DISTANCE IN CAYLEY GRAPHS ON PERMUTATION GROUPS GENERATED BY k m-CYCLES

2 authors:

Mohammad Hossein Ghaffari B.
Iran University of Science and Technology

Zohreh Mostaghim
Iran University of Science and Technology

toc.ui.ac.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 6 No. 3 (2017), pp. 45-59.

www.ui.ac.ir

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. Suceavă 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 $\Omega^n_{k,m}$ be the set of all permutations of the form $c_1c_2\cdots c_k$ where c_i's are arbitrary m-cycles in S_n. Suppose that $\Gamma^n_{k,m}$ be the Cayley graph on subgroup of S_n generated by all permutations in $\Omega^n_{k,m}$. We find a shortest path joining identity and any vertex of $\Gamma^n_{k,m}$, 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 Ω a subset of G that generates it. We assume that Ω 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 Ω. The *distance* between the vertices g and g' in Γ, 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 Γ is the maximum distance among the vertices of Γ.

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 $mk \le n$, suppose that $\Omega^n_{k,m}$ be the set of all permutations of the form $c_1c_2\cdots c_k$ where c_i's are arbitrary m-cycles, and $\Omega^n_{m^k}$ be the set of all permutations with cycle type m^k in S_n. Let G be the subgroup of S_n generated by generating set $\Omega^n_{k,m}$ (respectively, $\Omega^n_{m^k}$). 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 $\Omega^n_{k,m}$ (respectively, $\Omega^n_{m^k}$) by $\Gamma^n_{k,m}$ (respectively, $\Gamma^n_{m^k}$). We will omit superscript when it is clear from the context. We denote the distance function on $\Gamma^n_{k,m}$ (respectively, $\Gamma^n_{m^k}$) by $d_{k,m}$ (respectively, d_{m^k}). In this paper, we find a shortest path joining identity and any vertex of $\Gamma^n_{k,m}$, 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:

$$g = \prod_{i=1}^{t} a_i, \tag{2.1}$$

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,*

$$a_i = (\alpha_{i1}\ \alpha_{i2}\ \alpha_{i3}\cdots\ \alpha_{il_{a_i}}), \quad i = 1, 2, 3, \ldots, t.$$

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

$$g = \prod_{i=1}^{t} (\alpha_{i1}\ \alpha_{i2})(\alpha_{i1}\ \alpha_{i3})\cdots(\alpha_{i1}\ \alpha_{il_{a_i}}), \tag{2.2}$$

and we have,

$$d_{1,2}(1, g) = supp(g) - t. \tag{2.3}$$

Let h be a non-trivial element of A_n. In disjoint cycle decomposition of h we have:

$$h = \prod_{i=1}^{s} a_i \prod_{j=1}^{k} b_j c_j, \tag{2.4}$$

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,*

$$a_i = (\alpha_{i1}\ \alpha_{i2}\ \alpha_{i3} \cdots\ \alpha_{il_{a_i}}),$$
$$b_i = (\beta_{i1}\ \beta_{i2}\ \beta_{i3} \cdots\ \beta_{il_{b_i}}),$$
$$c_i = (\gamma_{i1}\ \gamma_{i2}\ \gamma_{i3} \cdots\ \gamma_{il_{c_i}}),$$

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

$$\begin{aligned} h = &\prod_{i=1}^{s} (\alpha_{i1}\ \alpha_{i2}\ \alpha_{i3})(\alpha_{i1}\ \alpha_{i4}\ \alpha_{i5}) \cdots (\alpha_{i1}\ \alpha_{il_{a_i}-1}\ \alpha_{il_{a_i}}) \\ &\prod_{j=1}^{k} (\beta_{j1}\ \gamma_{j1}\ \gamma_{j2})(\beta_{j1}\ \gamma_{j1}\ \beta_{j2}) \\ &(\beta_{j1}\ \beta_{j3}\ \beta_{j4})(\beta_{j1}\ \beta_{j5}\ \beta_{j6}) \cdots (\beta_{j1}\ \beta_{jl_{b_j}-1}\ \beta_{jl_{b_j}}) \\ &(\gamma_{j1}\ \gamma_{j3}\ \gamma_{j4})(\gamma_{j1}\ \gamma_{j5}\ \gamma_{j6}) \cdots (\gamma_{j1}\ \gamma_{jl_{c_j}-1}\ \gamma_{jl_{c_j}}). \end{aligned} \tag{2.5}$$

and we have,

$$d_{1,3}(1,h) = \Big(supp(h) - s\Big)/2, \tag{2.6}$$

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

3. On Cayley graph $\Gamma^n_{k,m}$

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 $\Omega^n_{m^k}$ is a subset of $\Omega^n_{k,m}$, the following theorem finds a lower bound for $d_{m^k}(1,g)$.

Theorem 3.1. *In $\Gamma^n_{k,m}$ we have,*

$$d_{k,m}(1,g) = \begin{cases} \lceil d_{1,m}(1,g)/k \rceil & \text{if} \quad 2 \nmid m \text{ or } 2|u \\ \lceil d_{1,m}(1,g)/k \rceil + 1 & \text{if} \quad 2|m \text{ and } 2 \nmid u, \end{cases}$$

where,

$$u = k\lceil d_{1,m}(1,g)/k \rceil - d_{1,m}(1,g).$$

Proof. We prove the theorem by presenting the desired path in $\Gamma^n_{k,m}$. 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: $2|u$. Set $y_i = c_i$ for $1 \leq i \leq t$. For $t+1 \leq i \leq t+u$ if $2|i$, then we set $y_i = c_t$ and otherwise $y_i = c_t^{-1}$. 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 $y_t = y_{t+1} = c_t^v$. 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 $2|i$, then we set $y_i = c_t$ and otherwise $y_i = c_t^{-1}$. We have, $\prod_{i=1}^{t+u} y_i = g$.

Case 3: $2 \nmid u$ and $2|m$. 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 $2|i$, then we set $y_i = c_t$ and otherwise $y_i = c_t^{-1}$. 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 $h_i \in \Omega^n_{k,m}$ 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. $\square$

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

Corollary 3.2. *We have,*

$$d_{k,2}(1, g) = \begin{cases} \lceil d_{1,2}(1, g)/k \rceil & \text{if} \quad 2|u \\ \lceil d_{1,2}(1, g)/k \rceil + 1 & \text{if} \quad 2 \nmid u, \end{cases}$$

where,

$$u = k\lceil d_{1,2}(1, g)/k \rceil - d_{1,2}(1, g)\,, \quad d_{1,2}(1, g) = supp(g) - t,$$

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

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

Corollary 3.3. *We have,*

$$diam(\Gamma^n_{k,2}) = \begin{cases} \lceil (n-2)/k \rceil & \text{if} \quad 2|k \\ \lceil (n-2)/k \rceil + 1 & \text{if} \quad 2 \nmid k. \end{cases}$$

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

Case 1: Suppose that $2|k$. In this case $\Gamma^n_{k,2} = Cay(A_n, \Omega^n_{k,2})$. For every permutation g in A_n we have $2|d_{1,2}(1, g)$. So, $2|b_g$. Since $2|k$, we have $2|u_g$.

Subcase 1-1: $2|n$. In this case, it is easily seen that $g_2 = (1\,2\ \cdots\ n-1)$ gives d_Γ. By Proposition 2.1,

we have $d_{1,2}(1,g_2) = n-2$. So, $\mathrm{diam}(\Gamma^n_{k,2}) = \lceil (n-2)/k \rceil$.
Subcase 1-2: $2 \nmid n$. In this case $g_1 = (1\,2\ \cdots\ n)$ gives d_Γ. By Proposition 2.1, we have $d_{1,2}(1,g_1) = n-1$. Since $2 \nmid (n-2)$, $k \nmid (n-2)$. Thus,

$$\mathrm{diam}(\Gamma^n_{k,2}) = \left\lceil \frac{n-1}{k} \right\rceil = \left\lceil \frac{n-2}{k} \right\rceil.$$

Case 2: Suppose that $2 \nmid k$. In this case $\Gamma^n_{k,2} = Cay(S_n, \Omega^n_{k,2})$. So, both $g_1 = (1\,2\ \cdots\ n)$ and $g_2 = (1\,2\ \cdots\ n-1)$ belong to the vertex set of $\Gamma^n_{k,2}$.
Subcase 2-1: $2 \nmid u_{g_1}$. In this case g_1 gives d_Γ. 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,

$$\mathrm{diam}(\Gamma^n_{k,2}) = \left\lceil \frac{n-1}{k} \right\rceil + 1 = \left\lceil \frac{n-2}{k} \right\rceil + 1.$$

Subcase 2-2: $2 \nmid u_{g_2}$. In this case, it is easily seen that g_2 gives d_Γ. So, $\mathrm{diam}(\Gamma^n_{k,2}) = \lceil (n-2)/k \rceil + 1$.
Subcase 2-3: $2|u_{g_1}$ and $2|u_{g_2}$. If we show that $k|n-2$, then,

$$\mathrm{diam}(\Gamma^n_{k,2}) = \left\lceil \frac{n-1}{k} \right\rceil = \left\lceil \frac{n-2}{k} \right\rceil + 1.$$

Suppose that, on the contrary, $k \nmid n-2$. Since $2|u_{g_2}$, we have $2|k - b_{g_2}$. So, $2 \nmid k - b_{g_1}$ and $k|n-1$. Thus, $b_{g_2} = k-1$; which contradicts $2|k - b_{g_2}$. □

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

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

$$d_{k,3}(1,g) = \left\lceil \frac{supp(g) - s}{2k} \right\rceil.$$

Corollary 3.5. *The diameter of* $\Gamma_{k,3}$ *is* $\lceil \lfloor \frac{n}{2} \rfloor / k \rceil$.

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

$$g = \prod_{i=1}^{c_0(g)} \alpha_i \prod_{j=1}^{c_1(g)} \beta_j \prod_{l=1}^{c_2(g)} \gamma_l \tag{3.1}$$

where $c_i(g)$'s are non-negative integer numbers, α_i's are $3m$-length cycles, β_j's are $(3m+1)$-length cycles with $|\beta_j| \geq 4$, γ_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*

$$r_4(g) = \frac{supp(g) + c_2(g) - c_1(g)}{3} + \frac{1 - (-1)^{c_0(g)}}{2}, \tag{3.2}$$

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

$$\begin{aligned}\alpha_i &= (\alpha_{i\,1}\ \alpha_{i\,2}\ \alpha_{i\,3} \cdots\ \alpha_{i\,l_{\alpha_i}}),\\ \beta_i &= (\beta_{i\,1}\ \beta_{i\,2}\ \beta_{i\,3} \cdots\ \beta_{i\,l_{\beta_i}}),\\ \gamma_i &= (\gamma_{i\,1}\ \gamma_{i\,2}\ \gamma_{i\,3} \cdots\ \gamma_{i\,l_{\gamma_i}}).\end{aligned}$$

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 γ_l's is more than 4, replace any $\gamma_i\gamma_j\gamma_t$ by $(|\gamma_i| + |\gamma_j| + |\gamma_t|)/3 + 1$ number of 4-cycles,

$$\begin{aligned}\gamma_i\gamma_j\gamma_t = {}& (\gamma_{i\,1}\ \gamma_{j\,1}\ \gamma_{t\,2}\ \gamma_{i\,2})(\gamma_{i\,2}\ \gamma_{j\,2}\ \gamma_{t\,2}\ \gamma_{j\,1})(\gamma_{j\,1}\ \gamma_{j\,2}\ \gamma_{t\,1}\ \gamma_{t\,2})\\ & \prod_{l=1}^{(|\gamma_i|-2)/3} (\gamma_{i\,1}\ \gamma_{i\,3l}\ \gamma_{i\,3l+1}\ \gamma_{i\,3l+2}) \prod_{l=1}^{(|\gamma_j|-2)/3} (\gamma_{j\,1}\ \gamma_{j\,3l}\ \gamma_{j\,3l+1}\ \gamma_{j\,3l+2})\\ & \prod_{l=1}^{(|\gamma_t|-2)/3} (\gamma_{t\,1}\ \gamma_{t\,3l}\ \gamma_{t\,3l+1}\ \gamma_{t\,3l+2}).\end{aligned}$$

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

$$\begin{aligned}\gamma_i\gamma_t = {}& (\gamma_{i\,1}\ \gamma_{t\,1}\ \gamma_{i\,2}\ \gamma_{t\,2})(\gamma_{i\,1}\ \gamma_{t\,1}\ \gamma_{i\,2}\ \gamma_{t\,2})\\ & \prod_{j=1}^{(|\gamma_i|-2)/3} (\gamma_{i\,1}\ \gamma_{i\,3j}\ \gamma_{i\,3j+1}\ \gamma_{i\,3j+2}) \prod_{l=1}^{(|\gamma_t|-2)/3} (\gamma_{t\,1}\ \gamma_{t\,3l}\ \gamma_{t\,3l+1}\ \gamma_{t\,3l+2}).\end{aligned}$$

So, after doing this step, there is at most one γ_j in g.

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

$$\begin{aligned}\gamma_i\beta_t = {}& (\beta_{t\,1}\ \beta_{t\,2}\ \gamma_{i\,1}\ \gamma_{i\,2})(\beta_{t\,1}\ \gamma_{i\,1}\ \beta_{t\,3}\ \beta_{t\,4})\\ & \prod_{j=1}^{(|\gamma_i|-2)/3} (\gamma_{i\,1}\ \gamma_{i\,3j}\ \gamma_{i\,3j+1}\ \gamma_{i\,3j+2}) \prod_{l=1}^{(|\beta_t|-4)/3} (\beta_{t\,1}\ \beta_{t\,3l+2}\ \beta_{t\,3l+3}\ \beta_{t\,3l+4}).\end{aligned}$$

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,

$$\begin{aligned}\gamma_i\alpha_t\alpha_q = {}& (\alpha_{t\,1}\ \alpha_{q\,3}\ \gamma_{i\,2}\ \gamma_{i\,1})(\alpha_{t\,1}\ \gamma_{i\,2}\ \alpha_{q\,1}\ \alpha_{q\,2})(\alpha_{t\,1}\ \alpha_{q\,3}\ \alpha_{t\,2}\ \alpha_{t\,3})\\ & \prod_{j=1}^{|\alpha_t|/3-1} (\alpha_{t\,1}\ \alpha_{t\,3j+1}\ \alpha_{t\,3j+2}\ \alpha_{t\,3j+3}) \prod_{j=1}^{|\alpha_q|/3-1} (\alpha_{q\,1}\ \alpha_{q\,3j+1}\ \alpha_{q\,3j+2}\ \alpha_{q\,3j+3})\\ & \prod_{j=1}^{(|\gamma_i|-2)/3} (\gamma_{i\,1}\ \gamma_{i\,3j}\ \gamma_{i\,3j+1}\ \gamma_{i\,3j+2}).\end{aligned}$$

As a result, after doing this step, either we have no γ_i in g, or there is at most one α_j in g.
Step 5. Replace any $\gamma_i\alpha_t$ by $(|\gamma_i| + |\alpha_t| + 4)/3$ number of 4-cycles,

$$\gamma_i\alpha_t = (\alpha_{t\,1}\ \alpha_{t\,3}\ \gamma_{i\,1}\ \gamma_{i\,2})(\alpha_{t\,1}\ \gamma_{i\,1}\ \gamma_{i\,2}\ \alpha_{t\,2})(\alpha_{t\,1}\ \alpha_{t\,3}\ \alpha_{t\,2}\ \gamma_{i\,2}) \prod_{j=1}^{|\alpha_t|/3-1} (\alpha_{t\,1}\ \alpha_{t\,3j+1}\ \alpha_{t\,3j+2}\ \alpha_{t\,3j+3}) \prod_{l=1}^{(|\gamma_i|-2)/3} (\gamma_{i\,1}\ \gamma_{i\,3l}\ \gamma_{i\,3l+1}\ \gamma_{i\,3l+2}).$$

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

$$\alpha_i\alpha_t = (\alpha_{i\,1}\ \alpha_{t\,1}\ \alpha_{t\,2}\ \alpha_{t\,3})(\alpha_{i\,1}\ \alpha_{t\,1}\ \alpha_{i\,2}\ \alpha_{i\,3}) \prod_{j=1}^{|\alpha_i|/3-1} (\alpha_{i\,1}\ \alpha_{i\,3j+1}\ \alpha_{i\,3j+2}\ \alpha_{i\,3j+3}) \prod_{l=1}^{|\alpha_t|/3-1} (\alpha_{t\,1}\ \alpha_{t\,3l+1}\ \alpha_{t\,3l+2}\ \alpha_{t\,3l+3}).$$

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

$$\alpha_i = (\alpha_{i\,1}\ \alpha_{i\,3}\ \delta\ \alpha_{i\,2})(\alpha_{i\,1}\ \alpha_{i\,3}\ \alpha_{i\,2}\ \delta) \prod_{j=1}^{|\alpha_i|/3-1} (\alpha_{i\,1}\ \alpha_{i\,3j+1}\ \alpha_{i\,3j+2}\ \alpha_{i\,3j+3}),$$

where δ is an arbitrary number in the $\{1, 2, \ldots, n\} \setminus \{\alpha_{i\,1}, \alpha_{i\,2}, \alpha_{i\,3}\}$.
Step 8. Replace any β_i by $(|\beta_i| - 1)/3$ number of 4-cycles,

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

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

$$\gamma_i = (\gamma_{i\,1}\ \gamma_{i\,5}\ \gamma_{i\,3}\ \gamma_{i\,4})(\gamma_{i\,1}\ \gamma_{i\,5}\ \gamma_{i\,2}\ \gamma_{i\,3}) \prod_{j=2}^{(|\gamma_i|-2)/3} (\gamma_{i\,1}\ \gamma_{i\,3j}\ \gamma_{i\,3j+1}\ \gamma_{i\,3j+2}).$$

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:

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

$\square$

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

$$\varepsilon_j = \Big|\{y \in Y \mid y \equiv j \pmod 3\}\Big| - \Big|\{x \in X \mid x \equiv j \pmod 3\}\Big|.$$

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 $|X| + |Y| < |c \pm 6|$ and exactly one of the c and $|Y| - |X|$ is an even integer, then*

$$\delta = max\Big\{\frac{\varepsilon_2 - \varepsilon_1 - c}{3} \pm \frac{1-(-1)^{\varepsilon_0}}{2}\Big\} \leq 1. \tag{3.3}$$

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 ε_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 $z \in \{-1, 0, 1\}$,

$$\begin{aligned}\varepsilon_0 &= |Y| - |X| + \sum_{x\in X} x^2 - \sum_{y\in Y} y^2 \\ &\equiv |Y| - |X| + \sum_{x\in X} x - \sum_{y\in Y} y \pmod{2}.\end{aligned}$$

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 $|\varepsilon_2 - \varepsilon_1| < |c \pm 6|$. 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 $\delta = 1$. □

Theorem 3.8. *By the above notations, for arbitrary permutation g, we have:*

$$d_{1,4}(1, g) = r_4(g). \tag{3.4}$$

Proof. Let $C_i(\rho)$ be the set of all cycles in disjoint cycle decomposition of permutation ρ 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 $|Supp(h) \cap Supp(c)|$ we show that

$$r_4(g) - r_4(h) \leq 1. \tag{3.5}$$

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 ρ, 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

$$r_4(g) - r_4(h) = \frac{supp(g) - supp(h) + \varepsilon_2 - \varepsilon_1}{3} \pm \frac{1 - (-1)^{\varepsilon_0}}{2}, \tag{3.6}$$

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

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

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

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

Subcase 3-1: c has some common points with two cycles of h. In this case $supp(g) = supp(h) + 2$. 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 ι_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

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

we have $x_1 + x_2 \equiv y_1 - 2 \pmod 3$. 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 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

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

So $x_1 + 2 \equiv y_1 + y_2 \pmod 3$, In this case $supp(g) = supp(h) + 2$. 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

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

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 $supp(g) = supp(h) + 1$. 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: $|Supp(h) \cap Supp(c)| = 3$. 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 $c = supp(h) - supp(g)$.

Product	c	$\lvert X\rvert$	$\lvert Y\rvert$
$(I_1\, \iota_1\, I_2\, \iota_2\, I_3\, \iota_3)(\iota_4\, \iota_1\, \iota_2\, \iota_3) = (I_1\, \iota_2\, I_3\, \iota_4\, \iota_1\, I_2\, \iota_3)$	-1	1	1
$(I_1\, \iota_1\, I_2\, \iota_2\, I_3\, \iota_3)(\iota_4\, \iota_1\, \iota_3\, \iota_2) = (I_1\, \iota_3)(\iota_1\, I_2\, \iota_4)(\iota_2\, I_3)$	-1	1	3
$(\iota_1\, I_2\, \iota_2\, I_3\, \iota_3)(\iota_4\, \iota_1\, \iota_3\, \iota_2) = (\iota_1\, I_2\, \iota_4)(\iota_2\, I_3)$	0	1	2
$(\iota_1\, I_2\, \iota_2\, \iota_3)(\iota_4\, \iota_1\, \iota_3\, \iota_2) = (\iota_1\, I_2\, \iota_4)$	1	1	1
$(I_1\, \iota_1\, I_2\, \iota_2)(I_3\, \iota_3)(\iota_4\, \iota_1\, \iota_2\, \iota_3) = (I_1\, \iota_2)(\iota_1\, I_2\, \iota_3\, I_3\, \iota_4)$	-1	2	2
$(\iota_1\, I_2\, \iota_2)(I_3\, \iota_3)(\iota_4\, \iota_1\, \iota_2\, \iota_3) = (\iota_1\, I_2\, \iota_3\, I_3\, \iota_4)$	0	2	1
$(I_1\, \iota_1)(I_2\, \iota_2)(I_3\, \iota_3)(\iota_4\, \iota_1\, \iota_2\, \iota_3) = (I_1\, \iota_2\, I_2\, \iota_3\, I_3\, \iota_4\, \iota_1)$	-1	3	1

TABLE 1. Case 4 of Theorem 3.8

Case 5: $|Supp(h) \cap Supp(c)| = 4$. 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 $c = supp(h) - supp(g)$.

Product	c	$\lvert X\rvert$	$\lvert Y\rvert$
$(I_1\,\iota_1\,I_2\,\iota_2\,I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2\,I_3\,\iota_4)(\iota_1\,I_2\,\iota_3\,I_4)$	0	1	2
$(I_1\,\iota_1\,I_2\,\iota_2\,I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1\,I_2\,\iota_4)(\iota_2\,I_3)$	0	1	2
$(I_1\,\iota_1\,I_2\,\iota_2\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1\,I_2\,\iota_4)$	1	1	1
$(I_1\,\iota_1\,I_2\,\iota_2\,I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_3\,\iota_2\,\iota_1) = (I_1\,\iota_4)(\iota_1\,I_2)(\iota_2\,I_3)(\iota_3\,I_4)$	0	1	4
$(I_1\,\iota_1\,I_2\,\iota_2\,I_3\,\iota_3\,\iota_4)(\iota_4\,\iota_3\,\iota_2\,\iota_1) = (I_1\,\iota_4)(\iota_1\,I_2)(\iota_2\,I_3)$	1	1	3
$(I_1\,\iota_1\,I_2\,\iota_2\,\iota_3\,\iota_4)(\iota_4\,\iota_3\,\iota_2\,\iota_1) = (I_1\,\iota_4)(\iota_1\,I_2)$	2	1	2
$(I_1\,\iota_1\,\iota_2\,\iota_3\,\iota_4)(\iota_4\,\iota_3\,\iota_2\,\iota_1) = (I_1\,\iota_4)$	3	1	1
$(\iota_1\,\iota_2\,\iota_3\,\iota_4)(\iota_4\,\iota_3\,\iota_2\,\iota_1) = 1$	-	-	-
$(I_1\,\iota_1)(I_2\,\iota_2\,I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2\,I_3\,\iota_4\,I_2\,\iota_3\,I_4\,\iota_1)$	0	2	1
$(I_1\,\iota_1)(I_2\,\iota_2\,I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1)(I_2\,\iota_4)(\iota_2\,I_3)$	0	2	3
$(I_1\,\iota_1)(I_2\,\iota_2\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1)(I_2\,\iota_4)$	-1	2	2
$(I_1\,\iota_1)(\iota_2\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1)$	2	1	2
$(I_1\,\iota_1\,I_2\,\iota_2)(I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2)(\iota_1\,I_2\,\iota_3\,I_4)(\iota_4\,I_3)$	0	2	3
$(I_1\,\iota_1\,I_2\,\iota_2)(\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2)(\iota_1\,I_2\,\iota_3\,I_4)$	1	2	2
$(\iota_1\,I_2\,\iota_2)(\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (\iota_1\,I_2\,\iota_3\,I_4)$	2	2	1
$(I_1\,\iota_1\,I_2\,\iota_2)(I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1\,I_2\,\iota_4\,I_3\,\iota_2)$,	0	2	1
$(I_1\,\iota_1)(I_2\,\iota_2)(I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2\,I_2\,\iota_3\,I_4\,\iota_1)(\iota_4\,I_3)$	0	3	2
$(I_1\,\iota_1)(I_2\,\iota_2)(\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2\,I_2\,\iota_3\,I_4\,\iota_1)$	1	3	1
$(I_1\,\iota_1)(I_2\,\iota_2)(I_3\,\iota_3\,I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_3\,\iota_2) = (I_1\,\iota_3\,I_4\,\iota_1)(\iota_2\,I_2\,\iota_4\,I_3)$	0	3	2
$(I_1\,\iota_1)(I_2\,\iota_2)(I_3\,\iota_3)(I_4\,\iota_4)(\iota_4\,\iota_1\,\iota_2\,\iota_3) = (I_1\,\iota_2\,I_2\,\iota_3\,I_3\,\iota_4\,I_4\,\iota_1)$,	0	4	1

TABLE 2. Case 5 of Theorem 3.8

It is easily seen that in the case $(\iota_1\,\iota_2\,\iota_3\,\iota_4)(\iota_4\,\iota_3\,\iota_2\,\iota_1) = 1$ in Table 2, the desired inequality holds. As a result, we have $r_4(g) - r_4(h) \le 1$ 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*

$$d_{k,4}(1,g) = \begin{cases} \lceil r_4(g)/k \rceil & \text{if} \quad 2|u \\ \lceil r_4(g)/k \rceil + 1 & \text{if} \quad 2 \nmid u, \end{cases}$$

where $u = k\lceil r_4(g)/k \rceil - r_4(g)$.

Corollary 3.10. *We have*

$$diam(\Gamma^n_{k,4}) = \begin{cases} \lceil (n-2)/(2k) \rceil & \text{if} \quad 2|k \\ \lceil (n-2)/(2k) \rceil + 1 & \text{if} \quad 2 \nmid k. \end{cases}$$

Proof. We find the maximum value of the function $d_{k,4}(1,g)$, denoted by d_Γ, for suitable permutation g in the generated group by $\Omega^n_{k,4}$. For every permutation g, suppose that b_g is the remainder of $r_4(g)$

divided by k. It is clear that for $u_g = k\lceil r_4(g)/k\rceil - r_4(g)$, 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 $\Gamma^n_{k,4} = Cay(A_n, \Omega^n_{k,4})$. 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 $g = (1\,2)(3\,4)\cdots(n-1\,n)$ gives d_Γ. By Corollary 3.9, $d_{k,4}(1,g) = \lceil n/(2k)\rceil$. Since $2k \nmid n-1$ and $2k \nmid n-2$, we have $\lceil n/(2k)\rceil = \lceil (n-2)/(2k)\rceil$. Thus, $\operatorname{diam}(\Gamma^n_{k,4}) = \lceil (n-2)/(2k)\rceil$.

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

$$\operatorname{diam}(\Gamma^n_{k,4}) = \left\lceil \frac{n-1}{2k} \right\rceil = \left\lceil \frac{n-2}{2k} \right\rceil.$$

Subcase 1-3: Let $n \equiv 2 \pmod 4$. Since $g = (1\,2)(4\,5)\cdots(n-3\,n-2)$ gives d_Γ, we have $\operatorname{diam}(\Gamma^n_{k,4}) = \lceil (n-2)/(2k)\rceil$.

Subcase 1-4: $n \equiv 3 \pmod 4$. In this case it is easily checked that $g = (1\,2\,3)(4\,5)\cdots(n-1\,n)$ gives d_Γ. Since $2k \nmid n$, $2k \nmid n-1$ and $2k \nmid n-2$, we have

$$\operatorname{diam}(\Gamma^n_{k,4}) = \left\lceil \frac{n+1}{2k} \right\rceil = \left\lceil \frac{n-2}{2k} \right\rceil.$$

Case 2: Suppose that $2 \nmid k$ and $2|n$. In this case $\Gamma^n_{k,4} = Cay(S_n, \Omega^n_{k,4})$. Let $g_1 = (1\,2)(3\,4)\cdots(n-1\,n)$ and $g_2 = (1\,2)(3\,4)\cdots(n-3\,n-2)$. 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_Γ. 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_Γ. 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_Γ. 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 $\Gamma^n_{k,4} = Cay(S_n, \Omega^n_{k,4})$. Let $g_3 = (1\,2\,3)(4\,5)\cdots(n-1\,n)$ and $g_4 = (1\,2)(3\,4)\cdots(n-2\,n-1)$. 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_Γ. 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_Γ. Thus,

$$\operatorname{diam}(\Gamma^n_{k,4}) = r_4(g_4) = \lceil (n-1)/(2k)\rceil + 1 = \lceil (n-2)/(2k)\rceil + 1.$$

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_Γ. 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. $\square$

4. Improvement of an Algorithm

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

---

Input : Permutations $s_1, s_2, \dots, s_t$ 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 $\langle s_1, s_2, \dots, s_t \rangle$.

```
foreach τ ∈ ⟨s_1, s_2, ..., s_t⟩ do
    for m = 1 to n do
        if τ^m is a good permutation OR τ^m and s have same cycle type
        then
            μ ← τ^m
            Go to Step 2.
        end
    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 μ.

```
A_0 ← {μ}
for l = 1 to maximum-tries do
    A_l ← ∅
    foreach i ∈ {1, 2, ..., t} each ϵ ∈ {1, −1} and each a ∈ A_{l−1} do
        if s_i^{−ϵ} a s_i^{ϵ} ∉ ⋃_{j=0}^{l} A_j then
            Add s_i^{−ϵ} a s_i^{ϵ} to A_l.
            if C ⊆ ⋃_{j=0}^{l} A_j then
                Go to Step 3.
            end
        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 $\Gamma^n_{k,m}$, a family of Cayley graphs, for $m = 2, 3, 4$. This problem for $\Gamma^n_{m^k}$ 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

[1] S. Annin and S. Maglione, Economical generating sets for the symmetric and alternating groups consisting of cycles of a fixed length, *J. Algebra Appl.*, **11** no. 16 (2012) pp.8.

[2] L. Babai and Á. Seress, On the diameter of Cayley graphs of the symmetric group, *J. Combin. Theory Ser. A*, **49** no. 1 (1988) 175–179.

[3] L. Babai and Á. Seress, On the diameter of permutation groups, *European J. Combin.*, **13** no. 4 (1992) 231–243.

[4] M. Camelo, D. Papadimitriou, L. Fbrega and P. Vil, Efficient routing in data center with underlying Cayley graph, In: *Complex Networks V*, (2014) (Springer) vol. 549 189–197.

[5] G. Cooperman and L. Finkelstein, A strong generating test and short presentations for permutation groups, *J. Symbolic Comput.*, **12** no. 4-5 (1991) 475–497.

[6] A. Kalka, M. Teicher and B. Tsaban, Short expressions of permutations as products and cryptanalysis of the algebraic eraser, *Adv. Appl. Math.*, **49** no. 1 (2012) 57–76.

[7] E. Konstantinova, On reconstruction of signed permutations distorted by reversal errors, *Discrete Math.*, **308** no. 5-6 (2008) 974–984.

[8] E. Konstantinova, Vertex reconstruction in Cayley graphs, *Discrete Math.*, **309** no. 3 (2009) 548–559.

[9] V. Levenshtein and J. Siemons, Error graphs and the reconstruction of elements in groups, *J. Combin. Theory Ser. A*, **116** no. 4 (2009) 795–815.

[10] T. Minkwitz, An algorithm for solving the factorization problem in permutation groups, *J. Symbolic Comput.*, **26** no. 1 (1998) 89–95.

[11] T. Phongpattanacharoen and J. Siemons, Metric intersection problems in Cayley graphs and the Stirling recursion, *Aequationes Math.*, **85** no. 3 (2013) 387–408.

[12] J. L. Soncco-Álvarez, G. M. Almeida, J. Becker and M. Ayala-Rincón, Parallelization of genetic algorithms for sorting permutations by reversals over biological data, *Int. J. Hybrid Intell. Syst.*, **12** no. 1 (2015) 53–64.

[13] B. Suceavă and R. Stong, The fewest 3-cycles to generate an even permutation, *Amer. Math. Monthly*, **110** no. 2 (2003) 162–162.

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`