The p-Cayley Graph of Cyclic Group of Order pqr

Athirah Zulkarnain,[1,a)] Nor Haniza Sarmin,[1,b)] Hazzirah Izzati Mat Hassim,[1,c)] and Ahmad Erfanian[2,d)]

[1]*Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 UTM, Johor Bahru, Johor, Malaysia.*

[2]*Department of Pure Mathematics, Faculty of Mathematical Sciences and Center of Excellence in Analysis on Algebraic Structures, Ferdowsi University of Mashhad, Mashhad, Iran.*

[a)]Corresponding author: athirah5@graduate.utm.my

[b)]nhs@utm.my

[c)]hazzirah@utm.my

[d)]erfanian@um.ac.ir

Abstract. A Cayley graph of a group with respect to a subset S is constructed based on that subset. Meanwhile, the p_i-Cayley graph is constructed using a subset comprising elements of prime power order within the group, where p_i is a prime number dividing the group's order. The set of vertices for these graphs is G, with two distinct vertices, g and h, being adjacent if gh^{-1} is in S. The objectives of this paper are to construct the p_i-Cayley graph for a cyclic group of order pqr concerning a subset containing elements of order p, and to determine their properties, including the diameter and chromatic number.

INTRODUCTION

The Cayley graph, introduced by Arthur Cayley in 1878 [1], is a graph constructed based on the subset S of the group. The vertices of the Cayley graph are the elements in group G, while the edges are formed by the adjacency between two distinct vertices g and h. Specifically, g and h are considered adjacent if $gh^{-1} \in S$. A newly introduced type of Cayley graph in 2021 is the p_i-Cayley graph [2]. It differs from the standard Cayley graph in its subset construction, which specifically includes elements with prime power order for each prime.

There have been numerous recent developments of Cayley graphs, including the identification of new variations or their applications in real-life scenarios. In 2019, Bussaban [3] explored Cayley graphs for gyrogroups, establishing the construction of this graph and several of its properties. In 2020, Fakrorri et al. [4] studied the relative Cayley graph of finite groups, focusing on its connectivity and certain forbidden structures. In 2022, Behajaina et al. [5] investigated the Cayley graph of finite groups, concentrating on integrality, distance integrality, and the powers of distances within the graphs. Aikawa [6], in 2023, applied Cayley graphs to explore hash function problems in cryptography. Finally, also in 2023, Naemah and Erfanian [7] introduced a new type of Cayley graph called the generalized Cayley graph. They specifically concentrated on exploring the structure and properties of this generalized Cayley graph when it forms a complete graph.

In this paper, the p_i-Cayley graph is constructed for a cyclic group of order pqr with respect to a subset containing elements of order p, as defined in [2]. Subsequently, various properties of this graph are determined, including its diameter and chromatic number. The construction process involves several steps: identifying the group elements and their respective orders, organizing them into subsets based on these orders, and constructing the graph using these subsets. Finally, the properties are determined by applying specific definitions.

The paper is divided into four parts. Firstly, it introduces Cayley graphs by providing background information on this type of graph. Secondly, it explores fundamental concepts within graph and group theories. The third part presents the main findings of the research. Lastly, the fourth section contains an overall summary of the paper.

PRELIMINARIES

In this section, fundamental concepts from graph theory and group theory used in this research are presented. These include the Cayley graph, p_i-Cayley graph, regular graph, complete graph, cyclic group, diameter, and chromatic number. The definition of the Cayley graph will be provided below.

Definition 1 [1] *A graph* Γ *is called a Cayley graph on a group* G *if there is a subset* $S \subseteq G \backslash \{e\}$*, with* $S = S^{-1} = \{g^{-1} | g \in S\}$*, such that* $V(\Gamma) = G$ *and two vertices* g *and* h *are adjacent if and only if* $hg^{-1} \in S$*. This Cayley graph is denoted by* $Cay(G,S)$*.*

A graph is considered a regular graph when each of its vertices shares the same degree [8]. Additionally, a complete graph is a simple graph where every vertex is adjacent to all others [9]. Subsequently, the definition of the p_i-Cayley graph is presented in the following.

Definition 2 [2] *Let* G *be a group with* $|G| = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$*,* p_i *primes,* $\alpha_i \in \mathbb{N}$*,* $i = 1,2,\cdots,k$ *and* $S_{p_i} = \{x \in G : |x| = p_i^n, n = 1,2,\ldots,\alpha_i\}$ *a subset of* G *with* $S_{p_i} = S_{p_i}^{-1} = \{s^{-1} | s \in S_{p_i}\}$*. The* p_i*-Cayley graph, denoted as* p_i*-*$Cay(G,S_{p_i})$*,* $i = 1,2,\cdots,k$*, is a graph where the vertices are the elements of the group* G *such that two different vertices,* g *and* h*, are adjacent if* $gh^{-1} \in S_{p_i}$ *for all* $g,h \in G$*.*

The definitions of the diameter of a graph and the diameter for a complete graph are provided in the following definition and proposition.

Definition 3 [10] *The greatest distance between all pairs of vertices of a graph* Γ *is called the diameter of* Γ *and is denoted by* $diam(\Gamma)$*, where the distance is the shortest path between two different vertices.*

Proposition 1 [10] *The diameter of* Γ*,* $diam(\Gamma)$*, is equal to 1 if and only if* Γ *is a complete graph.*

The definition of the chromatic number is provided as follows.

Definition 4 [11] *The proper coloring of a graph* Γ *is the coloring of the vertices and edges with minimal number of colors such that no two vertices should have the same color. The minimum number of colours is called as the chromatic number,* $\chi(\Gamma)$ *and the graph is called properly coloured graph.*

Within group theory, a group G is cyclic if there exists an element a within G such that G is defined as $\{a^n | n \in Z\}$. This specific element a serves as a generator for G.

The following section presents the construction of the prime power Cayley graph associated with a cyclic group having an order of pqr, followed by determining the properties of the graph.

RESULTS AND DISCUSSION

Constructions and determination of properties for the p_i-Cayley graph of the cyclic group G of pqr, where $p < q < r$, are provided in this section. These constructions are presented through lemmas and a theorem. The properties, including the diameter and chromatic number of the obtained graph, are subsequently explained in the propositions.

The construction is begun by listing all the elements of G, as in $G = \{e, x, x^2, \ldots, x^p, \ldots, x^q, \ldots, x^r, \ldots, x^{pqr-1}\}$ and the order of each element is identified. Three subsets are formed based on the elements of set G, with each subset containing elements of prime power orders for each prime. The first subset, denoted as $S^{(p)}$, contains elements with order p; the second subset, $S^{(q)}$, contains elements with order q and the third subset, $S^{(r)}$, contains elements with order r, as shown below.

1. $S^{(p)} = \{x \in G | |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$
2. $S^{(q)} = \{x \in G | |x| = q\} = \{x^{pr}, x^{2pr}, \ldots, x^{(q-1)pr}\}$
3. $S^{(r)} = \{x \in G | |x| = r\} = \{x^{pq}, x^{2pq}, \ldots, x^{(r-1)pq}\}$

The p-Cayley graph, named $Cay(G,S^{(p)})$, the q-Cayley graph, called $Cay(G,S^{(q)})$, and the r-Cayley graph, denoted as $Cay(G,S^{(r)})$, are formed according to the subsets $S^{(p)}$, $S^{(q)}$, and $S^{(r)}$, respectively.

The construction of the p-Cayley graph will be demonstrated in this paper. Identification of the set of vertices and set of edges is necessary in constructing the graph. The elements of G form the set of vertices for the p-Cayley graph, denoted as $V(p - Cay(G,S^{(p)}))$, as described in Definition 2. Then, Lemmas 1 through Lemmas 7 are used to get the edges between vertices in p-$Cay(G,S^{(p)})$. In the first lemma, Lemma 1, the vertices within p-$Cay(G,S^{(p)})$ are partitioned into multiple sets, denoted as Set A_i and Set B for $1 \leq i \leq p-1$.

Lemma 1 *Let G be a cyclic group of order pqr generated by x. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $A_i = \{x^{lqr+i} | 1 \leq l \leq p-1\}$ for $i = 1, 2, \ldots, qr$ and $B = \{x^j | 1 \leq j \leq qr\} = \{x, x^2, \ldots, x^q r\}$. Then, $B \cup (A_1 \cup A_2 \cup \ldots \cup A_{qr}) = G$.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$, and $|x| = pqr$. Consider $B \cup (A_1 \cup A_2 \cup \ldots \cup A_{qr})$ in G. For $g \in G$, where $g = x^k$ and $1 \leq k \leq pqr$, there are two cases to examine:

1. If $1 \leq k \leq qr$, then $x \in B$.
2. If $k = lq + i$ for $1 \leq l \leq p-1$, then $x \in A_i$, where $1 \leq i \leq qr$.

Therefore, $B \cup (A_1 \cup A_2 \cup \ldots \cup A_{qr})$ in G.

In Lemma 2, the adjacency among all vertices in each set A_i is demonstrated. It is shown that all vertices in each set A_i are adjacent to each other in p-$Cay(G, S^{(p)})$.

Lemma 2 *Let G be a cyclic group of order pqr generated by x. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $A_i = \{x^{lqr+i} | 1 \leq l \leq p-1\}$ for $i = 1, 2, \ldots, qr$. Then, all vertices in each A_i are adjacent with each other for $1 \leq i \leq qr$.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$, and $|x| = pqr$. Let g and h be elements in A_i where $g = x^{lqr+i}$ and $h = x^{l'qr+i}$ for $1 \leq l \neq l' \leq p-1$. Then, gh^{-1} is in $S^{(p)}$ since $gh^{-1} = x^{(l-l')qr} \in S^{(p)}$. Therefore, all elements in each A_i for $1 \leq i \leq qr$ are adjacent to each other.

Next, in Lemma 3, it is shown that the vertices in two different sets of A, such as A_i and A_j where $i \neq j$, are not adjacent to each other.

Lemma 3 *Let G be a cyclic group of order pqr generated by x. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $A_i = \{x^{lq+i} | 1 \leq l \leq p-1\}$ and $A_j = \{x^{lq+j} | 1 \leq l \leq p-1\}$ for $i, j = 1, 2, \ldots, qr$. Then, the vertices in A_i and A_j for $i \neq j$ are not adjacent.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$, and $|x| = pqr$. Let $A_i = \{x^{lqr+i} | 1 \leq l \leq p-1\}$ and $A_j = \{x^{lqr+j} | 1 \leq l \leq p-1\}$ for $i \neq j$. The product of x^{lqr+i} and the inverse of x^{lqr+j} is x^{i-j}, and this element is not in $S^{(p)}$. Therefore, x^{lqr+i} and x^{lqr+j} are not adjacent for $1 \leq l \leq p-1$, which implies that the vertices in different sets, A_i and A_j, are not adjacent for $i \neq j$.

Then, the adjacencies of vertices in set B are presented in Lemma 4. It is shown that all vertices in set B are not adjacent to each other.

Lemma 4 *Let G be a cyclic group of order pqr generated by x. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $B = \{x^j | 1 \leq j \leq qr\} = \{x, x^2, \ldots, x^{qr}\}$. Then, there is no adjacent vertices in set B.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$ and $|x| = pqr$. Let $x_i \in B$ and $x_j \in B$ for $1 \leq i \neq j \leq qr$ and $i > j$. Then, $(x^i)(x^j)^{-1} = x^{1-j} \notin S^{(p)}$. Therefore, there is no adjacent vertices in B.

In Lemma 5, the adjacencies between set A_i and set B are studied. Each vertex $x^j \in B$ is adjacent to all vertices in set A_i under the condition $i = j$.

Lemma 5 *Let G be a cyclic group of order pqr generated by x and $S^{(p)} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define the sets:*

$$A_i = \{x^{lqr+i} \mid 1 \leq l \leq p-1\} \text{ for } i = 1, 2, \ldots, qr,$$
$$B = \{x^j \mid 1 \leq j \leq qr\} = \{x, x^2, \ldots, x^{qr}\}.$$

Then, each vertex x^j in set B is adjacent to every vertex in set A_i for $1 \leq i = j \leq qr$.

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$ with $|x| = pqr$. For $1 \leq j \leq qr$, define $A_i = \{x^{lqr+i} \mid 1 \leq l \leq p-1\}$ and $x^j \in B$. Consider $(x^{lq+i})(x^j)^{-1}$, which is an element in $S^{(p)}$ since $(x^{lq+i})(x^j)^{-1} = x^{lq} \in S^{(p)}$. Therefore, x^j in B is adjacent to all vertices in A_i for $1 \leq i = j \leq qr$.

In Lemma 6, it is demonstrated that each vertex $x^j \in B$ is not adjacent to all vertices in set A_i given the condition $i \neq j$.

Lemma 6 *Let G be a cyclic group of order pqr generated by x. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $A_i = \{x^{lqr+i} | 1 \leq l \leq p-1\}$ for $i = 1, 2, \ldots, qr$ and $B = \{x^j | 1 \leq j \leq qr\} = \{x, x^2, \ldots, x^{qr}\}$. Then, for $i \neq j$, $x^{lqr+i} \in A_i$ and $x^j \in B$ are not adjacent.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$, where $|x| = pqr$ denotes the order of the element x. Now, define sets $A_i = \{x^{lqr+i} \mid 1 \leq l \leq p-1\}$ and let x^j belong to set B for $i \neq j$. Consider the product of x^{lqr+i} and the inverse of x^j, which is equal to $x^{lqr+i-j}$. The element $x^{lqr+i-j}$ does not belong to set $S^{(p)}$. Therefore, x^{lqr+i} and x^j from sets A_i and B, respectively, are not adjacent for $i \neq j$.
Finally, in Lemma 7, a complete graph with p vertices is formed by each vertex x^j in set B, which is adjacent to all vertices in set A_i when $i = j$.

Lemma 7 *Let G be a cyclic group of order pqr generated by x. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $A_i = \{x^{lqr+i} | 1 \leq l \leq p-1\}$ for $i = 1, 2, \ldots, qr$. Then, $\{x^j\} \cup A_j$ is a complete graph, K_p.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$, where $|x| = pqr$ denotes the order of the element x. Based on Lemma 2, all vertices in set A_i are adjacent to each other. According to Lemma 3, $\{x^j\}$ is adjacent to the vertices in A_j. Thus, there are p vertices in $\{x^j\} \cup A_j$, and each vertex is adjacent to every other vertex. Therefore, $\{x^j\} \cup A_j$ forms a complete graph, K_p.

Based on Lemma 1 through Lemma 7, the complete construction of the p-Cayley graph of G is presented in the following theorem.

Theorem 1 *Let G be a cyclic group of order pqr and $S^{(p)}$ a non-empty subset of G with $S^{(p)} = \{x \in G : |x| = p\}$ and $S^{(p)} = {S^{(p)}}^{-1}$. Then, the p-Cayley graph of G, $p - Cay(G, S^{(p)})$ is qrK_p, where K is the complete graph of order p.*

Proof
Let $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{pqr-1}\}$ and $|x| = pqr$. Let $S^{(p)} = \{x \in G : |x| = p\} = \{x^{qr}, x^{2qr}, \ldots, x^{(p-1)qr}\}$. Define $A_i = \{x^{lqr+i} | 1 \leq l \leq p-1\}$ for $i = 1, 2, \ldots, qr$ and $B = \{x^j | 1 \leq j \leq qr\} = \{x, x^2, \ldots, x^q r\}$.
All elements of Set A_i and Set B are in G, as proved in Lemma 1. Then, the vertices in each A_i are adjacent to each other, as proved in Lemma 2. Furthermore, there is no adjacency between the vertices in two distinct sets of A. Each set in A is an independent set because the vertices of set A_i are not adjacent to the vertices in set A_j for $i \neq j$, as proved in Lemma 3.
Besides, the vertices in set B are not adjacent to each other as showed in Lemma 4. Then, the vertices in set B is adjacent with the vertices in a set A such that $\{x^j\} \in B$ is adjacent with $x^{lqr+i} \in A_i$ for $i = j$. Hence, the adjacency of these elements, $\{x^j\} \in B$ and $x^{lqr+i} \in A_i$ for $i = j$ formed a component of graph. This component contains p vertices since there are p-1 vertices from Set A_i and a vertex from Set B. Following from this, a graph with qr-components is formed where each component contains p-vertices. This is because there are q vertices in Set B which each vertex is connected with all vertices of exactly one set from Set A. Therefore, the p-Cayley graph of the cyclic group of order pqr for $p < q < r$ is the union of qr copies of complete graphs with p vertices, qrK_p.

Similarly, we obtained the q-Cayley graph and r-Cayley graph as follows.

Theorem 2 *Let G be a cyclic group of order pqr and $S^{(q)}$ a non-empty subset of G with $S^{(q)} = \{x \in G : |x| = q\}$ and $S^{(q)} = {S^{(q)}}^{-1}$. Then, the q-Cayley graph of G, $q - Cay(G, S^{(q)})$ is prK_q, where K_q is the complete graph of order q.*

Theorem 3 *Let G be a cyclic group of order pqr and $S^{(r)}$ a non-empty subset of G with $S^{(r)} = \{x \in G : |x| = r\}$ and $S^{(r)} = {S^{(r)}}^{-1}$. Then, the r-Cayley graph of G, $r - Cay(G, S^{(r)})$ is pqK_r, where K_r is the complete graph of order r.*

The properties of the p-Cayley graph of G are demonstrated in the next two propositions, Proposition 2 and Proposition 3.

Proposition 2 *Let G be a cyclic group of order pqr, and let $S^{(p)} = \{x \in G | |x| = p\}$ with $S^{(p)} = S^{(p)^{-1}}$. Then, the diameter of p-Cay$(G, S^{(p)})$ is one.*

Proof
By Definition 1, the diameter of p-Cay$(G, S^{(p)})$ is one because, in a complete graph, all vertices are adjacent to each other.

Proposition 3 *Let G be a cyclic group of order pqr, and let $S^{(p)} = \{x \in G | |x| = p\}$ with $S^{(p)} = S^{(p)^{-1}}$. Then, the chromatic number of p-Cay$(G, S^{(p)})$ is p.*

Proof
Consider any two distinct vertices in p-Cay$(G, S^{(p)})$, denoted as x^i and x^j for $0 \leq i \neq j \leq pqr - 1$. The colouring between x^i and x^j uses different colours, as these two vertices are adjacent to each other for all $0 \leq i \neq j \leq p - 1$. Hence, there are p different colours of the vertices in p-Cay$(G, S^{(p)})$. Therefore, based on Definition 4, the chromatic number of p-Cay$(G, S^{(p)})$ is p.

Similarly, we obtained the properties q-Cayley graph and r-Cayley graph as follows.

Proposition 4 *Let G be a cyclic group of order pqr, and let $S^{(q)} = \{x \in G | |x| = q\}$ with $S^{(q)} = S^{(q)^{-1}}$. Then, the diameter of q-Cay$(G, S^{(q)})$ is one.*

Proposition 5 *Let G be a cyclic group of order pqr, and let $S^{(q)} = \{x \in G | |x| = q\}$ with $S^{(q)} = S^{(q)^{-1}}$. Then, the chromatic number of q-Cay$(G, S^{(q)})$ is q.*

Proposition 6 *Let G be a cyclic group of order pqr, and let $S^{(r)} = \{x \in G | |x| = r\}$ with $S^{(r)} = S^{(r)^{-1}}$. Then, the diameter of r-Cay$(G, S^{(r)})$ is one.*

Proposition 7 *Let G be a cyclic group of order pqr, and let $S^{(r)} = \{x \in G | |x| = r\}$ with $S^{(r)} = S^{(r)^{-1}}$. Then, the chromatic number of p-Cay$(G, S^{(r)})$ is r.*

CONCLUSION

In this paper, the p_i-Cayley graph is constructed for a cyclic group of order pqr. Three graphs are formed based on each subset: the p-Cayley graph constructed with respect to $S^{(p)}$ is qrK_p, the q-Cayley graph constructed with respect to $S^{(q)}$ is prK_q, and the r-Cayley graph constructed with respect to $S^{(r)}$ is pqK_r. All graphs demonstrate a diameter of one and a chromatic number of p for the p-Cayley graph, q for the q-Cayley graph and r for the r-Cayley graph.

ACKNOWLEDGMENTS

The authors wish to extend their appreciation for the financial assistance provided by Universiti Teknologi Malaysia through the Others Grant Scheme (R.J130000.7354.4B711) and Matching Grant Scheme (Q.J130000.3054.03M65), as well as the support from the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (FRGS/1/2020/STG06/UTM/01/2).

REFERENCES

1. J. Pan, Open Mathematics **18**, 595–602 (2020).
2. A. Zulkarnain, N. H. Sarmin, H. I. M. Hassim, and A. Erfanian, in *AIP Conference Proceedings*, Vol. 2266 (AIP Publishing LLC, 2020) p. 060001.

3. L. Bussaban, A. Kaewkhao, and S. Suantai, "Cayley graphs of gyrogroups," Quasigroups and Related Systems **27**, 25–32 (2019).
4. M. Farrokhi DG, M. Rajabian, and A. Erfanian, "Relative cayley graphs of finite groups," Asian-European Journal of Mathematics **12**, 2050003 (2020).
5. A. Behajaina and F. Legrand, Linear Algebra and its Applications **642**, 264–284 (2022).
6. Y. Aikawa, H. Jo, and S. Satake, "Left-right cayley hashing: A new framework for provably secure hash functions," Mathematical Cryptology **3**, 53–65 (2023).
7. A. A. NEAMAH, A. ERFANIAN, and A. H. MAJEED, "On a generalized cayley graph of column matrices of elements of a finite group." Mathematica (1222-9016) **64** (2022).
8. B. Tolue, "The prime order cayley graph," UPB Sci. Bull., Series A **77**, 207–218 (2015).
9. R. Diestel, *Graph theory*, 3rd ed., edited by S. A. . K.A.Ribet (Springer, 2005) p. 3.
10. H. Su and Y. Wei, "The diameter of unit graphs of rings," Taiwanese Journal of Mathematics **23**, 1–10 (2019).
11. B. Tosuni, "Graph coloring problems in modern computer science," European Journal of Interdisciplinary Studies **2**, 87–95 (2015).