DISTANCE IN CAYLEY GRAPHS ON PERMUTATION GROUPS GENERATED BY $km$-CYCLES

Article · September 2017

CITATIONS
0

READS
117

2 authors:

Mohammad Hossein Ghaffari B. Iran University of Science and Technology

Zohreh Mostaghim Iran University of Science and Technology

All content following this page was uploaded by Zohreh Mostaghim on 16 June 2017.
The user has requested enhancement of the downloaded file.
DISTANCE IN CAYLEY GRAPHS ON PERMUTATION GROUPS
GENERATED BY k m-CYCLES

MOHAMMAD HOSSEIN GHAFFARI AND ZOHREH MOSTAGHIM*

Communicated by Ali Reza Ashrafi

Abstract. In this paper, we extend upon the results of B. Suceava and R. Stong [Amer. Math. Monthly, 110 (2003) 162–162], which they computed the minimum number of 3-cycles needed to generate an even permutation. Let $\Omega^m_{k,m}$ be the set of all permutations of the form $c_1c_2\cdots c_k$ where $c_i$’s are arbitrary $m$-cycles in $S_n$. Suppose that $\Gamma^a_{k,m}$ be the Cayley graph on subgroup of $S_n$ generated by all permutations in $\Omega^m_{k,m}$. We find a shortest path joining identity and any vertex of $\Gamma^a_{k,m}$ for arbitrary natural number $k$, and $m = 2, 3, 4$. Also, we calculate the diameter of these Cayley graphs. As an application, we present an algorithm for finding a short expression of a permutation as products of given permutations.

1. Introduction

Let $G$ be a finite group and $\Omega$ a subset of $G$ that generates it. We assume that $\Omega$ does not contain identity element of $G$ and $\Omega = \Omega^{-1}$, where $\Omega^{-1} = \{s^{-1} \mid s \in \Omega\}$. The Cayley graph $\Gamma = Cay(G,\Omega)$ is a graph whose vertex set is $G$ and two vertices $g$ and $g'$ are adjacent if and only if $g' = gs$ for some $s$ in $\Omega$. The distance between the vertices $g$ and $g'$ in $\Gamma$, denoted by $d_\Gamma(g,g')$ or briefly $d(g,g')$, is the length of a shortest path joining $g$ and $g'$. It is easily seen that $d = d(g,g')$ is the least number of $h_i \in \Omega$ so that $g' = gh_1 \cdots h_d$. So, $d(g,g') = d(1,g^{-1}g')$. The diameter of $\Gamma$ is the maximum distance among the vertices of $\Gamma$.

For every permutation $g$, the support of $g$ is the set $Supp(g)$ of points moved by $g$, and the support size is $supp(g) = |Supp(g)|$. Every permutation $g$ may be expressed as a product of disjoint cycles.

MSC(2010): Primary: 05C12; Secondary: 05C25, 20F05.
Keywords: Permutation group, Cayley graph, Quadruple cycles, Diameter, Expressions of permutations.
Received: 11 December 2016, Accepted: 08 April 2017.
*Corresponding author.
This factorization is unique, ignoring 1-cycles, up to order. For permutation \( g \) with \( e_i \) cycles of length \( i \) for \( i = 2, 3, \ldots, n \), the cycle type of \( g \) is the formal product \( 2^{e_2}3^{e_3}\cdots n^{e_n} \).

Finding the distance between two vertices in the Cayley graphs appears in many applications; for example in network science, computational biology, coding theory and cryptography (see [4], [12], [7], [9] and [6]). In [10], [5] and [6] authors found algorithms that factor a permutation over a generating set. Among all types of generating sets for permutation groups, \( m \)-cycles play an important role (see [1] and [2]). Finding and estimating the diameter of Cayley graphs is an active research area in mathematics (see [3], [2] and [8]). In this paper, we calculate the distance function and the diameter of some family of Cayley graphs.

For natural numbers \( n, m \) and \( k \) satisfying \( mk \leq n \), suppose that \( \Omega_{n}^{n}_{k,m} \) be the set of all permutations of the form \( c_1c_2\cdots c_k \) where \( c_i \)'s are arbitrary \( m \)-cycles, and \( \Omega_{m}^{n} \) be the set of all permutations with cycle type \( m \) in \( S_n \). Let \( G \) be the subgroup of \( S_n \) generated by generating set \( \Omega_{n}^{n}_{k,m} \) (respectively, \( \Omega_{m}^{n} \)). It is clear that \( G \) is a normal subgroup of \( S_n \) and so \( G = S_n \) or \( A_n \) (for \( n = 4 \), it is easily seen that \( G \) is not isomorphic to the Klein four-group). It is easily seen that \( G = S_n \) if and only if \( (m+1)k \) is an odd integer. We denote the Cayley graph corresponded to the subgroup of \( S_n \) generated by all permutations in \( \Omega_{n}^{n}_{k,m} \) (respectively, \( \Omega_{m}^{n} \)) by \( \Gamma_{n}^{n}_{k,m} \) (respectively, \( \Gamma_{m}^{n} \)). We will omit superscript when it is clear from the context. We denote the distance function on \( \Gamma_{n}^{n}_{k,m} \) (respectively, \( \Gamma_{m}^{n} \)) by \( d_{k,m} \) (respectively, \( d_{m,k} \)). In this paper, we find a shortest path joining identity and any vertex of \( \Gamma_{k,m}^{n} \), for \( m = 2, 3 \) and 4. As a consequence, we calculate the diameter of these Cayley graphs.

With the purpose of attacking to a cryptosystem, authors in [6] presented an algorithm that can find a short expression for an arbitrary permutation in terms of given permutations. In Section 4, we improve their algorithm.

2. Preliminaries

Suppose that \( g \) is a non-trivial element of \( S_n \). The disjoint cycle decomposition of \( g \) has the following form:

\[
g = \prod_{i=1}^{t} a_i,
\]

where \( t \) is a natural number and \( a_i \)'s are disjoint cycles.

**Proposition 2.1.** ([11], Theorem 3.1) For \( g \in S_n \) in the form of Equation 2.1 suppose that,

\[
a_i = (\alpha_{i_1} \alpha_{i_2} \alpha_{i_3}\cdots \alpha_{i_{a_i}}), \quad i = 1, 2, 3, \ldots, t.
\]

Then, the following product has the minimum factors in the generating set \( \Omega_{1,2} \) for \( S_n \):

\[
g = \prod_{i=1}^{t} (\alpha_{i_1} \alpha_{i_2})(\alpha_{i_1} \alpha_{i_3})\cdots(\alpha_{i_1} \alpha_{i_{a_i}}),
\]

and we have,

\[
d_{1,2}(1, g) = \text{supp}(g) - t.
\]
Let $h$ be a non-trivial element of $A_n$. In disjoint cycle decomposition of $h$ we have:

\[ h = \prod_{i=1}^{s} a_i \prod_{j=1}^{k} b_j c_j, \]

where $s$ and $k$ are non-negative integer numbers, $a_i$’s are odd length cycles with $|a_i| \geq 3$, and $b_j$’s and $c_j$’s are even length cycles. We write the identity of the group as empty product of cycles, i.e. in the above form, $s = k = 0$.

**Proposition 2.2.** ([13], page 162) For $h \in A_n$ in the form of Equation 2.4 suppose that,

\[
\begin{align*}
    a_i &= (\alpha_{i1} \alpha_{i2} \alpha_{i3} \cdots \alpha_{i_d}), \\
    b_i &= (\beta_{i1} \beta_{i2} \beta_{i3} \cdots \beta_{i_d}), \\
    c_i &= (\gamma_{i1} \gamma_{i2} \gamma_{i3} \cdots \gamma_{i_d}),
\end{align*}
\]

then, the following product has the minimum factors in the generating set $\Omega_{1,3}$ for $A_n$

\[
    h = \prod_{i=1}^{s} (\alpha_{i1} \alpha_{i2} \alpha_{i3})(\alpha_{i1} \alpha_{i4} \alpha_{i5}) \cdots (\alpha_{i1} \alpha_{i_{d-1}} \alpha_{i_d})
\]

\[
    \prod_{j=1}^{k} (\beta_{j1} \gamma_{j1} \gamma_{j2})(\beta_{j1} \gamma_{j3} \beta_{j4}) \cdots (\beta_{j1} \beta_{j_{b-1}} \beta_{j_b})
\]

\[
    (\beta_{j1} \beta_{j3} \beta_{j4})(\beta_{j1} \beta_{j5} \beta_{j6}) \cdots (\beta_{j1} \beta_{j_{c-1}} \beta_{j_c})
\]

\[
    (\gamma_{j1} \gamma_{j3} \gamma_{j4})(\gamma_{j1} \gamma_{j5} \gamma_{j6}) \cdots (\gamma_{j1} \gamma_{j_{e-1}} \gamma_{j_e}).
\]

and we have,

\[
    d_{1,3}(1, h) = (\text{supp}(h) - s)/2,
\]

where, $s$ is the number of odd length cycles of permutation $h$ in $A_n$.

### 3. On Cayley graph $\Gamma_{k,m}^n$

In the next theorem we show that it is enough to consider the Cayley graph generated by single $m$-cycles; more precisely, we express $d_{k,m}$ as a function of $d_{1,m}$. Since $\Omega_{m}^n$ is a subset of $\Omega_{k,m}^n$, the following theorem finds a lower bound for $d_{m^{k}}(1, g)$.

**Theorem 3.1.** In $\Gamma_{k,m}^n$ we have,

\[
    d_{k,m}(1, g) = \begin{cases} 
        \lfloor d_{1,m}(1, g)/k \rfloor & \text{if } 2 \nmid m \text{ or } 2 \nmid u \\
        \lfloor d_{1,m}(1, g)/k \rfloor + 1 & \text{if } 2|m \text{ and } 2 \nmid u,
    \end{cases}
\]

where,

\[
    u = k\lfloor d_{1,m}(1, g)/k \rfloor - d_{1,m}(1, g).
\]
Proof. We prove the theorem by presenting the desired path in $\Gamma_{k,m}^n$. Suppose that $g = c_1c_2c_3 \cdots c_t$ where $c_i$’s are $m$-cycles and $t = d_{1,m}(1, g)$.

Case 1: Suppose that $2 \nmid u$. Set $y_i = c_i$ for $1 \leq i \leq t$. For $t + 1 \leq i \leq t + u$ if $2 \mid i$, then we set $y_i = c_t$ and otherwise $y_i = c_i^{-1}$. We have, $\prod_{i=1}^{t+u} y_i = g$.

Case 2: $2 \nmid u$ and $2 \nmid m$.

Subcase 2-1: $u = 1$. Since $\gcd(2,m) = 1$, there exists an integer number $v$ such that $2v \equiv 1 \pmod{m}$. Set $y_i = c_i$ for $1 \leq i < t$, and $y_t = y_{t+1} = c_t$. Therefore, $\prod_{i=1}^{t+u} y_i = g$.

Subcase 2-2: $3 \leq u$. Set $y_i = c_i$ for $1 \leq i \leq t$, and $y_{t+1} = y_{t+2} = c_t$, $y_{t+3} = c_t^2$. For $t + 4 \leq i \leq t + u$ if $2 \mid i$, then we set $y_i = c_t$ and otherwise $y_i = c_i^{-1}$. We have, $\prod_{i=1}^{t+u} y_i = g$.

Case 3: $2 \nmid u$ and $2 \mid m$. Since $m$-cycles are odd permutations, it is impossible to generate $g$ by $t + u$ number of $m$-cycles. We generate $g$ by $u + t + k$ number of $m$-cycles. Also note that $2 \nmid k$. Set $y_i = c_i$ for $1 \leq i \leq t$. For $t + 1 \leq i \leq t + u + k$, if $2 \mid i$, then we set $y_i = c_t$ and otherwise $y_i = c_i^{-1}$. Thus, $\prod_{i=1}^{t+u+k} y_i = g$.

Now, we show that the previous presented products are of minimal length. Suppose that $g = h_1h_2h_3 \cdots h_l$ where $h_i \in \Omega_{k,m}^n$ and $l \leq \lceil t/k \rceil - 1$. So, $kl < t$. This means that $g$ is written by less than $d_{1,m}(1, g)$ number of $m$-cycles, but this is impossible. \hfill \Box

As an immediate consequence of Proposition 2.1 and Theorem 3.1 the following corollary holds.

**Corollary 3.2.** We have,

$$d_{k,2}(1, g) = \begin{cases} \lfloor d_{1,2}(1, g) / k \rfloor & \text{if } 2 \mid u \\ \lfloor d_{1,2}(1, g) / k \rfloor + 1 & \text{if } 2 \nmid u, \end{cases}$$

where,

$$u = k \lfloor d_{1,2}(1, g) / k \rfloor - d_{1,2}(1, g), \quad d_{1,2}(1, g) = \text{supp}(g) - t,$$

and $t$ is the number of cycles in the disjoint cycle decomposition of $g$.

Now, we can find the diameter of $\Gamma_{k,2}^n$.

**Corollary 3.3.** We have,

$$\text{diam}(\Gamma_{k,2}^n) = \begin{cases} \lfloor (n-2) / k \rfloor & \text{if } 2 \mid k \\ \lfloor (n-2) / k \rfloor + 1 & \text{if } 2 \nmid k. \end{cases}$$

**Proof.** We find the maximum value of function $d_{k,2}(1, g)$, denoted by $d_1$, for suitable permutation $g$ in the group generated by $\Omega_{k,2}^n$. For every permutation $g$, suppose that $b_g$ is the remainder of division $d_{1,2}(1, g)$ on $k$. Set $u_g = k \lfloor d_{1,2}(1, g) / k \rfloor - d_{1,2}(1, g)$. We have $2 \mid u_g$ if and only if $k \mid d_{1,2}(1, g)$ or $2 \mid (k - b_g)$. Also, for $k > 1$, $\lceil (n-2) / k \rceil = \lceil (n-1) / k \rceil$ if and only if $k \mid (n-2)$.

Case 1: Suppose that $2 \mid k$. In this case $\Gamma_{k,2} = \text{Cay}(A_n, \Omega_{k,2}^n)$. For every permutation $g$ in $A_n$ we have $2 \mid d_{1,2}(1, g)$. So, $2 \mid b_g$. Since $2 \mid k$, we have $2 \mid u_g$.

Subcase 1-1: $2 \mid n$. In this case, it is easily seen that $g_2 = (12 \ldots n-1)$ gives $d_1$. By Proposition 2.1,
we have \(d_{1,2}(1, g_2) = n - 2\). So, \(\text{diam}(\Gamma_{k,2}^n) = \lceil (n - 2)/k \rceil\).

Subcase 1-2: \(2 \nmid n\). In this case \(g_1 = (1 \ 2 \ \cdots \ n)\) gives \(d_{1r}\). By Proposition 2.1, we have \(d_{1,2}(1, g_1) = n-1\). Since \(2 \nmid (n - 2), \ k \nmid (n - 2)\). Thus,

\[
\text{diam}(\Gamma_{k,2}^n) = \left\lceil \frac{n - 1}{k} \right\rceil = \left\lceil \frac{n - 2}{k} \right\rceil.
\]

Case 2: Suppose that \(2 \nmid k\). In this case \(\Gamma_{k,2}^n = \text{Cay}(S_n, \Omega_{k,2}^n)\). So, both \(g_1 = (1 \ 2 \ \cdots \ n)\) and \(g_2 = (1 \ 2 \ \cdots \ n - 1)\) belong to the vertex set of \(\Gamma_{k,2}^n\).

Subcase 2-1: \(2 \nmid u_{g_1}\). In this case \(g_1\) gives \(d_{1r}\). We have \(k \nmid (n - 1)\) and \(2 \nmid (k - b_{g_1})\). Thus \(2|b_{g_1}\) and \(1 < b_{g_1} < k\). Hence \(k \nmid (b_{g_1} - 1)\) and \(k \nmid (n - 2)\). We have,

\[
\text{diam}(\Gamma_{k,2}^n) = \left\lceil \frac{n - 1}{k} \right\rceil + 1 = \left\lceil \frac{n - 2}{k} \right\rceil + 1.
\]

Subcase 2-2: \(2 \nmid u_{g_2}\). In this case, it is easily seen that \(g_2\) gives \(d_{1r}\). So, \(\text{diam}(\Gamma_{k,2}^n) = \lceil (n - 2)/k \rceil + 1\).

Subcase 2-3: \(2|u_{g_1}\) and \(2|u_{g_2}\). If we show that \(k|n - 2\), then,

\[
\text{diam}(\Gamma_{k,2}^n) = \left\lceil \frac{n - 1}{k} \right\rceil = \left\lceil \frac{n - 2}{k} \right\rceil + 1.
\]

Suppose that, on the contrary, \(k \nmid n - 2\). Since \(2|u_{g_2}\), we have \(2|k - b_{g_2}\). So, \(2 \nmid k - b_{g_2}\) and \(k|n - 1\). Thus, \(b_{g_2} = k - 1\); which contradicts \(2|k - b_{g_2}\). \(\square\)

The following corollaries are immediate consequences of Proposition 2.2 and Theorem 3.1.

**Corollary 3.4.** By the above notations, we have:

\[
d_{k,3}(1, g) = \left\lfloor \frac{\text{supp}(g) - s}{2k} \right\rfloor.
\]

**Corollary 3.5.** The diameter of \(\Gamma_{k,3}\) is \(\left\lfloor \frac{n}{2} \right\rfloor/k\).

Suppose that \(n > 4\) and \(g\) is an element of \(S_n\) in the following form:

\[
g = \prod_{i=1}^{c_0(g)} \alpha_i \prod_{j=1}^{c_1(g)} \beta_j \prod_{l=1}^{c_2(g)} \gamma_l
\]

where \(c_i(g)\)'s are non-negative integer numbers, \(\alpha_i\)'s are 3m-length cycles, \(\beta_j\)'s are \((3m + 1)\)-length cycles with \(|\beta_j| \geq 4\), \(\gamma_j\)'s are \((3m + 2)\)-length cycles, and all cycles are disjoint. We write the identity of the group as empty product of cycles, i.e. \(c_0(1) = c_1(1) = c_2(1) = 0\). In this section, we consider the Cayley graph \(\Gamma_{k,4}\).

**Lemma 3.6.** Let \(n > 4\). For any permutation \(g\) in \(S_n\), we have:

\[
d_{1,4}(1, g) \leq r_4(g),
\]

where \(r_4(g) = 3\) if \(g\) is a transposition, and

\[
r_4(g) = \frac{\text{supp}(g) + c_2(g) - c_1(g)}{3} + \frac{1 - (-1)^{c_0(g)}}{2},
\]

for other permutations.
Proof. For transposition \( g = (\epsilon_1 \epsilon_2) \), we have:

\[
g = (\epsilon_1 \epsilon_3 \epsilon_4 \epsilon_5)(\epsilon_1 \epsilon_3 \epsilon_5 \epsilon_4)(\epsilon_1 \epsilon_3 \epsilon_5 \epsilon_2).
\]

It is easily seen that \( g \) cannot be generated by less than three generators; thus \( d_{1,4}(1, g) = 3 \). By the notations used in Equation 3.1, let

\[
\alpha_i = (\alpha_{i1} \alpha_{i2} \alpha_{i3} \cdots \alpha_{i\ell_i}),
\beta_i = (\beta_{i1} \beta_{i2} \beta_{i3} \cdots \beta_{i\ell_i}),
\gamma_i = (\gamma_{i1} \gamma_{i2} \gamma_{i3} \cdots \gamma_{i\ell_i}).
\]

In the following order, we rewrite non-transposition \( g \) by a product of 4-cycles. In this algorithm, we may relocate disjoint cycles to put the desired cycles near each other.

Step 1. Until the number of \( \gamma_i \)'s is more than 4, replace any \( \gamma_i \gamma_j \gamma \) by \((|\gamma_i| + |\gamma_j| + |\gamma_t|)/3 + 1\) number of 4-cycles,

\[
\gamma_i \gamma_j \gamma_t = (\gamma_{11} \gamma_{12} \gamma_{13} \gamma_{14})(\gamma_{21} \gamma_{22} \gamma_{23} \gamma_{24})(\gamma_{31} \gamma_{32} \gamma_{33} \gamma_{34})
\]

Step 2. Replace any \( \gamma_i \gamma_t \) by \((|\gamma_i| + |\gamma_t| + 2)/3\) number of 4-cycles,

\[
\gamma_i \gamma_t = (\gamma_{11} \gamma_{12} \gamma_{13} \gamma_{14})(\gamma_{21} \gamma_{22} \gamma_{23} \gamma_{24})
\]

So, after doing this step, there is at most one \( \gamma_j \) in \( g \).

Step 3. Replace any \( \gamma_i \beta_t \) by \((|\gamma_i| + |\beta_t|)/3\) number of 4-cycles,

\[
\gamma_i \beta_t = (\beta_{11} \beta_{12} \gamma_{13} \gamma_{14})(\beta_{21} \beta_{22} \gamma_{23} \gamma_{24})(\beta_{31} \beta_{32} \gamma_{33} \gamma_{34})
\]

Step 4. Replace any \( \gamma_i \alpha_t \alpha_q \) by \((|\gamma_i| + |\alpha_t| + |\alpha_q| + 1)/3\) number of the following 4-cycles,

\[
\gamma_i \alpha_t \alpha_q = (\alpha_{t1} \alpha_{t2} \alpha_{t3} \gamma_{1i})(\alpha_{t1} \alpha_{t2} \alpha_{t3} \alpha_{q1} \alpha_{q2})(\alpha_{t1} \alpha_{t2} \alpha_{t3} \alpha_{t4})
\]
As a result, after doing this step, either we have no $\gamma_i$ in $g$, or there is at most one $\alpha_j$ in $g$.

Step 5. Replace any $\gamma_i \alpha_t$ by $(|\gamma_i| + |\alpha_t| + 4)/3$ number of 4-cycles,

$$
\gamma_i \alpha_t = (\alpha_{t1} \alpha_{t3} \gamma_i \gamma_{i2}) (\alpha_{t1} \gamma_{i1} \gamma_{i2} \alpha_t) (\alpha_{t1} \alpha_{t3} \alpha_t \gamma_{i2})
\prod_{j=1}^{(|\gamma_i| / 3) - 1} (\alpha_{t1} \alpha_{t3j+1} \alpha_{t3j+2} \alpha_t)
\prod_{l=1}^{(|\gamma_i| - 2) / 3} (\gamma_{i1} \gamma_{i3l} \gamma_{i3l+1} \gamma_{i3l+2}).
$$

Step 6. Replace any $\alpha_i \alpha_t$ by $(|\alpha_i| + |\alpha_t| + 4)/3$ number of 4-cycles,

$$
\alpha_i \alpha_t = (\alpha_{i1} \alpha_{i3} \alpha_t \gamma_{i2}) (\alpha_{i1} \alpha_{i3} \alpha_t \gamma_{i2})
\prod_{j=1}^{(|\alpha_t| / 3) - 1} (\alpha_{i1} \alpha_{i3j+1} \alpha_{i3j+2})
\prod_{l=1}^{(|\alpha_t| - 2) / 3} (\alpha_{i1} \alpha_{i3l+1} \alpha_{i3l+2}).
$$

Step 7. Replace any $\alpha_i$ by $|\alpha_i|/3 + 1$ number of 4-cycles,

$$
\alpha_i = (\alpha_{i1} \alpha_{i3} \delta \alpha_{i2}) (\alpha_{i1} \alpha_{i3} \alpha_{i2} \delta)
\prod_{j=1}^{(|\alpha_i| / 3) - 1} (\alpha_{i1} \alpha_{i3j+1} \alpha_{i3j+2}).
$$

where $\delta$ is an arbitrary number in the $\{1, 2, \ldots, n\} \setminus \{\alpha_{i1}, \alpha_{i2}, \alpha_{i3}\}$.

Step 8. Replace any $\beta_i$ by $(|\beta_i| - 1)/3$ number of 4-cycles,

$$
\beta_i = \prod_{j=1}^{(|\beta_i| - 1)/3} (\beta_{i1} \beta_{i3j-1} \beta_{i3j} \beta_{i3j+1}).
$$

Step 9. Replace any $\gamma_i$ by $(|\gamma_i| + 1)/3$ number of 4-cycles,

$$
\gamma_i = (\gamma_{i1} \gamma_{i5} \gamma_{i3} \gamma_{i4}) (\gamma_{i1} \gamma_{i5} \gamma_{i2} \gamma_{i3})
\prod_{j=2}^{(|\gamma_i| - 2)/3} (\gamma_{i1} \gamma_{i3j} \gamma_{i3j+1} \gamma_{i3j+2}).
$$

So, we can write any non-transposition permutation $g$ by

$$
r_4(g) = \sum_{i=1}^{c_0(g)} |\alpha_i|/3 + (1 - (-1)^{c_0(g)})/2 + \sum_{i=1}^{c_1(g)} (|\beta_i| - 1)/3 + \sum_{i=1}^{c_2(g)} (|\gamma_i| + 1)/3
$$

number of 4-cycles. Since

$$
supp(g) = \sum_{i=1}^{c_0(g)} |\alpha_i| + \sum_{i=1}^{c_1(g)} |\beta_i| + \sum_{i=1}^{c_2(g)} |\gamma_i|,
$$

it is easily seen that we have:

$$
d_{1,4}(1, g) \leq r_4(g) = supp(g)/3 + (c_2(g) - c_1(g))/3 + (1 - (-1)^{c_0(g)})/2.
$$

□
Lemma 3.7. Let \( X, Y \) be two finite sets of integer numbers, and \( c \) an integer number, such that,
\[
\sum_{x \in X} x \equiv c + \sum_{y \in Y} y \pmod{3}.
\]
For \( j = 0, 1, 2 \), define
\[
\varepsilon_j = \left| \left\{ y \in Y \mid y \equiv j \pmod{3} \right\} \right| - \left| \left\{ x \in X \mid x \equiv j \pmod{3} \right\} \right|.
\]
Then, we have:
\[
(1) \sum_{j=0}^{2} \varepsilon_j = |Y| - |X|.
(2) |\varepsilon_2 - \varepsilon_1| \leq |X| + |Y|.
(3) \varepsilon_2 - \varepsilon_1 \equiv c \pmod{3}.
(4) \varepsilon_0 \equiv |Y| - |X| + \varepsilon_2 - \varepsilon_1 \pmod{2}.
(5) If \(|X| + |Y| < |c + 6|\) and exactly one of the \( c \) and \(|Y| - |X|\) is an even integer, then
\[
\delta = \max \left\{ \frac{\varepsilon_2 - \varepsilon_1 - c}{3} \pm \frac{1 - (-1)^{\varepsilon_0}}{2} \right\} \leq 1.
\]

Proof. The first equation is trivial. Without loss of generality we can replace any \( x_i \) and \( y_i \) by their incongruent modulo 3 in the set \( \{-1, 0, 1\} \). Since
\[
c \equiv \sum_{x \in X} x - \sum_{y \in Y} y \equiv \varepsilon_2 - \varepsilon_1 \pmod{3},
\]
we have \( |\varepsilon_2 - \varepsilon_1| \leq |X| + |Y| \). Define the functions
\[
f_0(t) = 1 - t^2, \quad f_1(t) = \frac{t(t+1)}{2}, \quad f_2(t) = \frac{t(t-1)}{2}.
\]
So, \( f_j(t) = 1 \) if and only if \( 3 | t - j \), and \( f_j(t) = 0 \) if and only if \( 3 \nmid t - j \), for any \( t \in \{-1, 0, 1\} \). By definition of \( \varepsilon_j \) we have:
\[
\varepsilon_j = \sum_{y \in Y} f_j(y) - \sum_{x \in X} f_j(x), \quad j = 0, 1, 2.
\]
Since \( z^2 \equiv z \pmod{2} \) for any \( z \in \{-1, 0, 1\} \),
\[
\varepsilon_0 = |Y| - |X| + \sum_{x \in X} x^2 - \sum_{y \in Y} y^2 \\
\equiv |Y| - |X| + \sum_{x \in X} x - \sum_{y \in Y} y \pmod{2}.
\]
Thus \( \varepsilon_0 \equiv |Y| - |X| + \varepsilon_2 - \varepsilon_1 \pmod{2} \).

For proving Equation 3.3 in Part 5 of the lemma, note that \( 2 \nmid |Y| - |X| + c \), and by Part 2 we have \( |\varepsilon_2 - \varepsilon_1| < |c + 6| \). If \( \varepsilon_2 - \varepsilon_1 = c \), then \( 2 \nmid \varepsilon_0 \), and \( \delta = 1 \). If \( \varepsilon_2 - \varepsilon_1 = c \pm 3 \), then \( 2 | \varepsilon_0 \), thus \( \delta = 1 \). \( \square \)

Theorem 3.8. By the above notations, for arbitrary permutation \( g \), we have:
\[
d_{1, 4}(1, g) = r_4(g).
\]

(3.4)
Proof. Let $C_i(\rho)$ be the set of all cycles in disjoint cycle decomposition of permutation $\rho$ whose lengths are congruent to $i$ modulo 3. Set $c_i = |C_i|$.

We prove Equation 3.4 by induction on $d(1, g)$. It is easily seen that $r_4(g) = 1$, for every 4-cycle $g$ in $S_n$. Suppose that the induction hypothesis is true for every permutation with distance less than $r$. For an arbitrary permutation $g$ with $d(1, g) = r > 1$ we show that $r_4(g) = r$. It is trivial that there exist $h \in S_n$ with $d(1, h) = r - 1$, and $c$, a 4-cycle in $S_n$ such that $g = hc$. By induction hypothesis we have $r_4(h) = r - 1$. By case-by-case checking of $|\text{Supp}(h) \cap \text{Supp}(c)|$ we show that

$$r_4(g) - r_4(h) \leq 1.$$  

If Inequality 3.5 holds, then $r_4(g) \leq r$, and from Lemma 3.6 we have $r_4(g) = r$. From the proof of Lemma 3.6, for any transposition $\rho$, we have $d(1, \rho) = 3$. It is enough that we only prove Inequality 3.5 when both $h$ and $g$ are not transpositions. By Equation 3.2, for non-transposition permutations $g$ and $h$, we have

$$r_4(g) - r_4(h) = \frac{\text{supp}(g) - \text{supp}(h) + \varepsilon_2 - \varepsilon_1}{3} + \frac{1 - (-1)^{c_0}}{2},$$

where $\varepsilon_k = c_k(g) - c_k(h)$, for $k = 0, 1$ and 2.

Case 1: $|\text{Supp}(h) \cap \text{Supp}(c)| = 0$. In this case $\text{supp}(g) = \text{supp}(h) + 4$, $\varepsilon_1 = 1$ and $\varepsilon_0 = \varepsilon_2 = 0$. So, by Equation 3.6, we have $r_4(g) - r_4(h) = 1$.

Case 2: $|\text{Supp}(h) \cap \text{Supp}(c)| = 1$. In this case $\text{supp}(g) = \text{supp}(h) + 3$ and $\varepsilon_0 = \varepsilon_1 = \varepsilon_2 = 0$. Thus, $r_4(g) - r_4(h) = 1$.

Case 3: $|\text{Supp}(h) \cap \text{Supp}(c)| = 2$. In this case $\text{supp}(g) \leq \text{supp}(h) + 2$.

Subcase 3-1: $c$ has some common points with two cycles of $h$. In this case $\text{supp}(g) = \text{supp}(h) + 2$. We can describe this situation with the following product of permutations

$$(I_1 \iota_1)(I_2 \iota_2)(I_3 \iota_1 I_4 \iota_2) = (I_1 I_4 \iota_2 I_2 I_3 \iota_1),$$

where $\iota_i$'s are distinct numbers in $\{1, 2, \ldots, n\}$ and $I_i$'s are arbitrary sequences of numbers (maybe empty) and for $i \neq j$, $I_i$ and $I_j$ are disjoint. Suppose that

$$(I_1 \iota_1) \in C_{x_1}, \ (I_2 \iota_2) \in C_{x_2}, \ c = (I_3 \iota_1 I_4 \iota_2) \in C_1, \ (I_1 I_4 \iota_2 I_2 I_3 \iota_1) \in C_{y_1}.$$  

Since

$$| (I_1 \iota_1) | + | (I_2 \iota_2) | + | c | - 2 = | (I_1 I_4 \iota_2 I_2 I_3 \iota_1) |,$$

we have $x_1 + x_2 \equiv y_1 - 2 \ (\text{mod } 3)$. By Lemma 3.7, for $c = -2$, $X = \{x_1, x_2\}$ and $Y = \{y_1\}$, we have $r_4(g) - r_4(h) \leq 1$.

Subcase 3-2: $c$ has two common points with just one cycle of $h$. We can describe this situation with the following product of permutations,

$$(I_1 \iota_1 I_2 \iota_2)(I_3 \iota_1 I_4 \iota_2) = (I_1 I_4 \iota_2)(\iota_1 I_2 I_3),$$
where for \( i \neq j, I_i \text{ and } I_j \) are disjoint and \( \iota_i \neq \iota_j \).

Subcase 3-2-1: If \( I_1 \cup I_4 \) and \( I_2 \cup I_3 \) are non-empty, then

\[
(I_1 \iota_1 I_2 \iota_2) \in C_{x_1}, \quad c = (I_3 \iota_1 I_4 \iota_2) \in C_1, \quad (I_1 I_4 \iota_2) \in C_{y_1}, \quad (\iota_1 I_2 I_3) \in C_{y_2},
\]

So \( x_1 + 2 \equiv y_1 + y_2 \pmod{3} \). In this case \( \text{supp}(g) = \text{supp}(h) + 2 \). By Lemma 3.7, for \( c = -2 \), \( X = \{x_1\} \) and \( Y = \{y_1, y_2\} \), we have \( r_4(g) - r_4(h) \leq 1 \).

Subcase 3-2-2: At least one of the \( I_1 \cup I_4 \) and \( I_2 \cup I_3 \) is empty; if for example, \( I_1 \) and \( I_4 \) are empty, then

\[
(\iota_1 I_2 \iota_2) \in C_{x_1}, \quad c = (I_3 \iota_1 \iota_2) \in C_1, \quad (\iota_1 I_2 I_3) \in C_{y_1}.
\]

Thus, \( (\iota_1 I_2 \iota_2)(I_3 \iota_1 \iota_2) = (\iota_1 I_2 I_3) \), and \( x_1 + 1 \equiv y_1 \pmod{3} \). In this case \( \text{supp}(g) = \text{supp}(h) + 1 \). By Lemma 3.7, for \( c = -1 \), \( X = \{x_1\} \) and \( Y = \{y_1\} \), we have \( r_4(g) - r_4(h) \leq 1 \).

Case 4: \( |\text{Supp}(h) \cap \text{Supp}(c)| = 3 \). Using Lemma 3.7 we can prove Inequality 3.5 similar to Case 3 by checking possible cases. We summarized these cases in Table 1. Note that in this table all \( I_i \)'s are non-empty and \( c = \text{supp}(h) - \text{supp}(g) \).

| Product | \( c \) | \( |X| \) | \( |Y| \) |
|----------|-----|-----|-----|
| \( (I_1 \iota_1 I_2 \iota_2 I_3 \iota_3)(I_4 \iota_1 \iota_2 \iota_3) = (I_1 \iota_2 I_3 \iota_4 \iota_1 \iota_2 \iota_3) \) | -1 | 1 | 1 |
| \( (I_1 \iota_1 I_2 \iota_2 I_3 \iota_3)(I_4 \iota_1 \iota_3 \iota_2) = (I_1 \iota_3)(I_1 \iota_2 \iota_4)(\iota_2 I_3) \) | -1 | 1 | 3 |
| \( (\iota_1 I_2 \iota_2 I_3 \iota_3)(I_4 \iota_1 \iota_3 \iota_2) = (\iota_1 I_2 \iota_4)(\iota_2 I_3) \) | 0 | 1 | 2 |
| \( (\iota_1 I_2 \iota_2 \iota_3)(I_4 \iota_1 \iota_3 \iota_2) = (\iota_1 I_2 \iota_4) \) | 1 | 1 | 1 |
| \( (I_1 \iota_1 I_2 \iota_2)(I_3 \iota_3)(I_4 \iota_1 \iota_2 \iota_3) = (I_1 \iota_2)(I_1 \iota_2 \iota_3 \iota_4) \) | -1 | 2 | 2 |
| \( (\iota_1 I_2 \iota_2)(I_3 \iota_3)(I_4 \iota_1 \iota_2 \iota_3) = (I_1 \iota_2 \iota_3 \iota_4) \) | 0 | 2 | 1 |
| \( (I_1 \iota_1)(I_2 \iota_2)(I_3 \iota_3)(I_4 \iota_1 \iota_2 \iota_3) = (I_1 \iota_2 \iota_3 \iota_4 \iota_1) \) | -1 | 3 | 1 |

**Table 1.** Case 4 of Theorem 3.8

Case 5: \( |\text{Supp}(h) \cap \text{Supp}(c)| = 4 \). Similar to Case 4, we can prove Inequality 3.5 by checking possible cases. We checked these cases in Table 2. Note that in this table all \( I_i \)'s are non-empty and \( c = \text{supp}(h) - \text{supp}(g) \).
Proof. As a result, we have

\[ (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_4 t_1 t_2 t_3) = (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_1 t_2 t_3 t_4) \]

We have

\[ c_0 \leq 2 \]

\[ c_1 \leq 3 \]

\[ c_2 \leq 4 \]

\[ c_3 \leq 5 \]

\[ j \leq 6 \]

\[ k \leq 7 \]

\[ g \leq 8 \]

\[ \left\lceil \frac{n}{2} \right\rceil \]

\[ \left\lfloor \frac{(n-2)}{(2k)} \right\rfloor \]

\[ \left\lceil \frac{(n-2)}{(2k)} \right\rceil + 1 \]

\[ 2 \nmid k \]

\[ 2 \nmid g \]

\[ \frac{r_4(g)}{k} \]

\[ \frac{r_4(g)}{k} + 1 \]

\[ 2 \mid u \]

\[ 2 \nmid u \]

\[ 2 \nmid k \]

\[ \left\lceil \frac{(n-2)}{(2k)} \right\rceil - r_4(g) \]

\[ d_{k,4}(1, g) \]

| Product | \( c \) | \(|X|\) | \(|Y|\) |
|---------|------|-----|-----|
| \( (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_4 t_1 t_2 t_3) = (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_1 t_2 t_3 t_4) \) | 0 | 1 | 2 |
| \( (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_4 t_1 t_2 t_3) = (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_1 t_2 t_3 t_4) \) | 0 | 1 | 2 |
| \( (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_4 t_1 t_3 t_2) = (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_1 t_2 t_3 t_4) \) | 1 | 1 | 1 |
| \( (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_4 t_3 t_2 t_1) = (I_1 t_1 I_2 t_2 I_3 t_3 I_4 t_4)(t_1 t_3 t_4 t_2) \) | 0 | 1 | 4 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_3 t_2 t_1) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_2 t_3 t_4) \) | 1 | 1 | 3 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_3 t_2 t_1) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_2 t_3 t_4) \) | 2 | 1 | 2 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_3 t_2 t_1) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_2 t_3 t_4) \) | 3 | 1 | 1 |
| \( (t_1 t_2 t_3 t_4)(t_4 t_3 t_2 t_1) = 1 \) | - | - | - |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_2 t_3) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_1 t_2 t_3 t_4) \) | 0 | 2 | 1 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_1 t_3 t_4 t_2) \) | 0 | 2 | 3 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_1 t_3 t_4 t_2) \) | -1 | 2 | 2 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_1 t_3 t_4 t_2) \) | 2 | 1 | 2 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_1 t_3 t_4 t_2) \) | 0 | 2 | 3 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_1 t_3 t_4 t_2) \) | 1 | 2 | 2 |
| \( (t_1 t_2 t_3 t_4)(t_4 t_3 t_2 t_1) = (t_1 t_2 t_3 t_4)(t_4 t_3 t_2 t_1) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_2 t_3) \) | 2 | 2 | 1 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) \) | 0 | 2 | 1 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) \) | 0 | 3 | 2 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) \) | 1 | 3 | 1 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) \) | 0 | 3 | 2 |
| \( (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) = (I_1 I_2 t_1 I_3 t_2 I_4 t_3)(t_4 t_1 t_3 t_2) \) | 0 | 4 | 1 |

| Table 2. Case 5 of Theorem 3.8 |

It is easily seen that in the case \((t_1 t_2 t_3 t_4)(t_4 t_3 t_2 t_1) = 1\) in Table 2, the desired inequality holds. As a result, we have \(r_4(g) - r_4(h) \leq 1\) for all cases. This completes the proof. \(\square\)

As an immediate consequence of Theorem 3.8 and Theorem 3.1 the following corollary holds.

**Corollary 3.9.** By the above notations, we have

\[ d_{k,4}(1, g) = \begin{cases} \left\lceil \frac{r_4(g)}{k} \right\rceil & \text{if } 2 \mid u \\ \left\lceil \frac{r_4(g)}{k} \right\rceil + 1 & \text{if } 2 \nmid u, \end{cases} \]

where \(u = k \left\lceil \frac{r_4(g)}{k} \right\rceil - r_4(g)\).

**Corollary 3.10.** We have

\[ \text{diam}(\Gamma_{k,4}^n) = \begin{cases} \left\lceil \frac{(n-2)}{(2k)} \right\rceil & \text{if } 2 \mid k \\ \left\lceil \frac{(n-2)}{(2k)} \right\rceil + 1 & \text{if } 2 \nmid k. \end{cases} \]

**Proof.** We find the maximum value of the function \(d_{k,4}(1, g)\), denoted by \(d_1\), for suitable permutation \(g\) in the generated group by \(\Omega_{k,4}^n\). For every permutation \(g\), suppose that \(b_g\) is the remainder of \(r_4(g)\)
divided by \( k \). It is clear that for \( u_g = k[r_4(g)/k] - r_4(g) \), we have \( 2|u_g \) if and only if \( k| r_4(g) \) or \( 2|(k - b_g) \).

Case 1: Suppose that \( 2|k \). In this case \( \Gamma^u_{k,A} = Cay(A_n, \Omega^n_{k,A}) \). For every permutation \( g \) in \( A_n \) we have \( 2| r_4(g) \); hence \( 2|b_g \) and \( 2|u_g \).

Subcase 1-1: \( 4|n \). In this case it is easily seen that \( g = (12)(34) \cdots (n - 1 \ n) \) gives \( d_\Gamma \). By Corollary 3.9, \( d_{k,A}(1, g) = \lceil n/(2k) \rceil \). Since \( 2k \nmid n - 1 \) and \( 2k \nmid n - 2 \), we have \( \lceil n/(2k) \rceil = \lceil (n - 2)/(2k) \rceil \). Thus, \( \text{diam}(\Gamma^u_{k,A}) = \lceil (n - 2)/(2k) \rceil \).

Subcase 1-2: Suppose that \( n \equiv 1 \pmod{4} \). In this case it is easily checked that \( g = (12)(34) \cdots (n - 2 \ n - 1) \) gives \( d_\Gamma \). Since \( 2k \nmid n - 2 \) and \( d_{k,A}(1, g) = \lceil (n - 1)/(2k) \rceil \), we have

\[
\text{diam}(\Gamma^u_{k,A}) = \lceil \frac{n - 1}{2k} \rceil = \lceil \frac{n - 2}{2k} \rceil.
\]

Subcase 1-3: Let \( n \equiv 2 \pmod{4} \). Since \( g = (12)(45) \cdots (n - 3 \ n - 2) \) gives \( d_\Gamma \), we have \( \text{diam}(\Gamma^u_{k,A}) = \lceil (n - 2)/(2k) \rceil \).

Subcase 1-4: \( n \equiv 3 \pmod{4} \). In this case it is easily checked that \( g = (123)(45) \cdots (n - 1 \ n) \) gives \( d_\Gamma \). Since \( 2k \nmid n \), \( 2k \nmid n - 1 \) and \( 2k \nmid n - 2 \), we have

\[
\text{diam}(\Gamma^u_{k,A}) = \lceil \frac{n + 1}{2k} \rceil = \lceil \frac{n - 2}{2k} \rceil.
\]

Case 2: Suppose that \( 2 \nmid k \) and \( 2|n \). In this case \( \Gamma^u_{k,A} = Cay(S_n, \Omega^n_{k,A}) \). Let \( g_1 = (12)(34) \cdots (n - 1 \ n) \) and \( g_2 = (12)(34) \cdots (n - 3 \ n - 2) \). Thus, \( r_4(g_1) = n/2 \) and \( r_4(g_2) = n/2 - 1 \).

Subcase 2-1: Let \( 2 \nmid u_{g_1} \). In this case it is easily checked that \( g_1 \) gives \( d_\Gamma \). By Corollary 3.9, \( r_4(g) = \lceil n/(2k) \rceil + 1 \). Since \( 2 \nmid u_{g_1} \), we have \( b_{g_1} \neq 1 \) and \( k \nmid n/2 - 1 \). So, \( 2k \nmid n - 2 \). Thus, \( \lceil n/(2k) \rceil = \lceil (n - 2)/(2k) \rceil \).

Subcase 2-2: If \( 2 \nmid u_{g_2} \) then \( g_2 \) gives \( d_\Gamma \). By Corollary 3.9, we have \( r_4(g) = \lceil (n - 2)/(2k) \rceil + 1 \).

Subcase 2-3: Let \( 2|u_{g_1} \) and \( 2|u_{g_2} \). In this case it is easily seen that \( g_1 \) gives \( d_\Gamma \). If we show that \( k|n/2 - 1 \) then \( \lceil n/(2k) \rceil = \lceil (n - 2)/(2k) \rceil + 1 \). Suppose that, on the contrary, \( k \nmid n/2 - 1 \). Since \( 2|u_{g_2} \), \( 2 \nmid b_{g_2} \). Hence \( 2|b_{g_1} \). So, \( k|n/2 \) and \( b_{g_1} = 0 \). Thus, \( b_{g_2} = k - 1 \) and \( 2|k \), which is a contradiction.

Case 3: Suppose that \( 2 \nmid k \) and \( 2 \nmid n \). In this case \( \Gamma^u_{k,A} = Cay(S_n, \Omega^n_{k,A}) \). Let \( g_3 = (123)(45) \cdots (n - 1 \ n) \) and \( g_4 = (12)(34) \cdots (n - 2 \ n - 1) \). It is easily checked that \( r_4(g_3) = (n + 1)/2 \) and \( r_4(g_2) = (n - 1)/2 \).

Subcase 3-1: Let \( 2 \nmid u_{g_3} \). In this case it is easily seen that \( g_3 \) gives \( d_\Gamma \). By Corollary 3.9, \( r_4(g_3) = \lceil (n + 1)/(2k) \rceil + 1 \). Since \( 2 \nmid u_{g_3} \), we have \( b_{g_3} \neq 1 \) and \( k \nmid (n - 1)/2 \). Therefore, \( 2k \nmid n - 1 \). Thus, \( \lceil (n + 1)/(2k) \rceil = \lceil (n - 2)/(2k) \rceil \).

Subcase 3-2: If \( 2 \nmid u_{g_4} \) then \( g_4 \) gives \( d_\Gamma \). Thus,

\[
\text{diam}(\Gamma^u_{k,A}) = r_4(g_4) = \lceil (n - 1)/(2k) \rceil + 1 = \lceil (n - 2)/(2k) \rceil + 1.
\]

Subcase 3-3: Let \( 2|u_{g_3} \) and \( 2|u_{g_4} \). In this case it is easily checked that \( g_3 \) gives \( d_\Gamma \). If we show that \( k|(n + 1)/2 - 1 \) then \( \lceil (n + 1)/(2k) \rceil = \lceil (n - 2)/(2k) \rceil + 1 \). Suppose that, on the contrary, \( k \nmid (n - 1)/2 \). Since \( 2|u_{g_4} \), we have \( 2 \nmid b_{g_4} \) and \( 2|b_{g_3} \). Therefore, \( k|(n + 1)/2 \) and \( b_{g_3} = 0 \). Thus, \( b_{g_4} = k - 1 \) and \( 2|k \), which is a contradiction.
4. Improvement of an Algorithm

**Algorithm 1:** An algorithm for finding a short expression of a permutation as products of given permutations

**Input:** Permutations \(s_1, s_2, \ldots, s_t\) in \(S_n\);

permutation \(s\) in \(S_n\) that can be generated by \(s_i\)'s.

**Output:** Find a short expression for \(s\).

**Step 1:** Find a good permutation in \(\langle s_1, s_2, \ldots, s_t \rangle\).

foreach \(\tau \in \langle s_1, s_2, \ldots, s_t \rangle\) do

for \(m = 1\) to \(n\) do

if \(\tau^m\) is a good permutation OR \(\tau^m\) and \(s\) have same cycle type

\[\mu \leftarrow \tau^m\]

Go to Step 2.

end

end

return fail

**Step 2:** Find a short expression for the additional good permutations.

Set \(C\) as the set of all permutations needed for expressing \(s\) as products of the permutations of the same cycle type of \(\mu\).

\[A_0 \leftarrow \{\mu\}\]

for \(l = 1\) to maximum-tries do

\[A_l \leftarrow \emptyset\]

foreach \(i \in \{1, 2, \ldots, t\}\) each \(\epsilon \in \{1, -1\}\) and each \(a \in A_{l-1}\) do

if \(s_i^{-\epsilon}as_i^\epsilon \notin \bigcup_{j=0}^{l-1} A_j\) then

Add \(s_i^{-\epsilon}as_i^\epsilon\) to \(A_l\).

if \(C \subseteq \bigcup_{j=0}^{l-1} A_j\) then

Go to Step 3.

end

end

end

return fail

**Step 3:** Find a short expression for \(s\) according to the algorithms presented in the previous sections using the good permutations in \(C\).

In [6], authors presented an algorithm for expressing a permutation by given generating set of \(G = S_n\) or \(A_n\). We call a permutation a good permutation if, it is a transposition, 3-cycle or 4-cycle, The main difference between Algorithm 1 and the algorithm in [6] is in the definition of the good
permutation. In [6], authors did not consider 4-cycles as a good permutation. By using the algorithm in the proof of Lemma 3.6 we can express a permutation as products of 4-cycles. According to our experiments for $n = 8, 16, 32, 64, 128$, depending on $n$, in the more than 35 percent of the cases, Step 1 of the Algorithm 1 returns a 4-cycle, that in general causes a shorter expression. Note that, the Algorithm 1 as its origin in [6] will not necessarily returns a shortest expression. Unlike the algorithm in [6], we do not specific the group $G$ in the input of Algorithm 1. It causes shorter runtime in most cases. If we interested in quicker algorithm rather than shorter result, we can drop 4-cycles from the definition of good permutation. For the proof and more details of Algorithm 1 we refer the reader to the proof of the origin algorithm in [6].

5. Conclusion

We find the distance function and the diameter for $\Gamma_{k,m}^n$, a family of Cayley graphs, for $m = 2, 3, 4$. This problem for $\Gamma_{m}^n$ is an interesting open problem. In Section 4 we improve an algorithm that finds a short path in the Cayley graphs on permutation groups, which has applications in cryptography and biological mathematics.

REFERENCES

Mohammad Hossein Ghaffari
School of Mathematics, Iran University of Science and Technology, Tehran, Iran
Email: mhghaffari@iust.ac.ir

Zohreh Mostaghim
Cryptography and Data Security Laboratory, School of Mathematics, Iran University of Science and Technology, Tehran, Iran
Email: mostaghim@iust.ac.ir