. Further, let γ denote an arbitrary cycle of length k, which is a positive integer. Also S_n has exactly $\frac{1}{k}({}^nP_k)$ different cycles of length k. But there are also some permutations that are not cycles themselves but are the product of the cycles with certain length. We consider that n_k denotes those permutations that are in the form of a product of cycles with order k. Then by definition of order incongruent simple graph, each vertex of length k is not adjacent to each other, as every integer is self-congruent for any modulus m. As cycles of same length are conjugate, no edge exists between them. We conclude that

$$\begin{aligned} deg(\gamma) &= |S_n| - \frac{1}{k}({}^nP_k) - n_k \\ &= |S_n| - \frac{1}{k}\left[\frac{n!}{(n-k)!}\right] - n_k \end{aligned}$$

Theorem 3.6: *In $\Gamma_i^o(S_n)$ if $\gamma = (\beta_1, \beta_2, \dots, \beta_m)$ is an arbitrary vertex of $\Gamma_i^o(S_n)$ then $deg(\gamma) \leq deg(e)$, where e denotes the identity permutation in S_n.*

Proof: Let S_n be a group of symmetries and $\Gamma_i^o(S_n)$ represents the order incongruent simple graph of S_n. And $(\beta_1, \beta_2, \dots, \beta_m)$ be an arbitrary cycle of length m. If $(\beta_1, \beta_2, \dots, \beta_m)$ is an identity permutation, then its degree is $n! - 1$. And the result is true. If $(\beta_1, \beta_2, \dots, \beta_m)$ is a non identity permutation of S_n, then by Theorem 3.5 its degree is $|S_n| - \frac{1}{m}\left[\frac{n!}{(n-m)!}\right] - n_m$. Also $\frac{1}{m}\left[\frac{n!}{(n-m)!}\right] \geq 1$ and $n_m \geq 0$. This implies that

$$|S_n| - \frac{1}{m}\left[\frac{n!}{(n-m)!}\right] - n_m < |S_n| - 1$$

Therefore,

$$deg(\gamma) < deg(e)$$

Theorem 3.7: *For* $3 \leq n \leq 6$,

$$\begin{aligned} m(\Gamma_i^o(S_n)) = \frac{1}{2}\Bigg[& n! - 1 + \sum_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \frac{n!}{2^i i!(n-2i)!}\left(n! - \sum_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \frac{n!}{2^i i!(n-2i)!}\right) \\ & + \sum_{1 \leq j \leq \left\lfloor \frac{n}{3} \right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!}\left(n! - \sum_{1 \leq j \leq \left\lfloor \frac{n}{3} \right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!}\right) \\ & + \frac{n!}{4}\left\lfloor \frac{n}{4} \right\rfloor\left(n! - \frac{n!}{4}\left\lfloor \frac{n}{4} \right\rfloor\right) + \frac{n!}{5}\left\lfloor \frac{n}{5} \right\rfloor\left(n! - \frac{n!}{5}\left\lfloor \frac{n}{5} \right\rfloor\right) + \frac{n!}{6}\left\lfloor \frac{n}{3} \right\rfloor\left\lfloor \frac{n}{5} \right\rfloor\left(n! - \frac{n!}{6}\left\lfloor \frac{n}{3} \right\rfloor\left\lfloor \frac{n}{5} \right\rfloor\right)\Bigg]. \end{aligned}$$

$$m(\Gamma_i^o(S_n)) = \frac{1}{2}[n! - 1 + \sum_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor} \frac{n!}{2^i i!(n-2i)!} - \sum_{1\le j\le\left\lfloor\frac{n}{2}\right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!} - \frac{n!}{4}\left\lfloor\frac{n}{4}\right\rfloor - \frac{n!}{5}\left\lfloor\frac{n}{5}\right\rfloor - \frac{n!}{6}\left\lfloor\frac{n}{3}\right\rfloor\left\lfloor\frac{n}{5}\right\rfloor].$$

Proof: Let S_n be a symmetric group of order $n!$ and $3 \le n \le 6$, and $\Gamma_i^o(S_n)$ be an order incongruent simple graph defined on S_n. For $3 \le n \le 6$, the following order elements exist in S_n: 1, 2, 3, 4, 5, and 6. And there exists $\sum_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor} \frac{n!}{2^i i!(n-2i)!}$ elements of order 2 in S_n, so the degree of order 2 elements in $\Gamma_i^o(S_n)$ is $n! - \sum_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor} \frac{n!}{2^i i!(n-2i)!}$. Also the number of elements of order 3 in S_n are $\sum_{1\le j\le\left\lfloor\frac{n}{3}\right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!}$ so the degree of order 3 elements is $n! - \sum_{1\le j\le\left\lfloor\frac{n}{3}\right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!}$. Similarly there exists, $\frac{n!}{4}\left\lfloor\frac{n}{4}\right\rfloor$, $\frac{n!}{5}\left\lfloor\frac{n}{5}\right\rfloor$, and $\frac{n!}{6}\left\lfloor\frac{n}{3}\right\rfloor\left\lfloor\frac{n}{5}\right\rfloor$ elements of order 4,5, and 6. Therefore, the degrees of order 4,5, and 6 elements are $n! - \frac{n!}{4}\left\lfloor\frac{n}{4}\right\rfloor$, n!- $\frac{n!}{5}\left\lfloor\frac{n}{5}\right\rfloor$, and $n! - \frac{n!}{6}\left\lfloor\frac{n}{3}\right\rfloor\left\lfloor\frac{n}{5}\right\rfloor$ respectively. By the Handshaking Lemma, the size of the order incongruent simple graph $\Gamma_i^o(S_n)$ of S_n is,

$$\begin{aligned} m(\Gamma_i^o(S_n)) &= \frac{1}{2}\sum_{u,v\in S_n} deg(u,v) \\ &= \frac{1}{2}\Bigg[n! - 1 + \sum_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor} \frac{n!}{2^i i!(n-2i)!}\left(n! - \sum_{i=1}^{\left\lfloor\frac{n}{2}\right\rfloor} \frac{n!}{2^i i!(n-2i)!}\right) \\ &+ \sum_{1\le j\le\left\lfloor\frac{n}{3}\right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!}\left(n! - \sum_{1\le j\le\left\lfloor\frac{n}{3}\right\rfloor} \frac{n!}{(3^j j!)(1^{n-3i})(n-3i)!}\right) \\ &+ \frac{n!}{4}\left\lfloor\frac{n}{4}\right\rfloor\left(n! - \frac{n!}{4}\left\lfloor\frac{n}{4}\right\rfloor\right) + \frac{n!}{5}\left\lfloor\frac{n}{5}\right\rfloor\left(n! - \frac{n!}{5}\left\lfloor\frac{n}{5}\right\rfloor\right) \\ &+ \frac{n!}{6}\left\lfloor\frac{n}{3}\right\rfloor\left\lfloor\frac{n}{5}\right\rfloor\left(n! - \frac{n!}{6}\left\lfloor\frac{n}{3}\right\rfloor\left\lfloor\frac{n}{5}\right\rfloor\right)\Bigg]. \end{aligned}$$

Theorem 3.8: In an order incongruent simple graph of S_n, $N[e] = S_n$ where e represents the identity permutation in S_n.

Proof: Let us consider the group of symmetries on n elements and $\Gamma_i^o(S_n)$ be an order incongruent simple graph of S_n. Also, the edges are produced among those elements $s, t \in S_n$ whose orders are incongruent under moduli $n!$. Moreover, if the order of an element is incongruent to the order of remaining elements, then it lies in the neighborhood of these elements. Since identity is always unique, so its order is incongruent with the order of the remaining elements. Thus, each non-identity element lies in the neighborhood of the identity permutation. Therefore, $N(e) = S_n - \{e\}$. And the closed neighborhood of e is $N[e] = N(e) \cup \{e\} = S_n$.

Theorem 3.9: *The radius of* $\Gamma_i^o(S_n)$ *is always* 1.

Proof: Let $\Gamma_i^o(S_n)$ be an order incongruent simple graph of S_n. As the radius of the of the graph is the minimum eccentricity of all vertices of $\Gamma_i^o(S_n)$. It is well known that there exists a unique identity permutation in S_n, so it is directly linked with all the vertices of the $\Gamma_i^o(S_n)$. This leads to the fact that the identity permutation has minimum eccentricity, which is 1. That is,

$$rad(\Gamma_i^o(S_n)) = 1.$$

Theorem 3.10: *The domination number of the $\Gamma_i^o(S_n)$ is always 1.*

Proof: For $n \geq 3$, $\Gamma_i^o(S_n)$ always contains an identity permutation of order 1 such that it is adjacent to all remaining vertices of the graph. So, the set containing only the identity permutation is the smallest subset of $\Gamma_i^o(S_n)$ that satisfies the condition of the dominating set. Thus, the domination number of the $\Gamma_i^o(S_n)$.

Theorem 3.11: *The closure of the order incongruent simple graph of $S_3, C(\Gamma_i^o(S_3)) \cong K_6$.*

Proof: Let S_3 be a symmetric group of order 6. And $\Gamma_i^o(S_3)$ represents the order incongruent simple graph of $S_3 =< a, b: a^3 = b^2 = 1, ba = a^{-1}b >$ as shown in Figure 1. It is also depicted from the Figure 1 that the minimum degree of any vertex is 3. Next, to construct the closure graph of $\Gamma_i^o(S_3)$, we add some extra edges produced from those pair of non adjacent vertices $v_1, v_2 \in \Gamma_i^o(S_3)$ that satisfies

$$deg(v_1) + deg(v_2) \geq 6$$

Also, the only pair of non adjacent vertices of $\Gamma_i^o(S_3)$ are $(a, a^2), (b, ab), (ab, a^2b)$ and (b, a^2b). And

$$deg(a) + deg(a^2) = 8 > |S_3|$$

Therefore, an edge between a and a^2 is produced. Moreover, for the rest of the pairs of vertices, the sum of their degrees is 6. Therefore, 3 more edges are added to $\Gamma_i^o(S_3)$. That is all non-adjacent vertices become adjacent. This completes the proof.

Theorem 3.12: $\Gamma_i^o(S_3)$ always contains a Hamiltonian path.

Proof: Let $\Gamma_i^o(S_3)$ be an order incongruent simple graph of order 6. It is Hamiltonian, if the degree of each vertex is greater than or equal to $\frac{|(\Gamma_i^o(S_3))|}{2}$. Figure 1 shows that $deg(e) = 5$, $deg(a) = deg(a^2) = 4$, and $deg(b) = deg(ab) = deg(a^2) = 3$, which implies that, $deg(v) \geq \frac{|(\Gamma_i^o(S_3))|}{2}$. Thus, $\Gamma_i^o(S_3)$ is Hamiltonian.

Theorem 3.13: *The $diam(\Gamma_i^o(S_n)) = 2$.*

Proof: Consider a symmetric group S_n of order $n!$, and $\Gamma_i^o(S_n)$ be an order incongruent simple graph defined on S_n. There are two possibilities: either an

arbitrary pair of vertices is adjacent or not. If the vertices are adjacent, then their distance is 1, and if the vertices are not adjacent, then $deg(e) = n! - 1$ implies that these vertices are adjacent via the identity element. Therefore, diameter of $\Gamma_i^o(S_n)$ is 2.

Theorem 3.14: *The center of the order incongruent simple graph $\Gamma_i^o(S_n)$ consists of identity element only.*

Proof: Let $\Gamma_i^o(S_n)$ be an order incongruent simple graph of S_n, of order $n!$. Surely, those vertices of $\Gamma_i^o(S_n)$ constitute the center of the graph whose eccentricity is identical to the radius of $\Gamma_i^o(S_n)$. By Theorem 3.9 $rad(\Gamma_i^o(S_n)) = 1$. This implies that the vertices that lie in the center must be adjacent to the remaining vertices of the graph. The definition of an order incongruent simple graph assures that there is only one element e that is adjacent to the remaining vertices. Thus, the center of $\Gamma_i^o(S_n)$ has only identity permutation.

Theorem 3.14 implies the following corollary.

Corollary 3.15: *The $Per(\Gamma_i^o(S_n)) = S_n - e$.*

Theorem 3.16: *For* $3 \leq n \leq 6$,

$$\beta(\Gamma_i^o(S_n)) = \begin{cases} \sum_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \frac{n!}{(2^i.i!)1^{(n-j)}(n-j)!} & , \ if\ n \in \{3,4\}, \\ \frac{n!}{n-1} & , \ if\ n = 5, \\ \frac{2n!}{n} & , \ if\ n = 6.a \end{cases}$$

where $\beta(\Gamma_i^o(S_n))$ denotes the vertex independence number of $\Gamma_i^o(S_n)$.

Proof: Let S_n be a group of symmetries of order $n!$. Now to discuss the independence number β of $\Gamma_i^o(S_n)$. We find the largest independent set of vertices of $\Gamma_i^o(S_n)$. The definition of an order incongruent simple graph reveals that the elements of identical orders constitute the independent set. To find the largest independent set among them is the set of elements of the same order that are maximum in numbers.

Case 1: For $n = 3,4$, the set of cycles of length 2 and product of cycles of length 2 is the largest set that contains the elements of the same orders. And the number of elements of order 2 in S_n are $\sum_{i=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \frac{n!}{(2^i.i!)1^{(n-j)}(n-j)!}$. Thus, it is the vertex independence number of $\Gamma_i^o(S_n)$, if $n = 3$ or 4.

Case 2: If $n = 5$, then it is obvious that the largest set of elements of the same order is the set of cycles of length 4. As there are $\frac{n!}{n-1}$ cycles of length 4 in S_4. So, in this case independence number is $\frac{n!}{n-1}$.

Case 3: If $n = 6$, then the largest set that contains the elements of the same order, is the set of cycles of length 6 and product of $2-$cycles and $3-$cycles. And its cardinality is $\frac{2n!}{n}$. Hence, the result is proved.

Theorem 3.17: *For an order incongruent simple graph $\Gamma_i^o(S_n)$ of S_n,*

$$\mu(\Gamma_i^o(S_n)) = \frac{2(n!-2)}{(n!)}[n! - 1 + \sum j(n! - j + 2)]$$

where $\mu(\Gamma_i^o(S_n))$ denote the average distance of $\Gamma_i^o(S_n)$ and j denotes the number of elements of the same order.

Proof: Let S_n be a periodic group. And $\Gamma_i^o(S_n)$ is an order incongruent simple graph of S_n. Next, we observe the distances of all vertices of this graph. For this, we distribute the whole vertices into two parts, one of the identity permutation and the other one with non-identity permutations .

Case 1: If the vertex is an identity permutation, then by the definition of order incongruent simple graph of S_n, it is adjacent to the remaining vertices of the graph. So the sum of distances of identity permutation from other vertices is $n! - 1$.

Case 2: When the vertex is a non-identity element of S_n of some order. Let j denote the number of vertices that are the elements of S_n of identical order. Then each such j number of vertices is directly linked to the remaining $n! - j$ vertices. Therefore, the sum of distances of such j elements is $j(n! - j)$. As these j vertices are not adjacent to each other, the distance among these vertices is 2. And the sum of the distances among them is $2j$. The sum of total distances of j vertices that are elements of identical orders of S_n is $j(n! - j + 2)$. Therefore, the sum of distances of non-identity elements is

$$\sum j(n! - j + 2)$$

And,

$$\sum_{u,v\in\Gamma_i^o(S_n)} d(u,v) = n! - 1 + \sum j(n! - j + 2)$$

Thus, the average distance of $\Gamma_i^o(S_n)$ is

$$\begin{aligned}\mu(\Gamma_i^o(S_n)) &= \frac{1}{\binom{n!}{2}}\sum_{u,v\in\Gamma_i^o(S_n)} d(u,v),\\ &= \frac{2(n!-2)}{(n!)!}[n! - 1 + \sum j(n! - j + 2)].\end{aligned}$$

4. Application: A Useful Encryption Via Proposed Graph

The order incongruent simple graph of symmetric groups has many applications, especially it plays a crucial role in cryptography. Encryption and decryption are fundamental techniques that are the backbone of cyber security. This section makes it familiar to communicate a secret message via encryption and decryption by incorporating order incongruent simple graphs.

Example 4.1: Consider the order incongruent simple graph of S_3 in Fig. 1. Its adjacency matrix A is

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

The degree matrix of S_3 is

$$B = \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix}$$

Take

$$C = A + B = \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 0 & 1 & 1 & 1 \\ 1 & 0 & 4 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 & 0 \\ 1 & 1 & 1 & 0 & 3 & 0 \\ 1 & 1 & 1 & 0 & 0 & 3 \end{bmatrix}$$

The Laplacian matrix of the order incongruent simple graph of S_3 is

$$L = \begin{bmatrix} 5 & -1 & -1 & -1 & -1 & -1 \\ -1 & 4 & 0 & -1 & -1 & -1 \\ -1 & 0 & 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & 3 & 0 & 0 \\ -1 & -1 & -1 & 0 & 3 & 0 \\ -1 & -1 & -1 & 0 & 0 & 3 \end{bmatrix}$$

In this example, we want to encrypt and decrypt the secret message " GROUPS". First we write the alphabets with the integers modulo 26.

This gives, 7 18 15 21 16 19 and $a \equiv b(modm)$ if and only if $a = b + mk$ for some k. If we assume $m = 7$ and $a = 7, 18, 15, 21, 16, 19$ then the values of b are $0, 4, 1, 0, 2,$ and 5 while the values of k become $1, 2, 2, 3, 2$ and 2. Suppose the diagonal matrices corresponding to values of b and k are labeled as D and E respectively, then

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix} \quad E = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

To encrypt the message, we take

$$F = C + E = \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 0 & 1 & 1 & 1 \\ 1 & 0 & 4 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 & 0 \\ 1 & 1 & 1 & 0 & 3 & 0 \\ 1 & 1 & 1 & 0 & 0 & 3 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 1 & 8 & 0 & 1 & 1 & 1 \\ 1 & 0 & 5 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 & 0 \\ 1 & 1 & 1 & 0 & 5 & 0 \\ 1 & 1 & 1 & 0 & 0 & 8 \end{bmatrix}$$

Now we encrypt this message into the following form

$$P = DF + L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 0 & 1 & 1 & 1 \\ 1 & 0 & 4 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 & 0 \\ 1 & 1 & 1 & 0 & 3 & 0 \\ 1 & 1 & 1 & 0 & 0 & 3 \end{bmatrix}$$

$$+ \begin{bmatrix} 5 & -1 & -1 & -1 & -1 & -1 \\ -1 & 4 & 0 & -1 & -1 & -1 \\ -1 & 0 & 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & 3 & 0 & 0 \\ -1 & -1 & -1 & 0 & 3 & 0 \\ -1 & -1 & -1 & 0 & 0 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 10 & 0 & 0 & 0 & 0 & 0 \\ 1 & 20 & 0 & 1 & 1 & 1 \\ 1 & 0 & 14 & 1 & 1 & 1 \\ 2 & 2 & 2 & 12 & 0 & 0 \\ 1 & 1 & 1 & 0 & 13 & 0 \\ 1 & 1 & 1 & 0 & 0 & 19 \end{bmatrix} (mod\ 26)$$

Thus, in the previous step, our message was transformed into a ciphertext. To decrypt this ciphertext into original text, we proceed with the following procedure. Firstly, we take

$$P - L = \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 2 & 16 & 0 & 2 & 2 & 2 \\ 2 & 0 & 10 & 2 & 2 & 2 \\ 3 & 3 & 3 & 9 & 0 & 0 \\ 2 & 2 & 2 & 0 & 10 & 0 \\ 2 & 2 & 2 & 0 & 0 & 16 \end{bmatrix}$$

In the next step, ciphertext is converted into the following form:

$$Q = D^{-1}(P - L) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 2 & 16 & 0 & 2 & 2 & 2 \\ 2 & 0 & 10 & 2 & 2 & 2 \\ 3 & 3 & 3 & 9 & 0 & 0 \\ 2 & 2 & 2 & 0 & 10 & 0 \\ 2 & 2 & 2 & 0 & 0 & 16 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 0 & 1 & 1 & 1 \\ 1 & 0 & 4 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 0 & 0 \\ 1 & 1 & 1 & 0 & 3 & 0 \\ 1 & 1 & 1 & 0 & 0 & 3 \end{bmatrix}$$

In the next step, the cipher is converted into the following form:

$$S = Q - C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

The final step of the decryption, which converts the ciphertext into original text, is

$$7D + S = \begin{bmatrix} 7 & 0 & 0 & 0 & 0 & 0 \\ 0 & 18 & 0 & 0 & 0 & 0 \\ 0 & 0 & 15 & 0 & 0 & 0 \\ 0 & 0 & 0 & 21 & 0 & 0 \\ 0 & 0 & 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 & 0 & 19 \end{bmatrix}$$

The diagonal of the above matrix is $7,18,15,21,16,$ and 19 which implies the text "GROUPS".

5. Conclusion

New graphs on symmetric groups are investigated. The structures of the proposed graphs, and many interesting characteristics are presented and proved. Finally, these newly defined graphs have been incorporated to introduce interesting ciphers to secure secret communications.

6. Conflict of Interest

The authors of this manuscript have no conflict of interest.

7. Data Statement

This work comprises the numerical data that is not from any data site.

References

[1] A. S. Alali, S. Ali, N. Hassan, A. M. Mahnashi, Y. Shang, and A. Assiry, Algebraic structure graphs over the commutative ring Z_m: exploring topological indices and entropies using M-polynomials, *Mathematics,* vol. 11, no. 18, p. 3833, (2023).

[2] T. Domada, S. A. Kumar, G. Ashok, and D. C. Kumari, Super-encryption with Pell-Lucas matrices and graphs via Laplace transformations, *J. Harbin Eng. Univ.,* vol. 44, no. 8, (2023).

[3] T. Domada, G. Ashok, S. A. Kumar, and D. C. Kumari, Super-encryption technique of graphs via matricial approach, *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. 1215-1222, (2024).

[4] A. G. Syarifudin, D. P. Malik, and I. G. A. W. Wardhana, Some characterization of coprime graph of dihedral group D_{2n}, in *J. Phys.: Conf. Ser.,* vol. 1722, no. 1, p. 012051, (2021).

[5] J. Friedman, On Cayley graphs on the symmetric group generated by transpositions, *Combinatorica*, vol. 20, no. 4, pp. 505-519, (2000).

[6] L. Somer and M. Krek, On a connection of number theory with graph theory, *Czechoslovak Math. J.,* vol. 54, pp. 465-485, (2004).

[7] D. Namli, Some results on cubic residues, *Int. J. Algebra,* vol. 9, pp. 245-249, (2015).

[8] M. H. Mateen, M. K. Mahmmod, D. Alghazzawi, and J. B. Liu, Structures of power digraphs over the congruence equation $x^y \equiv y (\mathrm{mod}\ m)$ and enumerations, *AIMS Math.*, vol. 6, no. 5, pp. 4581-4596, (2021).

[9] S. Asif, M. K. Mahmood, A. S. Alali, and A. A. Zaagan, Structures and applications of graphs arising from congruences over moduli, *AIMS Math.*, vol. 9, no. 8, pp. 21786-21798, (2024).

[10] S. Asif and M. K. Mahmood, Structural properties of the graphs arising from congruences over set of moduli, *JP J. Algebra Number Theory Appl.,* vol. 64, no. 1, pp. 81-98, (2025).

[11] S. Al-Kaseasbeh and A. Erfanian, A bipartite graph associated to elements and cosets of subgroups of a finite group, AIMS Math., vol. 6, no. 10, pp. 10395-10404, (2021).

[12] Aneela, M. K. Mahmood, and D. Ahmad, Order structured graphs of cyclic groups and their classification, *VFAST Trans. Math.,* vol. 12, no. 1, pp. 220-233, (2024).

[13] M. U. Romdhini, A. Nawawi, and C. Y. Chen, Neighbors degree sum energy of commuting and non-commuting graphs for dihedral groups, *Malays. J. Math. Sci.,* vol. 17, no. 1, pp. 53-65, (2023).

Received August, 2024