УДК 519.21
https://doi.org/10.17721/1812-5409.2021/4.1

М. С. Ольшевський[1], *аспірант*

Нижня межа діаметру груп парних підстановок

[1] Київський національний університет імені Тараса Шевченка, 01601, м. Київ, вул. Володимирська 64/13,
e-mail: msolshevskyi@gmail.com

M. Olshevskyi[1], *graduate student*

The lower bound of diameter of Alternating groups

[1]Taras Shevchenko National University of Kyiv, 01601, Kyiv, 64/13 Volodymyrska st,
e-mail: msolshevskyi@gmail.com

В данній роботі розглядається задача пошуку діаметру групи парних підстановок по заданій системі твірних. Вводиться поняття збалансованої парної підстановки та обчислюються довжини елементів, що є збалансованими чи близькими до збалансованих. За допомогою отриманих довжин було отримано основний результат роботи — нижню оцінку діаметра знакозмінної групи по заданій системі твірних.

Ключові слова: граф Келі, діаметр графа, система твірних, група парних підстановок.

In this paper we consider a specific case of the diameter search problem for finite groups, the case where the system of generators is fixed. This problem is well-known and can be formulated in the following way: find the diameter of a group over its system of generators. The diameter of the corresponding Cayley graph is the diameter of a group over its specific system of generators.

The main object of the research is the alternating group with the system of generators consisting of cycles having length three and the form $(1, 2, k)$. This system of generators is a classical irreducible system of generators of the alternating group. It is introduced the property of even permutations to be balanced. We consider the set of balanced permutations and permutations close enough to balanced and find minimum decompositions of them over defined system of generators.

The main result of the paper is the lower bound of the diameter of Alternating group over considered system of generators. The estimation is achieved using minimal decompositions of balanced permutations.

Key Words: Cayley graph, diameter of graph, system of generators, alternating group.

Статтю представив д.ф.-м.н., проф. А. П. Петравчук

Introduction

The diameter search problem for a finite group G can be formulated as follows. Find maximum of diameters $D_S(G)$ for all system of generators S of G. The interest to this problem was stimulated by the paper of L. Babai and A. Seress [2]. Recent results obtained in this direction can be found in [3], [4], [5], [6].

One closely related problem is the mimimum-length generators sequence. This search problem can be formulated in the following way: for a finite group G, its system of generators S and an element $g \in G$ find the shortest generators sequence realizing g. It was shown in [7] that this problem is NP-hard for permutations groups.

A partial case of the diameter search problem is the diameter search problem with respect to a fixed system of generators. An exact formula of the diameter of the symmetric group $Sym(n)$ with respect to the classical irreducible system of generators $\{(1, k)\}$, $k = 2, \ldots, n$ in obtained in [1].

In this work it is considered the alternating group $Alt(n)$ of degree $n \geqslant 3$ and its classical irreducible system of generators $(1, 2, k)$, $k = 3, \ldots, n$. We introduced a specific type of even permutations that we call balanced permutations. For balanced even permutations and close to balanced even permutations it is constructed their minimal decomposition. These minimal decompositions are used to estimate the lower bound of the diameter of $Alt(n)$ with respected to the mentioned system of generators.

Unless otherwise specified in the paper we denote a finite group by G and a system of generators of G by S.

1 Preliminaries

In this section we recall basic definitions, that correspond to decompositions of elements. The definitions of strictly growing systems of generators and groups-generators series were introduced in [8].

The main object of research of the paper is the alternating group $Alt(n)$ of degree n with its system of generators $((1,2,3),\dots,(1,2,n)), n \geqslant 3$. We consider some useful elementary properties of this system of generators and recall the trajectory of a point over permutation's decomposition. This notion will be intensively used in the sequel.

1.1 Basic definitions, notations and properties

Every element g of G can be decomposed as a product

$$g = \prod_{k=1}^{l} s_k$$

of generators from S for some natural l. The tuple of generators $(s_1,\dots, s_k)$ will be called a *decomposition of the element g over S*. The *length $|g|_S$ of the element* g over S is the length of the shortest decomposition of g over S. The diameter $D_S(G)$ of G with respect to S is the maximum of lengths $|g|_S$, $g \in G$. An element $g \in G$ such that $|g|_S = D_S(G)$ is called a diameter element.

Let us introduce the operation of concatenation over tuples of generators. Let π, τ be elements from G and $D = (d_1,\dots,d_m), T = (t_1,\dots,t_u)$ be its decompositions over S correspondingly. Then the concatenation of D and T is the decomposition $(d_1,\dots,d_m,t_1,\dots,t_u)$ of the element $\pi \cdot \tau$.

In this paper we consider the right rule of permutation's multiplication: for every permutation π, τ and for every natural number x we have:

$$(\pi \cdot \tau)(x) = \tau(\pi(x)).$$

As usual, the support of a permutation π in $Sym(n)$ will be denoted by $supp(\pi)$, i.e. $supp(\pi) = \{x \in \overline{1,n} : \pi(x) \neq x\}$ for some natural number n.

Fix a natural number $n \geqslant 3$. The group $A = Alt(n)$ is a permutation group on the set $\overline{1,n} = \{1,2,\dots,n\}$. The elements of this set will be called *points*. Let $S = SoG(n) = \{s_3,\dots,s_n)\}$, where $s_k = (1,2,k)$, $k \geqslant 3$.

Let $D = (i_1,\dots,i_m)$ be a tuple of $m \geqslant 1$ natural numbers, each greater or equal than 3. We will use notation $[i_1,\dots,i_m]_S$ for the product

$$\prod_{k=1}^{m} s_{i_k} = \prod_{k=1}^{m} (1,2,i_k).$$

For simplicity we will identify the tuple $D = (i_1,\dots,i_m)$ of indices with the tuple $(s_{i_1},\dots, s_{i_m})$ of generators. Note, that the later forms a decomposition of the permutation $[i_1,\dots,i_m]_S$ over S.

We will use notation $\overbrace{a \to b}^{\pi}$ for $\pi \in A$ and $a, b \in \{1,2,\dots,n\}$ such that $\pi(a) = b$. Moreover, if for some permutation $\tau \in A$ and a point c additional equality $\tau(b) = c$ holds then we use the following notation:

$$\overbrace{a \to b}^{\pi} \Rightarrow \overbrace{b \to c}^{\tau}.$$

This notation can be naturally generalized for products of arbitrary number of permutations.

1.2 The trajectory of a point over a decomposition

Let $\pi \in A$ be a permutation. Fix a decomposition $D = (i_1,\dots,i_m)$ of π over S. We assume that $m \geqslant 3$. Let $a \in \{1,2,i_1,\dots,i_m\}$. We will define the trajectory of a over the decomposition D as follows.

For arbitrary points c, d and $k \in \overline{1,m}$ such that $s_{i_k}(c) = d$ we will use notation

$$c \xrightarrow{k} d.$$

Then in the graph of the action of the generating system S on $\overline{1,n}$ the decomposition D defines the unique path of the form

$$a = a_0 \xrightarrow{1} a_1 \xrightarrow{2} a_2 \xrightarrow{3} \dots \xrightarrow{m} a_m = \pi(a).$$

Definition 1.1. The trajectory of the point a in the permutation π over the decomposition D is a tuple $Tr(a,\pi,D) := (j_1,\dots,j_t)$ of all indices from D, such that exactly one condition

$$a_{j_k} = 1 \text{ or } a_{j_k-1} = 2$$

holds, $1 \leqslant k \leqslant t$.

In other words, the trajectory of a is the tuple of all positions in D, such that in the graph of the action corresponding generator defines the arrow that either starts in 2 or terminates at 1. Since $m \geqslant 3$ the trajectory is well defined.

In many cases we can use more compact form of the path of a point. For arbitrary $k, l \in \overline{1,m}$,

$k < l$, such that $2 = s_{i_k}^{-1}(a_k) \neq a_k = \ldots = a_{l-1} \neq s_{i_l}(a_{l-1}) = 1$, $a_k \neq 1, 2$, we will use notation

$$a_k \overset{k,l}{\Longrightarrow} a_k.$$

Note that in this case both $k, l \in Tr(a, \pi, D)$.

The following properties of the trajectory $Tr(a, \pi, D) = (j_1, \ldots, j_t)$ hold:

1) $a_{j_k} \neq 2$ for every $k \in \overline{1, t}$;

2) $a_{j_k} = a_{j_{k+1}-1}$ if and only if $a_{j_k} \xRightarrow{j_k, j_{k+1}} a_{j_k}$ is well defined in the path of a over D.

We will omit the following parts of the path of a in π over D:

1) the initial part of the path up to the first occurrence of a, if $a \neq 1, 2$;

2) the closing part of the path after the last occurrence of $\pi(a)$, if $\pi(a) \neq 1, 2$.

Let $\pi \in A$ be a permutation with decomposition $D = (d_1, \ldots, d_m)$ over S, $m \geqslant 3$ and p be a point from $\{1, 2, d_1, \ldots, d_m\}$. We will say that the point p *has trivial path in π over D* if $|Tr(p, \pi, D)| \leqslant 2$.

2 Length of permutation over S

In this section we provide estimations of lengths of permutations over system of generators S. We introduce the special type of permutations, which we call balanced. We show that the minimum length is reached for balanced permutations and permutations, which are close to balanced, according to number of unfixed points.

We also provide the minimum decomposition classification for special permutations: odd cycles, products of two odd or even cycles, some cases of products of three cycles. We separately consider cases according to action on points $1, 2$.

In this section we fix some natural number $n \geqslant 5$ and consider permutations from the alternating group A.

2.1 Length estimations over system of generators S

Let $\pi \in A$ be a permutation, $D = (d_1, \ldots, d_m)$ be its decomposition over S, p be some point from $\{d_1, \ldots, d_m\}$. Note that if the point p has trivial path in π over D, then, based on [9, Proposition 2], the path of the point p over D has the form

$$p \xrightarrow{1} p \xrightarrow{2} \ldots \xrightarrow{x-1} p \xrightarrow{x}$$
$$\xrightarrow{x} 1 \xrightarrow{x+1} 2 \xrightarrow{x+2} \pi(p) \xrightarrow{x+3} \ldots \xrightarrow{m} \pi(p),$$

where x is the first position of p in $\{d_1, \ldots, d_m\}$ and $x + 2$ is the last position of $\pi(p)$ in $\{d_1, \ldots, d_m\}$.

Let $\pi \in A$ be a permutation with the decomposition $D = (d_1, \ldots, d_m)$ over S, $p \in \{d_1, \ldots, d_m\}$ be a point.

Definition 2.1. We will stay that the point p is *mixing point* in π over D if there are two consequence positions $j_1, j_2 \in \overline{1, m}$, $j_1 < j_2$ of the point p such that:

$$j_2 - j_1 \text{ — odd number}$$

Let $\pi \in A$ be a permutation. Recall that every permutation π can be decomposed into the unique product of independent cycles up to its multiplication order. In this article we consider cycles with the length greater or equal 2. We denote the set of independent cycles of π by $IC(\pi)$.

Let c be a cycle from $IC(\pi)$ and D be a decomposition of π over A. Denote $\{d \in D | d \in supp(c)\}$ by $P(c, D)$ — the set of positions of points from cycle c in the decomposition D, which are not equal to $1, 2$.

Proposition 1. *Let $\pi \in A$ be a permutation, $c \in IC(\pi)$ be a cycle with the length $\geqslant 2$ and $1, 2 \notin supp(c)$. Then:*

$$|P(c, D)| \geqslant |c| + 1.$$

Moreover, if $|P(c, d)| = |c| + 1$ then every point from c appears only once in D, except only one point, which is appeared twice. One of this double-point's positions is the minimum and another is the maximum over the positions of points of cycle c over D.

Proof. Let $D = (d_1, \ldots, d_m)$ be the decomposition of π and $c = (i_1, \ldots, i_l)$. Then there is the sequence $\{j_{k,1}, j_{k,2} : k \in \overline{1, r}\}$ of positions of points from D such that for every $k \in \overline{1, l}$:

$$Tr(i_k, \pi, D) = (j_{k,1}, \ldots, j_{k,2}),$$

where $d_{j_{k,1}} = i_k$, $d_{j_{k,2}} = i_{k+1}$. The minimum count of positions in D, which are represented points from $(i_1, \ldots, i_l)$, can be archived only if the end of one trajectory will be the begin of another:

$$\ldots < j_{k-1,2} = j_{k,1} < j_{k,2} = j_{k+1,1} < \ldots$$

Note, that this sequence is ordered as natural numbers. Hence, there is one $t \in \overline{1,l}$: $j_{t-1,2} \neq j_{t,1}$ ($j_{l,2} \neq j_{1,1}$ in case $t = 1$).

The last means, that for the cycle c, the decomposition D should consist at least $l+1$ points such that:

1) only one point from $i_1, \ldots, i_l$ will be presented twice and has the minimum and the maximum position over positions of points from $i_1, \ldots, i_l$;

2) other points from $i_1, \ldots, i_l$ will be presented in decomposition only once.

As the result, we have:

$$|P(c, D)| \geqslant l + 1.$$

The proof is complete. □

Corollary 1. *Let $\pi \in A$ be a permutation, $c_1, \ldots, c_r \in IC(\pi)$ be cycles and $1, 2 \notin supp(c_i)$, $i \in \overline{1,r}$. Then:*

$$\sum_{i=1}^{r} |P(c_i, D)| \geqslant \sum_{i=1}^{r} |c_i| + r.$$

Moreover, if $\sum_{i=1}^{r} |P(c_i, D)| = \sum_{i=1}^{r} |c_i| + r$ then the decomposition D will have exactly $|c_i| + 1$ positions for points from c_i, $i \in \overline{1,r}$.

Proof. Directly implies from Proposition 1. □

Corollary 2. *Let $\pi \in A$ be some permutation, $\{c_1, \ldots, c_r\} = IC(\pi)$ and $1, 2 \notin supp(\pi)$. Then:*

$$|\pi|_S \geqslant \sum_{i=1}^{r} |c_i| + r.$$

Moreover, if $|\pi|_S = \sum_{i=1}^{r} |c_i| + r$ then the decomposition D will have exactly $|c_i| + 1$ positions for points from c_i, $i \in \overline{1,r}$.

Proof. Directly implies from Corollary 1 □

Proposition 2. *Let $\pi \in A$ be a permutation with the decomposition $D = (d_1, \ldots, d_m)$, $c_1, \ldots, c_r \in IC(\pi)$ be cycles, $1, 2 \notin supp(c_i)$, $i \in \overline{1,r}$.*

Let the following conditions are hold:

1) the decomposition D contains exactly $\sum_{i=1}^{r} |c_i| + r$ positions of points from $c_1, \ldots, c_r$;

2) every point from $(d_1, \ldots, d_m)$, which is different from points of c_i, $i \in \overline{1,r}$, is not the mixing point in π over D.

Then all positions from $P(c_i, D)$ are odd or even at the same time for every $i \in \overline{1,r}$.

Proof. Let $c = (i_1, \ldots, i_l)$ be one of cycles from $c_1, \ldots, c_r$ with the length $l \geqslant 2$. Note, that cycle c has exactly $l+1$ positions in D, based on condition 1. Similar to proof of Proposition 1 we have sequence of positions $\{(j_{k,1}, j_{k,2}) : k \in \overline{1,r}\}$ such that:

$$Tr(i_k, \pi, D) = (j_{k,1}, \cdots, j_{k,2}),$$

$$\ldots < j_{k-1,2} = j_{k,1} < j_{k,2} = j_{k+1,1} < \ldots$$

Without loosing of generality, we can assume that the point i_1 appears twice in D.

Suppose, that positions of points of c are not all odd or even. Then there is at least one $t \in \overline{1,r}$ that $j_{t,1}, j_{t,2}$ have different parity. The last means that there is at least one mixing point p with positions u_1, u_2 in π over D such that:

$$Tr(i_t, \pi, D) = (j_{t,1}, \ldots, u_1, u_2, \ldots, j_{t,2}),$$

where $p = d_{u_1} = d_{u_2}$. Condition 2 states that there is another cycle g from $c_1, \ldots, c_r$ that g has mixing point p. Based on Condition 1 and Proposition 1: u_1, u_2 are the first and the last positions of points of g. Note, that they also have different parity. Similar to cycle c, there will be found another mixing point for g, which will correspond to another cycle.

It is enough to note, that:

1) every cycle, which positions of points are not all odd or even, requires to have another cycle with mixing point in the range of its positions;

2) on each step, range of positions is decreasing:

$$\{j_{1,1}, \ldots, j_{l,2}\} \supset \{u_1, \ldots, u_2\} \supset \ldots;$$

3) number of cycles are limited.

From this we have, that at some moment there is no mixing point for cycle, which positions of points are not all odd or even. Contradiction.

As the result, all positions of cycle c_i are even or odd at the same time for every $i \in \overline{1,r}$. □

2.2 Balanced permutations

Let C be the set of pairwise different cycles with length greater or equal 2. The value $\sum\limits_{c\in C}|c|+|C|$ we denote by $L(C)$.

Note that if π is a permutation from A, then value $L(IC(\pi))$ is even number, because:

1) if π consists of odd cycles
   (a) and its number is even, then $\sum\limits_{c\in IC(\pi)}|c|$ and $|IC(\pi)|$ are even numbers, so, its sum is also even;
   (b) and its number is odd, then $\sum\limits_{c\in IC(\pi)}|c|$ and $|IC(\pi)|$ are odd numbers, so, its sum is even number.
2) if π consists of even cycles, then the number of even cycles are even, so, $\sum\limits_{c\in IC(\pi)}|c|+|IC(\pi)|$ is even number;
3) all other cases is a combination of the previous two.

Let π be a permutation, $1,2\notin supp(\pi)$.

Definition 2.2. We say that π be *balanced* permutation if $1,2\notin supp(\pi)$ and there exists separation $IC(\pi)$ into uncrossed sub-sets C_1,C_2 such that:

$$L(C_1)=L(C_2).$$

Proposition 3. *Let $\pi\in A$ be a permutation. Then the permutation π be balanced permutation if and only if:*

$$|\pi|_S=L(IC(\pi)).$$

Proof. Necessity. Based on Corollary 2:

$$|\pi|_S\geqslant L(IC(\pi)).$$

For every cycle $c=(i_1,\dots,i_x)$ we have its representation in the permutation's decomposition in the following way:

$$[\dots,i_1,t_1,i_2,t_2,\dots,i_x,t_x,i_1,t_{x+1},\dots]_S,$$

where $c\in IC(\pi)$ and $\{t_1,t_2,\dots,t_{x+1}\}$ are some points. We identify cycle $c_l=(i_1^{(l)},\dots,i_l^{(l)})\in IC(\pi)$ with every $c_l\in IC(\pi)$. Let $C_1=(c_{l_1},\dots,c_{l_{m_1}})$, $C_2=(c_{r_1},\dots,c_{r_{m_2}})$ be sub-sets from definition of balanced permutations. We use the similar form of cycle's decomposition, as it was in Proposition 1.

Then π can be decomposed over S in the following way (without loosing of generality, we assume here that $l_1<r_1$):

$$\pi=[{i_1}^{(l_1)},{i_1}^{(r_1)},\dots,{i_{l_1}}^{(l_1)},{i_{r_1}}^{(r_1)},{i_1}^{(l_1)},{i_{r_1+1}}^{(r_1)},\dots,{i_{l_{m_1}}}^{(l_{m_1})},{i_{r_{m_2}}}^{(r_{m_2})},{i_1}^{(l_{m_1})},{i_1}^{(r_{m_2})}]_S.$$

The last means that the statement is correct, because proposed decomposition is a decomposition of π with length:

$$L(C_1)+L(C_2)=\sum_{c\in IC(\pi)}|c|+|IC(\pi)|.$$

Sufficiency. Let D be a decomposition of π such that the length of D equals $\sum_{c\in IC(\pi)}|c|+|IC(\pi)|$. Note that the permutation π satisfies conditions of Proposition 2 with all cycles from $IC(\pi)$ and no other points, different from them. From Proposition 2 it follows that all positions of points of cycle c are odd or even at the same time for every c from $IC(\pi)$. Construct the sub-sets C_1, C_2 in the following way: if cycle c has odd positions of its points in D, then we put c into C_1, otherwise — into C_2.

As the result:

- $\sum\limits_{c\in C_1}|c|+|C_1|$ — number of odd positions;
- $\sum\limits_{c\in C_2}|c|+|C_2|$ — number of even positions.

In the end, it is enough to note that $\sum\limits_{c\in IC(\pi)}l+|IC(\pi)|=\sum\limits_{c\in C_1}|c|+|C_1|+\sum\limits_{c\in C_2}|c|+|C_2|$ is always even number for any permutation from A. As the result:

$$\sum_{c\in C_1}|c|+|C_1|=\sum_{c\in C_2}|c|+|C_2|,$$

which means that the permutation π is balanced. □

Lemma 1. *Let π be some balanced permutation, p be a natural number greater 2 and $\notin supp(\pi)$. Then if there exists separation $IC(\pi)$ into uncrossed sub-sets C_1,C_2 such that:*

$$L(C_1)=\frac{|\pi|_S}{2}+1 \text{ and } L(C_2)=\frac{|\pi|_S}{2}-1 \quad (1)$$

then:

$$|\pi\cdot {s_p}^2|_S=|\pi|_S+1.$$

Otherwise:

$$|\pi\cdot {s_p}^2|_S=|\pi|_S+2.$$

Proof. Note that $|\pi \cdot {s_p}^2|_S \geqslant |\pi|_S + 1$ based on Proposition 1. Also note that $\pi \cdot {s_p}^2 = [\pi]_S \cdot [p, p]$ with the length equals $|\pi|_S + 2$, so: $|\pi \cdot p^2|_S \leqslant |\pi|_S + 2$. Let $|\pi|_S = m$.

Suppose that there exists the decomposition $D = (d_1, \ldots, d_m, d_{m+1})$ of $\pi \cdot {s_p}^2$. Note that $p \notin supp(\pi)$ and π is balanced, so, there exist paths:

$$1 \to \ldots \to p,\ p \to \ldots \to 2 \text{ and } 2 \to \ldots \to 1.$$

Based on [9, Lemma 9], the point p can be placed on the mth position without increasing decomposition's length:

$$\pi \cdot {s_p}^2 = [d_1, \ldots, d_{m-1}, p, d_{m+1}]_S,$$

where there is no other p in $d_1, \ldots, d_{m-1}$.

Consider different cases of value of d_{m+1}.

1) Let $d_{m+1} = p$. Based on [9, Proposition 1], we have:

$$\pi = [d_1, \ldots, d_{m-1}, p, p]_S \cdot [p]_S = [d_1, \ldots, d_{m-1}]_S \text{ or}$$

which means that $|\pi|_S \leqslant m - 1$ — contradiction.

2) Let $d_{m+1} \neq p$. Note that there are exactly m positions for cycles of π. From Proposition 2 it follows that all positions of points of cycle in D should be even or odd numbers at the same time for every cycle from $IC(\pi)$.

Let C_1 be the set of cycles, which are placed on odd positions and C_2 be set of cycles, which are placed on even positions in D. Note that there are exactly $\frac{m}{2} + 1$ positions for C_1 and $\frac{m}{2} - 1$ for C_2. It is enough to note, that:

(a) cycles from C_1 can be placed in decomposition on odd positions;

(b) cycles from C_2 can be placed in decomposition on even positions

if and only if the equality (1) is hold. In this case, we have (without loosing the generality, we assume that $l_1 < r_1$):

$$\pi = [i_1^{(l_1)}, i_1^{(r_1)}, i_2^{(l_1)}, i_2^{(r_1)}, \ldots, i_{l_1}^{(l_1)}, i_{l_1}^{(r_1)},$$
$$i_1^{(l_1)}, i_{l_1+1}^{(r_1)}, i_1^{(l_2)}, i_{l_1+2}^{(r_1)}, \ldots, i_{l_{m_1}-1}^{(l_{m_1})}, i_1^{(r_{m_2})},$$
$$i_{l_{m_1}}^{(l_{m_1})}, p, i_1^{(l_{m_1})}]_S,$$

which prove that:

$$|\pi \cdot p^2|_S = m + 1 = |\pi|_S + 1.$$

If there are no such separation of $IC(\pi)$ into C_1, C_2, then there is no decomposition D of $\pi \cdot p^2$ with length $m + 1$. As the result:

$$|\pi \cdot p^2|_S = m + 2 = |\pi|_S + 2.$$

The proof is complete. □

Lemma 2. *Let π be an balanced permutation, $p_1, p_2 \geqslant 3$, $p_1 \neq p_2$, such that $p_1, p_2 \notin supp(\pi)$. If there exists a separation $IC(\pi)$ into uncrossed sub-sets C_1, C_2 such that*

$$L(C_1) = \frac{|\pi|_S}{2} + 2 \text{ and } L(C_2) = \frac{|\pi|_S}{2} - 2 \quad (2)$$

or

$$L(C_1) = \frac{|\pi|_S}{2} - 1 \text{ and } L(C_2) = \frac{|\pi|_S}{2} + 1 \quad (3)$$

then

$$|\pi \cdot (1, 2)(p_1, p_2)|_S = |\pi|_S + 3.$$

Otherwise

$$|\pi \cdot (1, 2)(p_1, p_2)|_S = |\pi|_S + 4.$$

Proof. Let $|\pi|_S = m$. Then $|\pi \cdot (1, 2)(p_1, p_2)|_S \geqslant m + 3$ based on Proposition 1 and Corollary 1. Also note that $\pi \cdot (1, 2)(p_1, p_2) = \pi \cdot [p_1, p_2, p_2, p_1]_S$ with the length equals $m + 4$, so: $|\pi \cdot p^2|_S \leqslant m + 4$.

Suppose that there exists the decomposition $D = (d_1, \ldots, d_{m+3})$ of $\pi \cdot (1, 2)(p_1, p_2)$ over S. Note that $p_1, p_2 \notin supp(\pi)$ and π is balanced, so, there exists paths:

$$p_1 \to \ldots \to p_2 \text{ and } p_2 \to \ldots \to p_1.$$

Based on [9, Lemma 9], the points p_1, p_2 can be placed on the last positions of decomposition. There are 2 possible options:

1) $\pi \cdot (1, 2)(p_1, p_2) = [d_1, \ldots, d_{m-3}, p_1, d_{m-1}, p_2, d_{m+1}, p_1, d_{m+3}]_S$;

2) $\pi \cdot (1, 2)(p_1, p_2) = [d_1, \ldots, d_{m-2}, p_1, d_m, p_2, d_{m+2}, p_1]_S$.

Note that there are no other p_1, p_2 in decomposition. We consider each case separately.

Case 1. There are exactly m positions for cycles of π. Based on Proposition 2, all positions of points of the cycle in D should be odd or even numbers at the same time for every cycle from $IC(\pi)$.

Let C_1 be the set of cycles, which are placed on odd positions and C_2 be the set of cycles, which are placed on even positions. Note that there are exactly $\frac{m}{2}+2$ positions for C_1 and $\frac{m}{2}-2$ for C_2. The last one take place if and only if the equation (2) is hold.

If such C_1, C_2 exist, then, similar to previous proves (without loosing the generality, we assume that $l_1 < l_2$) we have the following decomposition:

$$\pi = [i_1^{(l_1)}, i_1^{(r_1)}, i_2^{(l_1)}, i_2^{(r_1)}, \ldots, i_{l_1}^{(l_1)}, i_{l_1}^{(r_1)}, i_1^{(l_1)}, i_{l_1+1}^{(r_1)},$$
$$i_1^{(l_2)}, i_{l_1+2}^{(r_1)}, \ldots, i_{l_{m_1}-3}^{(l_{m_1})}, i_1^{(l_{m_2})}, i_{l_{m_1}-2}^{(l_{m_1})}, p_1, i_{l_{m_1}-1}^{(l_{m_1})}, p_2,$$
$$i_{l_{m_1}}^{(l_{m_1})}, p_1, i_1^{(l_{m_1})}]_S,$$

which prove that:

$$|\pi \cdot (1,2)(p_1,p_2)|_S = m+3 = |\pi|_S + 3.$$

If there are no such sub-sets C_1, C_2, then there is no decomposition D of $\pi \cdot (1,2)(p_1,p_2)$ with the length $m+3$ over S. As the result, we have:

$$|\pi \cdot (1,2)(p_1,p_2)|_S = m+4 = |\pi|_S + 4.$$

Case 2. There are exactly m positions for cycles from $IC(\pi)$. Based on Proposition 2, all positions of points of cycle in D should be even or odd for every cycle from $IC(\pi)$.

Let C_1 be set of cycles presented on odd positions and C_2 be set of cycles presented on even positions. Note that for C_1 there are exactly $\frac{m}{2}-1$ positions and $\frac{m}{2}+1$ for C_2. The last one take place if and only if the equation (3) is hold.

If such C_1, C_2 exist, then, similar to previous proves (without loosing the generality, we assume that $l_1 < l_2$) we have the following decomposition:

$$\pi = [i_1^{(l_1)}, i_1^{(r_1)}, i_2^{(l_1)}, i_2^{(r_1)}, \ldots, i_{l_1}^{(l_1)}, i_{l_1}^{(r_1)}, i_1^{(l_1)}, i_{l_1+1}^{(r_1)},$$
$$i_1^{(l_2)}, i_{l_1+2}^{(r_1)}, \ldots, i_1^{(l_{m_1})}, i_{l_{m_2}-1}^{(r_{m_2})}, p_1, i_{r_{m_2}}^{(r_{m_2})},$$
$$p_2, i_1^{(r_{m_2})}, p_1]_S,$$

which prove that:

$$|\pi \cdot (1,2)(p_1,p_2)|_S = m+3 = |\pi|_S + 3$$

If there are no such sub-sets C_1, C_2, then there is no decomposition D of $\pi \cdot (1,2)(p_1,p_2)$ over S with length $m+3$. As the result, we have:

$$|\pi \cdot (1,2)(p_1,p_2)|_S = m+4 = |\pi|_S + 4$$

$\square$

Lemma 3. *Let π be some balanced permutation, $p_1, p_2, p_3 \geqslant 3$ be pairwise different natural numbers such that $p_1, p_2, p_3 \notin supp(\pi)$. If there exists a separation $IC(\pi)$ into uncrossed sub-sets C_1, C_2 such that:*

$$L(C_1) = \frac{|\pi|_S}{2} + 2 \textit{ and } L(C_2) = \frac{|\pi|_S}{2} - 2$$

or:

$$L(C_1) = \frac{|\pi|_S}{2} - 1 \textit{ and } L(C_2) = \frac{|\pi|_S}{2} + 1$$

then:

$$|\pi \cdot (1,p_1)(p_2,p_3)|_S = |\pi|_S + 4$$

Otherwise:

$$|\pi \cdot (1,p_1)(p_2,p_3)|_S = |\pi|_S + 5$$

Proof. It is enough to note that:

$$\pi \cdot (1,2)(p_2,p_3) \cdot (1,2,p_1) = \pi \cdot (1,p_1)(p_2,p_3),$$

so based on strong growing propositions from [9]:

$$|\pi \cdot (1,p_1)(p_2,p_3)|_S = |\pi \cdot (1,2)(p_2,p_3)|_S + 1$$

If Lemma's conditions are succeed, then, based on Lemma 2 we have:

$$|\pi \cdot (1,2)(p_2,p_3)|_S = |\pi|_S + 3,$$

which means that:

$$|\pi \cdot (1,p_1)(p_2,p_3)|_S = |\pi|_S + 4$$

If Lemma's conditions are succeed, then, based on Lemma 2:

$$|\pi \cdot (1,2)(p_2,p_3)|_S = |\pi|_S + 4,$$

which means that:

$$|\pi \cdot (1,p_1)(p_2,p_3)|_S = |\pi|_S + 5$$

$\square$

Lemma 4. *Let π be a balanced permutation, $p_1, p_2, p_3 \geqslant 3$ be pairwise different natural numbers such that $p_1, p_2, p_3 \notin supp(\pi)$. If there exists continuous separation $IC(\pi)$ into uncrossed subsets C_1, C_2 such that:*

$$L(C_1) = \frac{|\pi|_S}{2} + 2 \text{ and } L(C_2) = \frac{|\pi|_S}{2} - 2$$

or:

$$L(C_1) = \frac{|\pi|_S}{2} - 1 \text{ and } L(C_2) = \frac{|\pi|_S}{2} + 1$$

then:

$$|\pi \cdot (2, p_1)(p_2, p_3)|_S = |\pi|_S + 4$$

Otherwise:

$$|\pi \cdot (2, p_1)(p_2, p_3)|_S = |\pi|_S + 5$$

Proof. It is enough to note that:

$$(1, 2, p_1) \cdot \pi \cdot (1, 2)(p_2, p_3) = \pi \cdot (1, p_1)(p_2, p_3),$$

so based on strong growing propositions from [9]:

$$|\pi \cdot (2, p_1)(p_2, p_3)|_S = |\pi \cdot (1, 2)(p_2, p_3)|_S + 1$$

If the conditions of the lemma are satisfied, then, based on Lemma 2 we have:

$$|\pi \cdot (1, 2)(p_2, p_3)|_S = |\pi|_S + 3$$

The last means, that:

$$|\pi \cdot (2, p_1)(p_2, p_3)|_S = |\pi|_S + 4$$

If conditions of the lemma aren't satisfied, then, based on Lemma 2, we have:

$$|\pi \cdot (1, 2)(p_2, p_3)|_S = |\pi|_S + 4$$

The last means, that:

$$|\pi \cdot (2, p_1)(p_2, p_3)|_S = |\pi|_S + 5$$

□

Lemma 5. *Let π be balanced permutation, $p_1, p_2, p_3, p_4 \geqslant 2$ be pairwise different natural numbers such that $p_1, p_2, p_3, p_4 \notin supp(\pi)$. If there exists a separation $IC(\pi)$ into uncrossed sub-sets C_1, C_2 such that:*

$$L(C_1) = \frac{|\pi|_S}{2} + 2 \text{ and } L(C_2) = \frac{|\pi|_S}{2} - 2$$

or:

$$L(C_1) = \frac{|\pi|_S}{2} - 1 \text{ and } L(C_2) = \frac{|\pi|_S}{2} + 1$$

then:

$$|\pi \cdot (1, p_1, 2, p_2)(p_3, p_4)|_S = |\pi|_S + 5$$

Otherwise:

$$|\pi \cdot (1, p_1, 2, p_2)(p_3, p_4)|_S = |\pi|_S + 6$$

Proof. It is enough to note that:

$$\pi \cdot (1, p_1)(p_3, p_4) \cdot (1, 2, p_2) = \pi \cdot (1, p_1, 2, p_2)(p_3, p_4),$$

so based on strong growing propositions from [9]:

$$|\pi \cdot (1, p_1, 2, p_2)(p_3, p_4)|_S = |\pi \cdot (1, p_1)(p_3, p_4)|_S + 1$$

If the conditions of the lemma are satisfied, then, based on Lemma 3:

$$|\pi \cdot (1, p_1)(p_3, p_4)|_S = |\pi|_S + 4,$$

The last means, that:

$$|\pi \cdot (1, p_1, 2, p_2)(p_3, p_4)|_S = |\pi|_S + 5$$

If the conditions of lemma aren't satisfied, then, based on Lemma 3:

$$|\pi \cdot (1, p_1)(p_3, p_4)|_S = |\pi|_S + 5,$$

The last means, that:

$$|\pi \cdot (1, p_1, 2, p_2)(p_3, p_4)|_S = |\pi|_S + 6$$

□

Lemma 6. *Let π be a balanced permutation, $p_1, p_2, p_3, p_4 \geqslant 3$ be pairwise different natural numbers such that $p_1, p_2, p_3, p_4 \notin supp(\pi)$. If there exists a separation $IC(\pi)$ into uncrossed subsequences C_1, C_2 such that:*

$$L(C_1) = \frac{|\pi|_S}{2} + 2 \text{ and } L(C_2) = \frac{|\pi|_S}{2} - 2$$

or:

$$L(C_1) = \frac{|\pi|_S}{2} - 1 \text{ and } L(C_2) = \frac{|\pi|_S}{2} + 1$$

then:

$$|\pi \cdot (1, 2, p_1, p_2)(p_3, p_4)|_S = |\pi|_S + 5$$

Otherwise:

$$|\pi \cdot (1, 2, p_1, p_2)(p_3, p_4)|_S = |\pi|_S + 6$$

Proof. It is enough to note that:

$\pi \cdot (2, p_2)(p_3, p_4) \cdot (1, 2, p_1) = \pi \cdot (1, 2, p_1, p_2)(p_3, p_4)$,

so based on strong growing propositions from [9]:

$|\pi \cdot (1, 2, p_1, p_2)(p_3, p_4)|_S = |\pi \cdot (2, p_2)(p_3, p_4)|_S + 1$

If the conditions of the lemma are satisfied, then, based on Lemma 4 we have:

$$|\pi \cdot (2, p_2)(p_3, p_4)|_S = |\pi|_S + 4$$

The last means, that:

$$|\pi \cdot (1, 2, p_1, p_2)(p_3, p_4)|_S = |\pi|_S + 5$$

If the conditions of the lemma aren't satisfied, then, based on Lemma 4 we have:

$$|\pi \cdot (2, p_2)(p_3, p_4)|_S = |\pi|_S + 5$$

The last means, that:

$$|\pi \cdot (1, 2, p_1, p_2)(p_3, p_4)|_S = |\pi|_S + 6$$

□

Lemma 7. *Let π be a balanced permutation, c be odd cycle with length u, c is independent to π and $1, 2 \notin supp(c)$. Then if there exists a separation $IC(\pi)$ into uncrossed sub-sets C_1, C_2 such that*

$L(C_1) = \dfrac{|\pi|_S}{2} + \dfrac{u+1}{2}$ *and* $L(C_2) = \dfrac{|\pi|_S}{2} - \dfrac{u+1}{2}$

then

$$|\pi \cdot c|_S = |\pi|_S + (u + 1).$$

Otherwise

$$|\pi \cdot c|_S = |\pi|_S + (u + 2).$$

Proof. Note that $|\pi \cdot c|_S \geqslant |\pi|_S + (u+1)$ based on Corollary 1. Also note that:

$$|\pi \cdot p^2|_S \leqslant |\pi|_S + |c|_S = |\pi|_S + (u + 2),$$

as product of two elements of A.

Suppose that there exists decomposition $D = (d_1, \dots, d_m, d_{m+1}$
$, \dots, d_{m+u+1})$ of $\pi \cdot c$ with $|\pi|_S = m$. Note that c is independent to π, $1, 2 \notin c$ and π is balanced. Then, without loosing of generality, we can assume that for cycle $c = (c_1, \dots, c_u)$: c_i has trivial path in $\pi \cdot c$ over D.

Based on rules of Multiplication of permutations by generators [9]: all points of cycle c can be placed on the last positions of decomposition, corresponding to its cycle order. As the result, we have the 2 options:

1) $\pi \cdot c = [d_1, \dots, d_{m-u}, c_1, d_{m-u+2}, c_2, \dots,$ $d_{m+u-2}, c_u, d_{m+u}, c_1]_S$.
2) $\pi \cdot c = [d_1, \dots, d_{m-u}, d_{m-u+1}, c_1,$ $d_{m-u+3} \dots, c_u, d_{m+u-1}, c_1, d_{m+u+1}]_S$.

Note that there are no other points of c in decomposition, based on Corollary 1. In both cases there are exactly m positions for cycles of π. Based on Corollary 2: every cycle from $IC(\pi)$ should be presented only on odd or even positions in decomposition D.

Let C_1 be set of cycles presented on odd positions and C_2 be set of cycles presented on even positions. Note that there are exactly $\frac{m}{2} + (u+1)$ positions for C_1 and $\frac{m}{2} - (u+1)$ for C_2. The last one takes place only if there exist sub-sets C_1, C_2 from lemma's condition. We will show that in case if the first lemma's conditions are satisfied, then can be constructed the decomposition of π with corresponding length. The second case can be similar constructed.

If such C_1, C_2 exist, then similar to previous proves:

$$\pi = [i_1^{(l_1)}, i_1^{(r_1)}, i_2^{(l_1)}, i_2^{(r_1)}, \dots, i_{l_1}^{(l_1)}, i_{l_1}^{(r_1)}, i_1^{(l_1)}, i_{l_1+1}^{(r_1)},$$
$$i_1^{(l_2)}, i_{l_1+2}^{(r_1)}, \dots, i_x^{(l_y)}, i_1^{(r_{m_2})}, i_{x+1}^{(l_y)}, c_1, \dots, i_{l_{m_1}}^{(l_{m_1})},$$
$$c_u, i_1^{(l_{m_1})}, c_1]_S,$$

where x some position for cycle in group C_1 with length y. Provided decomposition proves that:

$$|\pi \cdot c|_S = m + (u + 1) = |\pi|_S + (u + 1)$$

If there are no such sub-sets C_1, C_2, then there is no such decomposition D of $\pi \cdot c$ with length $m + (u + 1)$. As the result, we have:

$$|\pi \cdot c|_S = m + (u + 2) = |\pi|_S + (u + 2)$$

□

Lemma 8. *Let π be balanced permutation, c be odd cycle with length u, c is independent to π, $1, 2 \notin supp(c)$ and p be some natural number greater 2, $p \notin supp(\pi), supp(c)$. If there exists a separation $IC(\pi)$ into uncrossed sub-sets C_1, C_2 such that:*

$L(C_1) = \dfrac{|\pi|_S}{2} + \dfrac{u+1}{2}$ *and* $L(C_2) = \dfrac{|\pi|_S}{2} - \dfrac{u+1}{2}$

then:

$$|\pi \cdot c \cdot (1, 2, p)|_S = |\pi|_S + (u + 1) + 1$$

Otherwise:

$$|\pi \cdot c \cdot (1, 2, p)|_S = |\pi|_S + (u + 2) + 1$$

Proof. It is enough to note that from strong growing propositions of [9] it follows:

$$|\pi \cdot c \cdot (1, 2, p)|_S = |\pi \cdot c|_S + 1$$

If the conditions of the lemma are satisfied, then based on Lemma 7 we have:

$$|\pi \cdot c|_S = |\pi|_S + (u + 1)$$

The last means, that:

$$|\pi \cdot c \cdot (1, 2, p)|_S = |\pi|_S + (u + 1) + 1$$

If the conditions of the lemma aren't satisfied, then based on Lemma 2 we have:

$$|\pi \cdot c|_S = |\pi|_S + (u + 2)$$

The last means, that:

$$|\pi \cdot c \cdot (1, 2, p)|_S = |\pi|_S + (u + 2) + 1$$

□

3 Lower bound of diameter of alternating group

Theorem 3.1. *Let n be a natural number, $n \geqslant 7$. Then:*

$$D_{SoG(n)}(Alt(n)) \geqslant \begin{cases} [\frac{n-2}{4}] \cdot 6 + 2 & \text{if } n \bmod 4 = 3 \\ [\frac{n-2}{4}] \cdot 6 + 4 & \text{if } n \bmod 4 = 0 \\ [\frac{n-2}{4}] \cdot 6 + 5 & \text{if } n \bmod 4 = 1 \\ [\frac{n-2}{4}] \cdot 6 & \text{if } n \bmod 4 = 2 \end{cases}$$

Proof. Remind that series of subgroups $Alt(n)$ with system of generators $SoG(n)$ are stable and strong growing according to properties of $SoG(n)$ described in [9]. The last means that diameter elements can be found only in case if every generator from $SoG(n)$ will be presented in its decomposition. So, the diameter element should move nonidentical every point from 3 to n. Consider every case separately.

1) Let $n \bmod 4 = 3$. The last means that count of points from 3 to n can be presented as: $n - 2 = 4 \cdot k + 1$ for $k = \frac{n-2}{4}$. Consider the following element:

$$a = (1, i_1, 2) \cdot (i_2, i_3)(i_4, i_5) \ldots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$

with some combination $(i_1, \ldots, i_{n-2})$ from $(3, \ldots, n)$. Remind that series of subgroups $Alt(n)$ with system of generators $SoG(n)$ are homogeneous according to properties of $SoG(n)$ in [9]. So, without loosing of generality, the chosen of combination has no effect on its length over $SoG(n)$.

Note that $b = (i_2, i_3) \ldots (i_{n-3}, i_{n-2})$ is balanced permutation as a product of $2k$ transpositions with length 2. So,

$$|b|_S = 2 \cdot 2k + 2k = 3 \cdot 2k = 6 \cdot k$$

Moreover, every cycle has the length 2, so it cannot achieved condition for L_1, L_2 in Lemma 1. Hence, for $a = (1, i_1, 2) \cdot b$ by Lemma 1:

$$|a|_S = |b|_S + 2 = 6 \cdot k + 2$$

2) Let $n \bmod 4 = 0$. The last means that count of points from 3 to n can be presented as: $n - 2 = 4 \cdot k + 2$ for $k = \frac{n-2}{4}$. Consider the following element:

$$a = (1, 2)(i_1, i_2) \cdot (i_3, i_4)(i_5, i_6) \ldots$$
$$s(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$

with some combination $(i_1, \ldots, i_{n-2})$ from $(3, \ldots, n)$. Remind that series of subgroups $Alt(n)$ with system of generators $SoG(n)$ are homogeneous according to properties of $SoG(n)$ in [9]. Without loosing of generality, the chosen of combination has no effect on its length over $SoG(n)$.

The permutation $b = (i_3, i_4)(i_5, i_6) \ldots (i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2})$ is balanced, $|b|_S = 6 \cdot k$ and cannot archived condition for L_1, L_2 in Lemma 2. Hence, for $a = (1, 2)(i_1, i_2) \cdot b$ by Lemma 2:

$$|a|_S = |b|_S + 2 = 6 \cdot k + 4$$

3) Let $n \bmod 4 = 1$. The last means that count of points from 3 to n can be presented as: $n - 2 = 4 \cdot k + 3$ for $k = \frac{n-2}{4}$. Consider the following elements:

$$a_1 = (1, i_1)(i_2, i_3) \cdot (i_4, i_5)(i_6, i_7) \ldots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$
$$a_2 = (2, i_1)(i_2, i_3) \cdot (i_4, i_5)(i_6, i_7) \ldots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$
$$a_3 = (i_1, i_2, i_3) \cdot (i_4, i_5)(i_6, i_7) \ldots$$

$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$

with some combination $(i_1, \dots, i_{n-2})$ from $(3, \dots, n)$. Remind that series of subgroups $Alt(n)$ with system of generators $SoG(n)$ are homogeneous according to properties of $SoG(n)$ in [9], so without loosing of generality, the chosen of combination has no effect on its length over $SoG(n)$.

The permutation $b = (i_4, i_5)(i_6, i_7) \dots (i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2})$ is balanced, $|b|_S = 6 \cdot k$ and cannot archived condition for L_1, L_2 in Lemmas 3, 4 and 7. As the result, we have:

$$|a_1|_S = |(1, i_1)(i_2, i_3) \cdot b|_S = 6 \cdot k + 5$$

$$|a_2|_S = |(2, i_1)(i_2, i_3) \cdot b|_S = 6 \cdot k + 5$$

$$|a_3|_S = |(i_1, i_2, i_3) \cdot b|_S = 6 \cdot k + 5$$

4) Let $n \, mod \, 4 = 2$. The last means that count of points from 3 to n can be presented as: $n - 2 = 4 \cdot k$ for $k = \frac{n-2}{4}$. Consider the following elements:

$$a_1 = (1, i_1, 2, i_2)(i_3, i_4) \cdot (i_5, i_6)(i_7, i_8) \dots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$
$$a_2 = (1, 2, i_1, i_2)(i_3, i_4) \cdot (i_5, i_6)(i_7, i_8) \dots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$
$$a_3 = (1, 2, i_1)(i_2, i_3, i_4) \cdot (i_5, i_6)(i_7, i_8) \dots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$
$$a_4 = (i_1, i_2)(i_3, i_4) \cdot (i_5, i_6)(i_7, i_8) \dots$$
$$(i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2}),$$

with some combination $(i_1, \dots, i_{n-2})$ from $(3, \dots, n)$. Remind that series of subgroups $Alt(n)$ with system of generators $SoG(n)$ are homogeneous according to properties of $SoG(n)$ in [9], so without loosing of generality, the chosen of combination has no effect on its length over $SoG(n)$.

Again, $b = (i_5, i_6)(i_7, i_8) \dots (i_{n-5}, i_{n-4})(i_{n-3}, i_{n-2})$ is balanced, $|b|_S = 6 \cdot (k - 1)$ and cannot archived condition for L_1, L_2 in Lemmas 5, 6 and 8. As the result, we have:

$$|a_1|_S = |(1, i_1, 2, i_2)(i_3, i_4) \cdot b|_S = 6 \cdot k$$

$$|a_2|_S = |(1, 2, i_1, i_2)(i_3, i_4) \cdot b|_S = 6 \cdot k$$

$$|a_3|_S = |(1, 2, i_1)(i_2, i_3, i_4) \cdot b|_S = 6 \cdot k$$

$$|a_4|_S = |(i_1, i_2)(i_3, i_4) \cdot b|_S = 6 \cdot k$$

Note that in case $n = 10$ there is element

$$a_5 = (1, 2)(i_1, i_2)(i_3, i_4, i_5)(i_6, i_7, i_8) \in Alt(n)$$

with same length as for a_1, a_2, a_3, a_4, $|a_5|_S = 10$ by Lemma 2.

$\square$

Список використаних джерел

1. *S. Akers* The Star Graph: An Attractive Alternative to the n-Cube. / B. Krishnamurthy, D. Harel // International Conference on Parallel Processing: international conference, 15-19 August 1994, North Carolina, United States: abstracts. — Raleigh. — 1994.
2. *L. Babai* On the diameter of permutation groups / A. Seress // European Journal of Combinatorics, 1992. — Vol. 13, N4, pp.231-243.
3. *E. Breuillard* Approximate subgroups of linear groups [Електронний ресурс] / B. Green, T. Tao // arXiv. — Електронні дані. — Режим доступу: https://arxiv.org/abs/1005.1881. — Дата публікації: 11.05.2010.
4. *L. Pyber* Growth in finite simple groups of Lie type of bounded rank [Електронний ресурс] / E. Szabo // arXiv. — Електронні дані. — Режим доступу: https://arxiv.org/abs/1005.1858. — Дата публікації: 8.04.2011.
5. *H. Helfhott* On the diameter of permutation groups / A. Seress // Annals of Mathematics, 2014. — Vol. 199, N2, pp.611-658.
6. *J. Bajpai* D. DONA and H. HELFGOTT (2021) Growth estimates and diameter bounds for classical Chevalley groups [Електронний ресурс] / D. Dona, H. Helfgott // arXiv. — Електронні дані. — Режим доступу: https://arxiv.org/abs/2110.02942. — Дата публікації: 06.10.2021.
7. *S. Even* The minimum-length generator sequence problem is NP-hard / O. Goldreich // Journal of Algorithms, 1981. — Vol. 2, N3, pp.311-313.
8. *M. Olshevskyi* Diameter search algorithms for directed Cayley graphs // Mohyla Mathematical Journal, 2021. — N4, pp.614-625.
9. *M. Olshevskyi* Metric properties of Cayley graphs of Alternating groups // Carpathian Mathematical Publications, 2021. — Vol. 13, N2, pp.545-581.

References

1. S. AKERS, B. KRISHNAMURTHY and D. HAREL (1994) *The Star Graph: An Attractive Alternative to the n-Cube.* In *International Conference on Parallel Processing.* Raleigh, North Carolina, Monday 15th to Friday 19th August 1994. North Carolina State University.
2. L. BABAI and A. SERESS (1992) *On the diameter of permutation groups. European Journal of Combinatorics.* 13 (4). p.231-243.
3. E. BREUILLARD, B. GREEN and T. TAO (2010) *Approximate subgroups of linear groups* [Online] Available from: https://arxiv.org/abs/1005.1881 m. [Accessed: 11th May 2010].
4. L. PYBER and E. SZABO (2011) *Growth in finite simple groups of Lie type of bounded rank.* [Online] Available from: https://arxiv.org/abs/1005.1858 m. [Accessed: 8th April 2011].
5. H. HELFHOTT and A. SERESS (2014) *On the diameter of permutation groups. Annals of Mathematics.* 199 (2). p.611-658.
6. J. BAJPAI, D. DONA and H. HELFGOTT (2021) *Growth estimates and diameter bounds for classical Chevalley groups.* [Online] Available from: https://arxiv.org/abs/2110.02942 m. [Accessed: 6th October 2021].
7. S. EVEN and O. GOLDREICH (1981) *The minimum-length generator sequence problem is NP-hard. Journal of Algorithms.* 2 (3). p.311-313.
8. M. OLSHEVSKYI (2021) *Diameter search algorithms for directed Cayley graphs. Mohyla Mathematical Journal.* (4). p.614-625.
9. M. OLSHEVSKYI (2021) *Metric properties of Cayley graphs of Alternating groups. Carpathian Mathematical Publications.* 13 (2). -p.545-581.

Надійшла до редколегії 23.11.2021