ROMAI J., v.13, no.1(2017), 117–139

INVOLUTIVE IRREDUCIBLE GENERATING SETS AND STRUCTURE OF SYLOW 2-SUBGROUPS OF ALTERNATING GROUPS

Ruslan Skuratovskii

PL of National Technical University "KPI" of Kiev, Ukraine

ruslcomp@mail.ru

Abstract

The authors of [1] didn't proof minimality of finding by them system of generators for such Sylow 2-subgroups of A_n and structure of it were founded only descriptively. The purpose of this paper is to research the structure of Sylow 2-subgroups alternating group and to construct a minimal generating set for Syl_2A_n, where $n = 4k + 2$, $n = 4k + 3$. In other words, the problem is not simply in the proof of existence of a generating set. For the construction of minimal generating set we used the representation of elements of group by automorphisms of portraits for binary tree. Also, the goal of this paper is to investigate the structure of 2-sylow subgroup of alternating group. We obtain a symmetric irreducible generating set $\Lambda = S \cup S^{-1} = S$ because every generator has order two.

In this article the research of Sylow p-subgroups of A_n and S_n, which was started in [1, 2, 3] is continued. Let $syl_2A_{2^k}$ and syl_2A_n be Sylow 2-subgroups of the corresponding alternating groups A_{2^k} and A_n. We find a minimal generating set and the structure for such subgroups $syl_2A_{2^k}$ and syl_2A_n, $n = 4k + 2$, $n = 4k + 3$.

Keywords: minimal generating sets; iterated wreath product of groups; wreath power; semidirect product; Sylow 2-subgroups; alternating group; number of minimal generating sets; group of automorphisms Reebs graph.

2010 MSC: 20Exx, 20Dxx.

1. INTRODUCTION

In the articles [1, 3], the the sets of generators for Sylow p-subgroups of A_n and its normalizer as well as the structure of this subgroups were investigated. We found the following inaccuracies in these articles: minimal generating sets for the Sylow 2-subgroups of A_n were not investigated, also the structure of the Sylow 2-subgroups was described not fully, besides for case $n = 2^k$ the structure of Syl_2A_n was not described. Moreover, there was a mistake in a statement about irreducibility of a set of $k + 1$ elements for $Syl_2(A_{2^k})$ that

appeared in the abstract [4]. All obtained results were reported by the author at the conferences [28, 29, 30].

The aim of this paper is to study the structure of Sylow 2-subgroups of A_{2^k}, A_n and to construct a minimal generating set for $syl_2A_{2^k}$, syl_2A_n. The case of a Sylow subgroup where $p = 2$ is very special because the group $C_2 \wr C_2 \wr \ldots \wr C_2$ admits odd permutations, so $C_2 \wr C_2 \wr \ldots \wr C_2$ is not a subgroup of A_{2^k}. This case was not fully investigated in [1, 2] and the question remains open.

Let X be a finite alphabet. Sylow p-subgroups of A_{2^k} appear in the automaton theory, because if all states of an automaton A have output function that can be presented as a cycle $(1, 2, ..., p)$ then the profinite group $G_A(X)$ of this automaton is a Sylows p-subgroup of the restriction of the group of all automaton transformations $GA(X)$ also $G_A(X) < GA(X)$ [6]. In this case for the profinite groups we have $Syl_p(AutX) > FGA(X)$ [6]. Thus, finding the minimum cardinality of a generating set is important.

Acknowledgment. I would like to thanks to Igor Samoilovych for sharing his knowledge with me.

2. PRELIMINARIES

Let X^* be the free monoid freely generated by $X = \{0, 1\}$. Stated another way the set X^* is naturally a vertex set of a regular rooted tree, i.e. a connected graph without cycles and a designated vertex v_0 called the root, in which two words are connected by an edge if and only if they are of form v and vx, where $v \in X^*$, $x \in X$. The set $X^n \subset X^*$ is called the n-th level of the tree X^* and $X^0 = v_\varnothing$. We denote by $v_{j,i}$ the vertex of X^j, $j > 0$, which has the number i, $1 \leq i \leq 2^j$, indexing starts from left most vertex. The subtree of X^* induced by the set of vertices $\cup_{i=0}^{k} X^i$ is denoted by $X^{[k]}$. Note that the unique vertex $v_{k,i}$ corresponds to the unique word v in alphabet X. For every automorphism $g \in AutX^*$ and every word $v \in X^*$ define the section (state) $g_{(v)} \in AutX^*$ of g at v by the rule: $g_{(v)}(x) = y$ for $x, y \in X^*$ if and only if $g(vx) = g(v)y$. The restriction of the action of an automorphism $g \in AutX^*$ to the subtree $X^{[l]}$ is denoted by $g_{(v)}|_{X^{[l]}}$. A restriction $g_{(v)}|_{X^{[1]}}$ is called the vertex permutation (v.p.) of g in a vertex v. Let us introduce conventional signs for a v.p. state value of α in v_{ki} as $s_{ki}(\alpha)$ we put that $s_{ki}(\alpha) = 1$ if $\alpha_{(v_{ki})}|_{X^{[1]}}(x) = y$, $x \neq y$ such state of v.p. is active, and $s_{ki}(\alpha) = 0$ if $\alpha_{(v_{ki})}|_{X^{[1]}}(x) = x$ such state of v.p. is trivial. Let us label every vertex of X^l, $0 \leq l < k$ by sign 0 or 1 in relation to state of v.p. in it. Obtained by such way a vertex-labeled regular tree is an element of $AutX^{[k]}$. All undeclared terms are from [7, 11].

Let us denote by $v_{j,i}X^{[k-j]}$ subtree of $X^{[k]}$ with a root in $v_{j,i}$.

An automorphism of $X^{[k]}$ with non-trivial states of v.p. in some of $v_{1,1}$, $v_{1,2}$, $v_{2,1}$,..., $v_{2,4}$, ... ,$v_{m,1}$, ... ,$v_{m,j}$, $m < k, j \leq 2^m$ is denoted by $\beta_{1,(i_{11},i_{12});\ldots;l,(i_{l1},\ldots,i_{l2^l});\ldots;m,(i_{m1},\ldots,i_{m2^m})}$ where the index that stands straight be-

fore parentheses are number of a level in parentheses we write a tuple of states of v.p. of this level. In other words we set $i_{mj} = 0$ if v.p. in v_{mj} is trivial, $i_{mj} = 1$ in other case, i.e., $i_{mj} = s_{mj}(\beta)$, where $\beta \in AutX^{[k]}$, $m < k$. If for some l all $i_{lj} = 0$ then 2^l-tuple $l, (i_{l1}, ..., i_{l2^l})$ does not figure in indexes of β. But if numbers of active vertices are certain, for example $v_{j,1}$ and $v_{j,s}$, we can use more easy notation $\beta_{j,(1,s);}$, where in parentheses numbers of vertices with active state of v.p. from a level j. If in parentheses only one index presents then parentheses can be omitted for instance $\beta_{j,(s);} = \beta_{j,s;}$. Denote by $\tau_{i,...,j}$ the automorphism of $X^{[k]}$, which has a non-trivial v.p. only in vertices $v_{k-1,i}$, ... ,$v_{k-1,j}$, $j \leq 2^{k-1}$ of the level X^{k-1}. Denote by τ the automorphism $\tau_{1,2^{k-1}}$. Let us consider special elements such that: $\alpha_0 = \beta_0 = \beta_{0,(1)}, \alpha_1 = \beta_1 = \beta_{1,(1)}, \ldots, \alpha_l = \beta_l = \beta_{l,(1)}$.

As well known, the set of Sylow p-subgroups of G is denoted as $Syl_p(G)$ [8, 9]. Since all Sylow p-subgroups are conjugated [8], we may investigate any one Sylow p-subgroup instead of all subgroups from $Syl_p(A_{p^n})$ and denote this group as $syl_p(A_{p^n})$. Analogously, one Sylow p-subgroup from the $Syl_p(S_{p^n})$ is denoted by us as $syl_p(S_{p^n})$.

3. MAIN RESULT

Recall that the wreath product of permutation groups is an associative construction. We consider C_2 as additive group with two elements 0, 1. For constructing a wreath product we define an action of C_2 by shift on X. As well known, that $AutX^{[k-1]} \simeq \wr_{i=1}^{k-1} C_2$ [6].

Lemma 3.1. *Every automorphism that has active v.p. only on X^l, $l < k-1$ acts by even permutation on X^k.*

Proof. Actually every transposition in vertex from X^l, $l < k-1$ acts on even number of pair of vertexes because of binary tree structure. More precisely it realizes an even permutation on the set X^k with cyclic structure [13] $(1^{2^{k-1}-2^{k-l-l}}, 2^{2^{k-l-l}})$ because it formed by the structure of binary tree. ∎

Corollary 3.1. *Due to Lemma 3.1 automorphisms from $AutX^{[k-1]} = \langle \alpha_0, ..., \alpha_{k-2} \rangle$ form a group $B_{k-1} = \wr_{i=1}^{k-1} C_2$ acting on X^{k-1} by even permutations. Size of B_{k-1} equals to $2^{2^{k-1}-1}$.*

The parity of the action follows from Lemma 3.1.

Let us denote by W_{k-1} the subgroup of $AutX^{[k]}$ such that has active states only on X^{k-1} and number of such states is even, i.e., $W_{k-1} \lhd St_{AutX^{[k]}}(k-1)$ [7].

Proposition 3.1. *The order of* W_{k-1} *is equal to* $2^{2^{k-1}-1}$, $k > 1$ *and* $W_{k-1} = C_2^{2^{k-1}-1}$.

Proof. On X^{k-1} we have 2^{k-1} vertices where can be elements of a group $V_{k-1} \simeq C_2 \times C_2 \times ... \times C_2 \simeq (C_2)^{2^{k-1}}$, but as a result of the fact that X^{k-1} contains only even number of non trivial v.p. from X^{k-1}, there are only half of all permutations from $V_{k-1} \simeq St_{G_k}(k-1)$ on X^{k-1}. So it is the subgroup $W_{k-1} \simeq {}^{C_2^{2^{k-1}}}/_{C_2}$ of V_{k-1}. So we can state that $|W_{k-1}| = 2^{2^{k-1}-1}$, W_{k-1} has $k-1$ generators and we can consider W_{k-1} as a vector space of dimension $k-1$. ∎

For example let us consider the subgroup W_{4-1} of A_{2^4} its cardinality is $2^{2^{4-1}-1} = 2^7$ and $|A_{2^4}| = 2^{14}$. Let us denote by G_k the subgroup of $AutX^{[k]}$ such that $G_k \simeq B_{k-1} \ltimes W_{k-1}$.

Lemma 3.2. *The elements* τ *and* $\alpha_0, ..., \alpha_{k-1}$ *generate arbitrary element* τ_{ij}. *The set* $\{\tau, \alpha_0, ..., \alpha_{k-1}\}$ *is enough to generate a basis of* W_{k-1}.

Proof. Firstly, we shall prove the possibility of generating arbitrary τ_{ij}, $1 \leq i, j \leq 2^{k-1}$. According to [11, 2] the set $\alpha_0, ..., \alpha_{k-2}$ is the minimal generating set for group $AutX^{[k-1]}$.

Since $Autv_{1,1}X^{[k-2]} \simeq \langle \alpha_1, ..., \alpha_{k-2} \rangle$ acts on X^{k-1} transitively [10], then there exists a transposition of $v_{k-1,1}$ and $v_{k-1,j}$, $j \leq 2^{k-2}$. For this goal we act by α_{k-j} on τ: $\alpha_{k-j}\tau\alpha_{k-j} = \tau_{j,2^{k-2}}$. Similarly we act on τ by the corespondent α_{k-i} to get $\tau_{i,2^{k-2}}$ from τ: $\alpha_{k-i}\tau\alpha_{k-i}^{-1} = \tau_{i,2^{k-2}}$. Note that the automorphisms α_{k-j} and $\alpha_{k-i}, 1 < i, j < k-1$ acts non-trivial only on subtree $v_{1,1}X^{[k-1]}$. To get $\tau_{m,l}$ from $v_{1,2}X^{[k-1]}$, i.e., $2^{k-2} < m, l \leq 2^{k-1}$ we use α_0 to map $\tau_{i,j}$ in $\tau_{i+2^{k-2},j+2^{k-2}} \in v_{1,2}AutX^{[k-1]}$. To express an arbitrary transposition $\tau_{j,m}$ from W_{k-1} we have to multiply $\tau_{1,j}\tau\tau_{m,2^{k-1}} = \tau_{j,m}$. To construct an permutation of $v_{k-1,1}$ and $v_{k-1,j}$ we need to realize a natural number j, $1 < j < 2^{k-2}$, in 2-adic set of presentation (binary arithmetic). Then $j = \delta_{j_1}2^{m_j} + \delta_{j_2}2^{m_j-1} + ... + \delta_{j_{m_j+1}}$, $\delta_{j_i} \in \{0, 1\}$ where is a correspondence between δ_{j_i} that from such presentation and expressing of automorphisms: $\tau_{j,2^{k-1}} = \prod_{i=1}^{m_j} \alpha_{k-2-(m_j-i)}^{\delta_{j_i}} \tau \prod_{i=1}^{m_j} \alpha_{k-2-(m_j-i)}^{\delta_{j_i}}, 1 \leq m_j \leq k-2$. Generating the basis of W_{k-1} by all τ_{ij} is clear. ∎

Lemma 3.3. *Orders of groups* $G_k = \langle \alpha_0, \alpha_1, \alpha_2, ..., \alpha_{k-2}, \tau \rangle$ *and* $syl_2(A_{2^k})$ *are equal to* 2^{2^k-2}.

Proof. In accordance with Legendre's formula, the power of 2 in $2^k!$ is $\left[\frac{2^k}{2}\right] + \left[\frac{2^k}{2^2}\right] + \left[\frac{2^k}{2^3}\right] + ... + \left[\frac{2^k}{2^k}\right] = \frac{2^k-1}{2-1}$. We need to subtract 1 from it because we have only $\frac{n!}{2}$ of all permutations as a result: $\frac{2^k-1}{2-1} - 1 = 2^k - 2$.

So $|Syl(A_{2^k})| = 2^{2^k-2}$. The same size has group $G_k = B_{k-1} \ltimes W_{k-1}$ and $|G_k| = |B_{k-1}| \cdot |W_{k-1}| = |syl_2 A_{2^k}|$. Since size of groups G_k according to Proposition 3.1 and the fact that $|B_{k-1}| = 2^{2^{k-1}-1}$ is 2^{2^k-2}. For instance the orders of $syl_2(A_8)$, B_{3-1} and W_{3-1} are such $|W_{3-1}| = 2^{2^{3-1}-1} = 2^3 = 8$, $|B_{3-1}| = |C_2 \wr C_2| = 2 \cdot 2^2 = 2^3$ and according to Legendre's formula, the power of 2 in $2^k!$ is $\frac{2^3}{2} + \frac{2^3}{2^2} + \frac{2^3}{2^3} - 1 = 6$ so $syl_2(A_8) = 2^6 = 2^{2^k-2}$, where $k = 3$. Next example for A_{16}: $syl_2(A_{16}) = 2^{2^4-2} = 2^{14}, k = 4$, $|W_{4-1}| = 2^{2^{4-1}-1} = 2^7$, $|B_{4-1}| = |C_2 \wr C_2 \wr C_2| = 2 \cdot 2^2 \cdot 2^4 = 2^7$. So we have the $|A_{16}| = |W_3||B_3|$ equality which endorse the condition of this Lemma. ∎

An automorphisms group of the subgroup $C_2^{2^{k-1}-1}$ is based on permutations of copies of C_2. Orders of $\wr_{i=1}^{k-1} C_2$ and $C_2^{2^{k-1}-1}$ are equals. A homomorphism from $\wr_{i=1}^{k-1} C_2$ into $Aut(C_2^{2^{k-1}-1})$ is injective because a kernel of action $\wr_{i=1}^{k-1} C_2$ on $C_2^{2^{k-1}-1}$ is trivial, action is effective. The group G_k is a proper subgroup of index 2 in the group $\wr_{i=1}^{k} C_2$ [2, 14].

Theorem 3.1. ***A maximal 2-subgroup*** *of $AutX^{[k]}$ which consists of even permutations on X^k has the structure of the semidirect product $G_k \simeq B_{k-1} \ltimes W_{k-1}$ and is isomorphic to $syl_2 A_{2^k}$.*

Proof. A maximal 2-subgroup of $AutX^{[k-1]}$ is isomorphic to $B_{k-1} \simeq \underbrace{C_2 \wr C_2 \wr ... \wr C_2}_{k-1}$ acting by even permutation on X^k according to Lemma 3.1. A maximal 2-subgroup which has elements with active states only on X^{k-1} is isomorphic to subgroup W_{k-1}. The construction of W_{k-1} contributes an action of W_{k-1} by even permutations. From Lemma 3.1 it follows that every element of B_{k-1} acts by an even permutation on X^k. Thus, G_k acts by even permutations on X^k.

Using the Corollary 3.1 and Proposition 3.1 about sizes of B_{k-1} and W_{k-1} we get size of $G_k \simeq B_{k-1} \ltimes W_{k-1}$ is $2^{2^{k-1}-1} \cdot 2^{2^{k-1}-1} = 2^{2^k-2}$. A group G_k is subgroup of $AutX^{[k]}$ and it is well known that $AutX^{[k]} \simeq syl_2 S_{2^k}$, so G_k is isomorphic to some subgroup $\widetilde{G_k}$ of $syl_2 S_{2^k}$. A group $syl_2 A_{2^k}$ is subgroup of $syl_2 S_{2^k}$. As supplementary according to Lemma 3.3 order of $\widetilde{G_k}$ equals to order of $syl_2(A_{2^k})$. Hence, according to Sylow's theorems 2-subgroup $G_k \simeq syl_2 A_{2^k}$.

Since subgroups B_{k-1} and W_{k-1} are embedded in $AutX^{[k]}$, then define an action of B_{k-1} on elements of W_{k-1} as $\tau^\sigma = \sigma\tau\sigma^{-1}$, $\sigma \in B_{k-1}$, $\tau \in W_{k-1}$, i.e., action by inner automorphism (inner action) from $AutX^{[k]}$. Note that W_{k-1} is subgroup of stabilizer of X^{k-1} i.e. $W_{k-1} < St_{AutX^{[k]}}(k-1) \lhd AutX^{[k]}$ and

is normal too $W_{k-1} \lhd AutX^{[k]}$, because conjugation keeps a cyclic structure of permutation so even permutation maps in even. Therefore such conjugation induce an automorphism of W_{k-1} and $G_k \simeq B_{k-1} \ltimes W_{k-1}$. ∎

Proposition 3.2. *The group G_k is normal subgroup in the group $\wr_{i=1}^{k} C_2$ i.e. $G_k \lhd B_k$.*

Proof. The commutator of B_k is $B'_k = B_{k-1}$. In other hand $B_{k-1} < G_k$ because $G_k \simeq B_{k-1} \ltimes W_{k-1}$. Thus, $G_k \lhd B_k$. In other words, as well known [7] wreath product $\wr_{i=1}^{k} C_2$ can be defined as equality $Aut(X^{[k-1]}) \ltimes St_{Aut(X^{[k]})}(X^k)$. But $Aut(X^{[k-1]}) \simeq B_{k-1}$, $V_{k-1} \simeq St_{Aut(X^{[k]})}(k-1)$ and $W_{k-1} < V_{k-1}$ and taking in consideration the order of this semidirect product we have $|B_k : G_k| = 2$, so $G_k \lhd \wr_{i=1}^{k} C_2 = B_k$. ∎

Theorem 3.2. *The set $S_\alpha = \{\alpha_0, \alpha_1, \alpha_2, ..., \alpha_{k-2}, \tau\}$ of elements from $AutX^{[k]}$ generates the group G_k.*

Proof. The fact that the group G_k are generated by S_α results from Corollary 3.1 and Lemma 3.2. The order of G_k equals the order of $syl_2(A_{2^k})$ according to Lemma 3.3. Isomorphism of $syl_2(A_{2^k})$ and G_k is proved in Theorem 1. ∎

Consequently, we construct a generating set, which contains k elements, that is less than in [4]. We will not distinguish $syl_2(A_{2^k})$ and its isomorphic copy G_k in $AutX^{[k]}$.

The structure of Sylow 2-subgroup of A_{2^k} is the following: $\wr_{i=1}^{k-1} C_2 \ltimes \prod_{i=1}^{2^{k-1}-1} C_2$, where we consider C_2 as group of action on two elements and this action is faithful. It adjusts with construction of normalizer for $syl_p(S_n)$ from [16], where it was said that $syl_2(A_{2^l})$ is self-normalized in S_{2^l}.

Definition 3.1. *Let us call the index of automorphism β on X^l a number of active v.p. of β on X^l.*

Definition 3.2. *Define an element of type $\mathtt{T}$ as an automorphism $\tau_{i_0,...,i_{2^{k-1}};j_{2^{k-1}},...,j_{2^k}}$, that has an even index at X^{k-1} and has exactly m_1 active states, $m_1 \equiv 1 mod 2$, in vertexes of form $v_{k-1,j}$, $1 \leq j \leq 2^{k-2}$ and m_2 active states in vertices of form $v_{k-1,j}$, $2^{k-2} < j \leq 2^{k-1}$, $m_2 \equiv 1 mod 2$. Set of such elements is denoted by $\mathtt{T}$. In this article we use case $m_1 = m_2$.*

Definition 3.3. *A combined generator is such an automorphism $\beta_{l;\tilde{\tau}}$, that the restriction $\beta_{l;\tilde{\tau}}|_{X^{k-1}}$ coincides with α_l and $Rist_{<\beta_{i_l;\tilde{\tau}}>}(k-1) = \langle \tau' \rangle$, where $\tau' \in \mathtt{T}$.*

Definition 3.4. *A combined element is such an automorphism* $\beta_{1,i_1;2,i_2;\ldots;k-1,i_{k-1};\tilde{\tau}}$, *that its restriction* $\beta_{1,i_1;2,i_2;\ldots;k-1,i_{k-1};\tilde{\tau}}\big|_{X_{k-1}}$ *coincides with one of elements that can be generated by* S_α *and*

$$Rist_{<\beta_{1,i_1;2,i_2;\ldots;k-1,i_{k-1};\tilde{\tau}}>}(k-1) = \langle \tau' \rangle$$

[7] where $\tau' \in \mathtt{T}$. *The set of such elements is denoted by* $\mathtt{C}$.

In other words elements $g \in \mathtt{C}$ on level X^{k-1} have such structure as elements and generators of type T. As well $\tau_{i_0,\ldots,i_{2^{k-1}};j_{2^{k-1}},\ldots,j_{2^k}} \in St_{AutX^k}(k-1)$.

The minimum size of a generating set S of G we denote by rk$G$ and call the rank of G [17]. By the distance between vertices we shall understand the usual distance at graph between these vertexes. By the distance $\rho(g)$ of automorphism $g \in AutX^{[k]}$ (element) we shall understand the maximal distance between two vertexes with active v.p. of g.

Lemma 3.4. *The automorphism having a distance* d_0 *that has v.p. only on* X^{k-1} *can not be generated by automorphism with a distance* d_1 *such that* $d_1 < d_0$.

Proof. An element g with a distance $\rho(g) = d_0$, $d_0 < d_1$ can be mapped by automorphic mapping only in automorphism with a distance d_0 because automorphic mapping keeps incidence relation. So it possess property of isometry. Also multiplication of portraits (labeled graphs) of automorphisms that have distance d_1 gives us portrait of an element with distance no greater than d_1, it follows from properties of group operation. For instance $\tau_{1i}\tau_{1j} = \tau_{ij}$, where $i, j > 2^{k-2}$, $\rho(\tau_{1i}) = \rho(\tau_{1j}) = 2k-2$ but $\rho(\tau_{ij}) < 2k-2$. ∎

Lemma 3.5. *An arbitrary automorphism* $\tau' \in \mathtt{T}$ *can be expressed only as a product of the odd number of automorphisms from* $\mathtt{C}$ *or* $\mathtt{T}$.

Proof. Let us assume that there is no such element τ_{ij}, which has distance $2k-2$ then accord to Lemma 3.4 it is imposable to generate are pair of transpositions τ' with distance $\rho(\tau_{ij}) = 2k-2$. If we consider product P of even number elements from T then automorphism P has even number of active states in vertexes $v_{k-1,i}$ with number $i \leq 2^{k-2}$ so P does not satisfy the definition of type T generator. An combined element $\beta_{i_l;\tau}$ can be decomposed in product $\beta_{i_l;\tau} = \tau\dot{\beta}_{i_l}$ so we can express τ by using a combine element or using a product, where odd number elements from T or C. ∎

Corollary 3.2. *Any element of type* $\mathtt{T}$ *cannot be generated by* $\tau_{ij} \in Autv_{1,1}X^{[k-1]}$ *and* $\tau_{ml} \in Autv_{1,2}X^{[k-1]}$. *The same corollary is true for a combined element.*

Proof. It can be obtained from Lemma 3.4 because τ_{ij} from $Autv_{1,1}X^{[k-1]}$ has distance less then $2k-2$. So it does not satisfy conditions of Lemma 3.4,

i.e. τ' can not be generated by the automorphisms having distance between vertices less than $2k-2$ such distance has only automorphisms of type $\mathtt{T}$ and $\mathtt{C}$. But elements from $Autv_{1,1}X^{[k-1]}$ do not belongs neither to type $\mathtt{T}$ nor $\mathtt{C}$. ∎

Lemma 3.6. *Sets of types $\mathtt{T}$, $\mathtt{C}$ elements are not closed with respect to multiplication and raising to even power.*

Proof. Let $\varrho, \rho \in \mathtt{T}$ (or $\mathtt{C}$) and $\varrho\rho = \eta$. Let μ_0 be a tuple of vertices $v_{k-1,i}$, $1 \leq i \leq 2^{k-2}$. In the product $\varrho\rho = \eta$ the number of active states of η in the tuple μ_0 congruent to the sum by $mod2$ of active states of ϱ and ρ from μ_0. The same sum is in the tuple μ_1 which consists of vertices $v_{k-1,i}$, $2^{k-2} < i \leq 2^{k-1}$. Thus, η has even numbers of active states on these tuples. Hence, $RiSt_{\langle\eta\rangle}(k-1)$ does not contain elements of type $\mathtt{T}$, so $\eta \notin \mathtt{T}$. If we raise the element $\beta_{1,i_1;2,i_2;\ldots;k-1,i_{k-1};\tau} \in \mathtt{T}$ to even power or we evaluate a product of even number of multipliers from $\mathtt{C}$ then tuples μ_0 and μ_1 permutes with whole subtrees $v_{1,1}X^{[k-1]}$ and $v_{1,2}X^{[k-1]}$, then we get an element g with even indices on X^{k-2} in subtrees $v_{1,1}X^{[k-1]}$ and $v_{1,2}X^{[k-1]}$. Thus, $g \notin \mathtt{T}$. Consequently, elements of $\mathtt{C}$ do not form a group, the set $\mathtt{T}$ as a subset of $\mathtt{C}$ is not closed too. ∎

We have to take into account that all elements from $\mathtt{T}$ have the same main property to comprise odd number m_1 of active v.p. in vertices of form $v_{k-1,j}$, $j \leq 2^{k-2}$ and odd number m_2 of active v.p. in vertices with index $j : 2^{k-2} < j \leq 2^{k-1}$.

Let $S'_\alpha = \langle \alpha_0, \alpha_1, ..., \alpha_{k-2} \rangle$ so as it well known [11] $\left\langle S'_\alpha \right\rangle = AutX^{[k-1]}$. The cardinality of a generating set S is denoted by $\mid S \mid$ so $\mid S'_\alpha \mid = k-1$. Recall that $rk\,(G)$ is the rank of a group G [17].

Let $S_\beta = S'_\alpha \cup \tau_{i\ldots j}$, where $\tau_{i\ldots j} \in \mathtt{T}$ and S'_β is generating system which contains combine elements, $\mid S'_\beta \mid = k$.

It's known that $rk(AutX^{[k-1]}) = k-1$ and $\mid S'_\alpha \mid = k-1$ [11]. So if we complete S'_α by τ or element of type $\mathtt{T}$ we obtain set S_β such that $G_k \simeq \langle S_\beta \rangle$ and $|S_\beta| = k$. Hence to construct combined element β we multiply generator α_i of S'_α or arbitrary element that can be express from S'_α on the element of type $\mathtt{T}$, i.e., we take $\tau' \cdot \beta_i$ instead of β_i and denote it $\beta_{i;\tau'}$. It's equivalent that $Rist_{\beta_{i;\tau'}}(k-1) = \langle \tau' \rangle$, where τ' – generator of type $\mathtt{T}$.

Let us assume that S'_β has a cardinality $k-1$. If in this case S'_β is generating system again, then element τ can be expressed from it. There exist too ways to express the element of type $\mathtt{T}$ from S'_β. To express element of type $\mathtt{T}$ from S'_β we can use a word $\beta_{i,\tau}\beta_i^{-1} = \tau$ but if $\beta_{i,\tau} \in S'_\beta$ then $\beta_i \notin S'_\beta$ in contrary case $\mid S'_\beta \mid = k$. So we can not express word $\beta_{i,\tau}\beta_i^{-1}\,|_{X^{[k-1]}} = e$ to get $\beta_{i,\tau}\beta_i^{-1} = \tau$. For this goal we have to find relation in a group that is

a restriction of the group G_k on $X^{[k-1]}$. We have to take in consideration that $G_k\,|_{X^{[k-1]}} = B_{k-1}$. Really in wreath product $\wr_{j=1}^{k}\mathfrak{C}_2^{(j)} \simeq B_{k-1}$ holds a constitutive relations $\alpha_i^{2^m} = e$ and $\left[\alpha_m^i\alpha_{i_n}\alpha_m^{-i},\, \alpha_m^j\alpha_{i_k}\alpha_m^{-j}\right] = e,\ i \neq j$, where $\alpha_m \in S_\alpha^{'}$, $\alpha_{i_k} \in S_\alpha^{'}$ are generators of factors of $\wr_{j=1}^{k}\mathfrak{C}_2^{(j)}$ $(m < n,\, m < k)$ [2, 5]. Such relations are words $\left[\beta_m^i\beta_{i_n,\pi}\beta_m^{-i},\, \beta_m^j\beta_{i_k,\pi}\beta_m^{-j}\right],\ i \neq j$ or $\beta_i^{2^m} = e$, β_{i_n}, β_m, β_{i_k}, $\beta_{i_n,\pi}$ are generators of $S_\beta^*(k-1)$, that could be an automorphism θ. But $\left[\beta_m^i\beta_{i_n,\pi}\beta_m^{-i},\, \beta_m^j\beta_{i_k,\pi}\beta_m^{-j}\right],\ i \neq j$ does not belongs to $\mathtt{T}$ because this word has logarithm 0 by every element [15]. According to Lemma 3.5 and Lemma 3.6 product of even number element of type C doesn't equal to the element of C or T.

Lemma 3.7. *A generating set of G_k contains $S_\alpha^{'}$ and has at least $k-1$ generators.*

Proof. The subgroup $B_{k-1} < G_k$ is isomorphic to $AutX^{k-1}$ that has a minimal set of generators of $k-1$ elements [11]. Moreover, the subgroup $B_{k-1} \simeq {}^{G_k}\!/_{W_{k-1}}$, because $G_k \simeq B_{k-1} \ltimes W_{k-1}$, where $W_{k-1} \rhd G_k$. As it is well known that if $H \lhd G$ then $\mathrm{rk}(G) \geq \mathrm{rk}({}^{G}\!/_{H})$, because all generators of G_k may belongs to the different quotient classes [12]. ∎

As a corollary of last Lemma we see that generating set of size $k-1$ does not exist because $S_\beta^{'} \setminus \{\tau\}$ generates only a proper subgroup B_{k-1} of G_k as it was shown above.

Note that Frattini subgroup of any finite 2-group is equal to $\phi(G_k) = {G_k}^2 \cdot [G_k, G_k] = {G_k}^2$ because ${G_k}^2 > [G_k, G_k]$. Hence, generating sets of a 2-group G_k correspond to generating sets of 2-abelization and to generating sets of the quotient group by ${G_k}^2$.

Let $X_1 = \{v_{k-1,1}, v_{k-1,2}, ..., v_{k-1,2^{k-2}}\}$ and $X_2 = \{v_{k-1,2^{k-2}+1}, ..., v_{k-1,2^{k-1}}\}$.

Lemma 3.8. *Commutators of all elements from $syl_2A_{2^k}$ have all possible even indexes on X^l, $l < k-1$ of $X^{[k]}$ and on X^{k-2} of subtrees $v_{11}X^{[k-1]}$ and $v_{12}X^{[k-1]}$.*

Proof. Recall that any authomorphism $\theta \in syl_2A_n$ has an even index on X^{k-1} so the number parities of the active v. p. on X_1 and on X_2 are the same. Conjugation by automorphism α from $Autv_{11}X^{[k-1]}$ of the automorphism θ, that has some number $x : 1 \leq x \leq 2^{k-2}$ of active v. p. on X_1 does not change x. Also automorphism θ^{-1} has the same number x of v. p. on X_{k-1} as θ has. If α from $Autv_{11}X^{[k-1]}$ and $\alpha \notin AutX^{[k]}$ then conjugation $(\alpha\theta\alpha^{-1})$ permutes vertices only inside X_1 (X_2).

Thus, $\alpha\theta\alpha^{-1}$ and θ have the same parities of number of active v.p. on X_1 (X_2). Hence, a product $\alpha\theta\alpha^{-1}\theta^{-1}$ has an even number of active v.p. on X_1

(X_2) in this case. More over a coordinate-wise sum by `mod2` of active v. p. from $(\alpha\theta\alpha^{-1})$ and θ^{-1} on X_1 (X_2) is even and equal to $y : 0 \leq y \leq 2x$.

If the conjugation by α permutes sets X_1 and X_2 then there are coordinate-wise sums of no trivial v.p. from $\alpha\theta\alpha^{-1}\theta^{-1}$ on X_1 (analogously on X_2) have form: $(s_{k-1,1}(\alpha\theta\alpha^{-1}), ..., s_{k-1,2^{k-2}}(\alpha\theta\alpha^{-1})) \oplus (s_{k-1,1}(\theta^{-1}), ..., s_{k-1,2^{k-2}}(\theta^{-1}))$. This sum has even number of v.p. on X_1 and X_2 because $(\alpha\theta\alpha^{-1})$ and θ^{-1} have the same parity of no trivial v.p. on X_1 (X_2). Hence, $(\alpha\theta\alpha^{-1})\theta^{-1}$ has even number of v.p. on X_1 as well as on X_2.

An authomorphism θ from G_k was arbitrary so number of the active v.p. x on X_1 is arbitrary. And α is arbitrary from $AutX^{[k-1]}$ so vertices can be permuted in such way that the commutator $[\alpha, \theta]$ has arbitrary even number y of the active v.p. on X_1, $0 \leq y \leq 2x$.

A conjugation of an automorphism θ having arbitrary index x, $1 \leq x \leq 2^l$ on X^l by different $\alpha \in AutX^{[k]}$ gives us all permutations of active v.p. that θ has on X^l. So the multiplication $(\alpha\theta\alpha^{-1})\theta$ generates a commutator having index y equal to coordinate-wise sum by $mod2$ of no trivial v.p. from vectors $(s_{l1}(\alpha\theta\alpha^{-1}), s_{l2}(\alpha\theta\alpha^{-1}), ..., s_{l2^l}(\alpha\theta\alpha^{-1})) \oplus (s_{l1}(\theta), s_{l2}(\theta), ..., s_{l2^l}(\theta))$ on X^l. A indexes parities of $\alpha\theta\alpha^{-1}$ and θ^{-1} are the same so their sum by $mod2$ are even. Choosing θ we can choose an arbitrary index x of θ also we can choose arbitrary α to make a permutation of active v.p. on X^l. Thus, we obtain an element with arbitrary even index on X^l and arbitrary location of active v.p. on X^l.

Check that property of number parity of v.p. on X_1 and on X_2 is closed with respect to conjugation. We know that numbers of active v. p. on X_1 as well as on X_2 have the same parities. So the action by conjugation only can permutes it, hence, we again get the same structure of element. Conjugation by an automorphism α from $Autv_{11}X^{[k-1]}$ of an automorphism θ, that has the odd number of the active v. p. on X_1 does not change its parity. Choosing the θ we can choose an arbitrary index x of θ on X^{k-1} and number of active v.p. on X_1 and X_2 also we can choose arbitrary α to make a permutation active v.p. on X_1 and X_2. Thus, we can generate all possible elements from a commutant.

Let us check that the set of all commutators K from $syl_2A_{2^k}$ is closed with respect to the multiplication of commutators.

Let $\kappa_1, \kappa_2 \in K$ then $\kappa_1\kappa_2$ has an even index on X^l, $l < k-1$ because coordinate-wise sum $(s_{l,1}(\kappa_1), ..., s_{k-1,2^l}(\kappa_1)) \oplus (s_{l,\kappa_1(1)}(\kappa_2), ..., s_{l,\kappa_1(2^l)}(\kappa_2))$ of two 2^l-tuples of v.p. with an even number of no trivial coordinate has even number of such coordinate. Note that conjugation of κ can permute sets X_1 and X_2 so parities of x_1 and X_2 coincide. It is obviously index of $\alpha\kappa\alpha^{-1}$ is even as well as index of κ.

Check that a set K is a set closed with respect to the conjugation.

Let $\kappa \in K$, then $\alpha\kappa\alpha^{-1}$ also belongs to K, it is so because conjugation does not change index of an automorphism on a level. The conjugation only permutes vertices on level because the elements of $AutX^{[l-1]}$ acts on the vertices of X^l. But as it was proved above the elements of K have all possible indexes on X^l, so as a result of the conjugation $\alpha\kappa\alpha^{-1}$ we obtain an element from K.

Check that the set of commutators is closed with respect to the multiplication of commutators. Let κ_1, κ_2 be an arbitrary commutators of G_k. The parity of the number of vertex permutations on X^l in the product $\kappa_1\kappa_2$ is determined exceptionally by the parity of the numbers of active v.p. on X^l in κ_1 and κ_2 (independently from the action of v.p. from the higher levels). Thus $\kappa_1\kappa_2$ has an even index on X^l.

Hence, normal closure of the set K coincides with K. ∎

Proposition 3.3. *Frattini subgroup $\phi(G_k)$ acts by all even permutations on X^l, $0 \leq l \leq k-1$ and any element of $\phi(G_k)$ has even indexes on X^{k-2} of subtrees $v_{11}X^{[k-1]}$ and $v_{12}X^{[k-1]}$.*

Proof. Since a group G_k^2 contains the subgroup G' then a product G^2G' contains all elements from the commutant. We need to prove that $G_k^2 \simeq G'$.

An indexes of the automorphisms α^2, $(\alpha\beta)^2$ and $\alpha, \beta \in G_k$ on X^l, $l < k-1$ are always even. In more detail the indexes of α^2, $(\alpha\beta)^2$ and $\beta\alpha\beta^{-1}\alpha^{-1}$ on X^l are determined exceptionally by the parity of indexes of α and β on X^l (independently of the action of v.p. from the higher levels) and this parity is even. Since an index of $\alpha\beta$ on X^l is an arbitrary $x : 0 \leq x \leq 2^l$ then an index of $(\alpha\beta)^2$ is arbitrary even number that is between 0 and 2^l. As it was shown in Lemma 3.8 any $\gamma \in G_k$ has same parities of numbers of active v.p. on X_1 as well as on X_2. Then γ^2 has an even number of active v.p. on each sets X_1 and X_2. There are no elements with odd number of active v.p. on each sets X_1 and X_2 in G_k.

Thus, we can generate all possible elements from the commutant which was studied in Lemma 3.8. ∎

We denote as $G_k(l)$ such subgroup of $AutX^{[k]}$ that contains all v.p. from X^l, $l < k-1$. In other words it contains all v.p. from $Stab_{AutX^{[k]}}(l)$ and does not contains v.p. from $Stab_{AutX^{[k]}}(l+1)$, $l < k-1$. We denote as $G_k(k-1)$ such subgroup of $AutX^{[k]}$ that consists of v.p. which are located on X^{k-1} and isomorphic to W_{k-1}. Let us construct a homomorphism from $G(l)$ onto C_2 in the following way: $\varphi_l(\alpha) = \sum_{i=1}^{2^l} s_{li}(\alpha) \bmod 2$. Note that $\varphi_l(\alpha \cdot \beta) = \varphi_l(\alpha) \circ \varphi_l(\beta) = (\sum_{i=1}^{2^l} s_{li}(\alpha) + \sum_{i=1}^{2^l} s_{li}(\beta))\texttt{mod2}$.

Structure of subgroup $G_k^2 {G_k}' \lhd \wr_1^k S_2 \simeq AutX^{[k]}$ can be described in next way. This subgroup contains the commutant G_k'. So it has on each $X^l,\ 0 \leq l < k-1$ all even indexes that can exists there. There does not exist v.p. of type `T` on X^{k-1}, rest of even the indexes are present on X^{k-1}. It is so, because the sets of elements of types `T` and `C` are not closed with respect to operation of rasing to the even power as it proved in Lemma 3.6. Thus, the squares of the elements don't belong to `T` and `C`. This implies the corollary.

Corollary 3.3. *A quotient group* ${}^{G_k}/_{G_k^2 G_k'}$ *is isomorphic to* $\underbrace{C_2 \times C_2 \times ... \times C_2}_{k}$.

Proof. The proof is based on two facts $G_k^2 G_k' \simeq G_k^2 \lhd G_k$ and $\left|G : G_k^2 G_k'\right| = 2^k$. Construct a homomorphism from $G_k(l)$ onto C_2 in the following way: $\varphi_l(\alpha) = \sum\limits_{i=1}^{2^l} s_{li}(\alpha) \bmod 2$. Note that $\varphi_l(\alpha \cdot \beta) = \varphi_l(\alpha) \circ \varphi_l(\beta) = (\sum\limits_{i=1}^{2^l} s_{li}(\alpha) + \sum\limits_{i=1}^{2^l} s_{li}(\beta))\texttt{mod2}$, where $\alpha,\ \beta \in AutX^{[n]}$. Index of $\alpha \in G_k^2$ on X^l, $l < k-1$ is even but index of $\beta \in G_k$ on X^l can be both even and odd. Note that $G_k(l)$ is abelian subgroup of G_k and $G_k^2(l) \trianglelefteq G_k$.

By virtue of the fact that we can construct the homomorphism φ_i from every subgroup $G_k(i)$ of this product to ${}^{G_k(i)}/_{G_k^2(i)}$ we have homomorphism from G_k to ${}^{G_k}/_{G_k^2}$. The group ${}^{G_k}/_{G_k^2}$ is elementary abelian 2-group because $g^2 = e,\ g \in G$ and $G' \lhd G^2$. Let us find a 2-rank of this group.

We use the homomorphism φ_l which is described above, to map $G_k(l)$ onto ${}^{G_k(l)}/_{G_k^2(l)}$ the $\ker \varphi_l = G_k^2(l)$. If α from $G_k(l)$ has odd number of active states of v.p. on $X^l,\ l < k-1$ than $\varphi_l(\alpha) = 1$ in ${}^{G_k(l)}/_{G_k^2(l)}$ otherwise if this number is even than α from $\ker \varphi_i = G_k^2(l)$, so $\varphi_l(\alpha) = 0$. Hence we have ${}^{G_k(l)}/_{G_k^2(l)} \simeq C_2$. Let us check that mapping $\varphi = (\varphi_0, \varphi_1, ..., \varphi_{k-2}, \phi_{k-1})$ is the homomorphism from G_k onto $(C_2)^k$.

Parity of index of $\alpha \cdot \beta$ on X^l is equal to sum by $\bmod 2$ of indexes of α and β hence $\varphi_l(\alpha \cdot \beta) = (\varphi_l(\alpha) + \varphi_l(\beta))$ because the multiplication $\alpha \cdot \beta$ in G_k does not change a parity of index of β, $\beta \in G_k$ on X^l. Really action of element of active group $A = \underbrace{C_2 \wr C_2 \wr ... \wr C_2}_{l-1}$ from wreath power $(\underbrace{C_2 \wr C_2 \wr ... \wr C_2}_{l-1}) \wr C_2$ on element from passive subgroup C_2 of second multiplier from product $gf,\ g, f \in A \wr C_2$ does not change a parity of index of β on X^l, if index of β was even then under action it stands to be even and the sum $\varphi_l(\alpha) \bmod 2 + \varphi_l(\beta) \bmod 2$ will be equal to $(\varphi_l(\alpha) + \varphi_l(\beta)) \bmod 2$, hence it does not change a $\varphi(\beta)$.

Indexes of $\alpha_{(v_{11})}$ and $\alpha_{(v_{12})}$ for arbitrary $\alpha \in G_k$ on X^{k-1} can be as even as well as odd. But these indexes of $\alpha_{(v_{11})}$ and $\alpha_{(v_{12})}$ are equal by `mod 2`.

The subgroup $G_k^2 G_k^{'}$ admits only automorphisms α such that $\alpha_{(v_{11})}$ and $\alpha_{(v_{12})}$ have even indexes on X^{k-1}. So this set is a kernel of mapping from $G_k(k-1)$ onto C_2. This homomorphism can be obtained from the formula $\phi(\alpha) = \sum\limits_{i=1}^{2^{k-2}} s_{k-1,i}(\alpha)(\mathrm{mod}2) \cdot \sum\limits_{i=2^{k-2}+1}^{2^{k-1}} s_{k-1,i}(\alpha)(\mathrm{mod}2)$. It follows from structure of G_k that $\sum\limits_{i=1}^{2^{k-2}} s_{k-1,i}(\alpha)(\mathrm{mod}2) = \sum\limits_{i=2^{k-2}+1}^{2^{k-1}} s_{k-1,i}(\alpha)(\mathrm{mod}2)$. Thus the image $\phi(G_k(k-1))$ consist of 2 elements: 0 and 1, these elements we map in different elements of C_2. Hence homomorphism ϕ is surjective.

Hence for an abelian subgroup $G_k(k-1) \simeq W_{k-1}$ such that $G_k(k-1) \triangleright {G_k}^2(k-1)$ it was constructed a homomorphism $\phi : (G_k(k-1)) \to {}^{G_k(k-1)}/_{G_k^2(k-1)} \simeq C_2$. This homomorphism is injective because for every j two different elements of ${}^{G_k(j)}/_{G_k^2 G_k^{'}(j)}$, $0 \leq j < k$, map in 2 different images in C_2. Element α that is in accord with a condition $\sum\limits_{i=1}^{2^l} s_{li}(\alpha) \equiv 0(\ \mathtt{mod2})$ has an image 0 and if $\sum\limits_{i=1}^{2^l} s_{li}(\alpha)) \equiv 1(\mathtt{mod2})$ its image is 1.

Since words of generators with no equal logarithms to any bases by mod 2 [15] belong to distinct cosets of the commutator, the subgroup $G_k^2(l)$ is the kernel of this mapping. The number of such bases is k because there are k generators. Hence the homomorphism from ${}^{G_k}/_{G_k^2}$ onto $(C_2)^k$ is injective.

Let us check that the homomorphism φ is surjective. For this goal we shall indicate preimage of arbitrary generator $g_l = (0, ..., 0, 1, 0, ..., 0)$ of $(C_2)^k$, where 1 1s on l coordinate. This preimage is $\alpha_{l,1} \in G_k$. As the result we have ${}^{G_k}/_{G_k^2} \simeq \underbrace{C_2 \times C_2 \times ... \times C_2}_{k}$. ∎

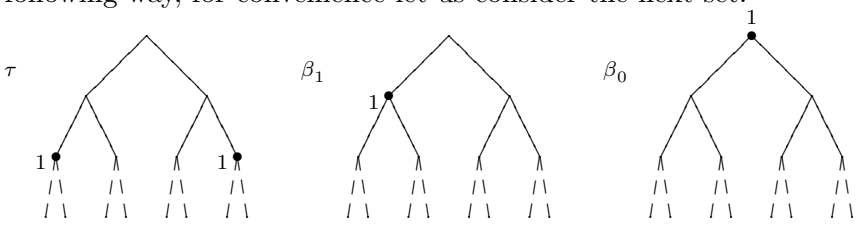
Corollary 3.4. *The group $syl_2 A_{2^k}$ has a minimal generating set of k generators.*

Proof. Since quotient group of G_k by subgroup of Frattini $G_k^2 G_k^{'}$ has minimal set of generators from k elements because ${}^{G_k}/_{G_k^2 G_k^{'}}$ is isomorphic to linear p-space ($p = 2$) of dimension k (or elementary abelian group). Then according to theorems from [18] $rk(G_k) = k$. Since $G_k \simeq A_{2^k}$ it means that A_{2^k} is a group with fixed size of minimal generating set. ∎

Main Theorem. *The set S_α is a minimal generating set for a group G_k that is isomorphic to Sylow 2-subgroup of A_{2^k}, $rk(syl_2 A_{2^k}) = k$.*

The existing of isomorphism between G_k and $syl_2(A_{2^k})$ follows from Theorem 3.2. The minimality of S_β follows from Lemma 3.7 which says that the rank of $syl_2(A_{2^k})$ is not less than $k-1$ and Theorem 3.2. The fact that set of k elements is enough to generate G_k follows from Corollary 3.3 and from Theorem 3.2. Hence, we prove that $rk(syl_2A_{2^k}) = k$. Another way to prove the minimality of S_β is given in Corollary 3.3 because generating set of such group corresponds to generating sets of 2-abelianisation.

For example a minimal generating set of $syl_2(A_8)$ may be constructed by following way, for convenience let us consider the next set:



Consequently, in such a way we construct the second k-element generating set for A_{2^k}, that is less than in [4], and this set is minimal.

We will call ***diagonal base*** (S_d) for $syl_2S_{2^k} \simeq AutX^{[k]}$ such base that has the following two properties. First $s_{jx}(\alpha_i) = 0$ iff $i \neq j$ (for $1 \leq x \leq 2^j$). Second, every $\alpha_i\,(i < k)$ has odd number of active v.p. This base is the similar to S_α that described in Theorem for $syl_2A_{2^k}$. A number of no trivial v.p. that can be on X^j is odd, the number of ways to chose a tuple of non trivial v.p. on X^j for generator from S_d is equal to $2^{2^j} : 2 = 2^{2^j-1}$. Thus, general cardinality of S_d for $syl_2S_{2^k}$ is 2^{2^k-k-1}. There is at least one generator of type $\mathtt{T}$ in S_d for $syl_2A_{2^k}$. If m_1, m_2 which are mentioned above in Definition 2 are equal to 1 then this generator can be chosen in $C^1_{2^{k-2}}C^1_{2^{k-2}} = \left(2^{k-2}\right)^2 = 2^{2k-4}$ ways. If $m_1 = m_2 = j$ then this generator can be chosen in $C^j_{2^{k-2}}C^j_{2^{k-2}}$ ways. In general case $m_1 \neq m_2$ and there are $C^{m_1}_{2^{k-2}}C^{m_2}_{2^{k-2}}$ generators. Thus, general cardinality of S_d for $syl_2A_{2^k}$ is not less than $2^{2^{k-1}-k-2}\sum\limits_{j=1}^{2^{k-2}-1}(C^j_{2^{k-2}})^2$. The total number of S_d for $syl_2S_{2^k}$ is 2^{2^k-k-1}.

Property 1. *The total number of minimal generating sets for $syl_2A_{2^k}$ is $2^{k(2^k-k-2)} \cdot (2^k-1)(2^k-2)(2^k-2^2)...(2^k-2^{k-1})$, for $syl_2S_{2^k}$ it is $2^{k(2^k-k-1)} \cdot (2^k-1)(2^k-2)...(2^k-2^{k-1})$.*

Proof. Find the total number of minimal generating sets for G_k and analogous sets for $AutX^{[k]}$. We take into account, that the number of generating sets for $(C_2)^k \simeq {}^{G_k}/_{G_k^2G_k'}$ equals to $(2^k-1)(2^k-2)(2^k-2^2)...(2^k-2^{k-1})$ and equals to the order of the group $GL\,(k, \mathbb{F}_2)$. Also take into account that every element from $(C_2)^k$ has $|G_k| : 2^k$ inverse images in G_k, because $(C_2)^k$ is a factor-group.

Hence, generating sets of a 2-group G_k correspond to generating sets of 2-abelization. Since $(C_2)^k$ is a quotient group of G_k by Frattini subgroup $\phi(G_k)$, any inverse image of quotient group generator is generator of G_k, so preimages number for each generator of $(C_2)^k$ is equal to size of normal subgroup $\phi(G_k)$.

There are k generators in a minimal generating set of $(C_2)^k$, therefore to calculate number of preimages of the whole minimal generating set of $(C_2)^k$ the number $|\phi(G_k)| = |G_k| : 2^k$ should be raised to the power of k. So we can count a number of minimal generating sets of G_k. It equals to $(|G_k| : 2^k)^k = (2^{2^k-2} : 2^k)^k = 2^{k(2^k-k-2)}$. As a result, we have $2^{k(2^k-k-2)} \cdot (2^k-1)(2^k-2)(2^k-2^2)...(2^k-2^{k-1})$. In the similar way we obtain a number of minimal generating sets of $Syl_2S_{2^k}$. It equals to $2^{k(2^k-k-1)} \cdot (2^k-1)(2^k-2)(2^k-2^2)...(2^k-2^{k-1})$. ∎

Thus, if we associate generating set with alphabet and choice of generating set will be a private key, then it can be applied in cryptography [19]. A group G_k can be used as a platform group G in the key establishment protocol [31] of generating common secret key (shared secret key). This group G_k satisfies all six properties from [31]. More over our group G_k has exponential grows of different generating sets and diagonal bases that can be used for extention of key space. Diagonal bases and minimal generating sets are useful for easy constructing of normal form [31] and minimal length form [32] of an element $g \in G_k$. As a privet key we choose one of generating sets. For every permutation π from Syl_2A_n we introduce a notion of canonical presentation in fixed generating set. We consider a classification of permutations in fixed generating set. For finding canonical presentations we consider a set of words $\Lambda_n, k, k \geq n-2$, elements of Λ_n, k are images of π after defined by us mapping ϕ and a tuple $V_m(\overrightarrow{v}, \overrightarrow{u})$, where $m > 1, v, u$ – some vectors with elements from Z. On base of this notions it was proposed an algorithm of middle incline for constructing of canonical representation of any permutation. Conjugacy problem for this subgroup can be used as base in application for designing braidbased protocols. Also researching of the structure of Syl_2A_n give us possibility to solving of inclusion problem for set of elements of this subgroup. As well known this problem is NP hard.

4. STRUCTURE AND PROPERTIES OF SYL_2A_N

Let us consider an examples of syl_2A_n for a cases $n = 4k + r$, where $r \leq 3$.

The structure of syl_2A_{12} is the same as of the subgroup $H_{12} < syl_2(S_8) \times syl_2(S_4)$, for that $[syl_2(S_8) \times syl_2(S_4) : H_{12}] = 2$, $|syl_2(A_{12})| = 2^{[12/2]+[12/4]+[12/8]-1} = 2^9$.

Also $|syl_2(S_8)| = 2^7$, $|syl_2(S_4)| = 2^3$, so $|syl_2(S_8) \times syl_2(S_4)| = 2^{10}$ and $|H_{12}| = 2^9$, because its index in $syl_2(S_8) \times syl_2(S_4)$ is 2.

The structure of $syl_2(A_6)$ is the same as of $H_6 < syl_2(S_4) \times (C_2)$. Here $H_6 = \{(g, h_g) | g \in syl_2(S_4), h_g \in C_2\}$, where

$$\begin{cases} h_g = e, \ \ if \ g|_{X_2} \in syl_2(A_6), \\ h_g = (5,6), \ if \ g|_{X^2} \in syl_2(S_6) \setminus syl_2 A_6. \end{cases} \tag{1}$$

The structure of $syl_2(A_6)$ is the same as subgroup $H_6 : H_6 < syl_2(S_4) \times (C_2)$ where $H_6 = \{(g, h) | g \in syl_2(S_4), h \in AutX\}$. So last bijection determined by (1) giving us $syl_2 A_6 \simeq Syl_2 S_4$. As a corollary we have $syl_2 A_{2^k+2} \simeq syl_2 S_{2^k}$. The structure of $syl_2(A_7)$ is the same as of the subgroup $H_7 : H_7 < syl_2(S_4) \times S_2$ where $H_6 = \{(g, h) | g \in syl_2(S_4), h \in S_2\}$ and h depends of g:

$$\begin{cases} h_g = e, \ \ if \ g|_{X^2} \in syl_2 A_7, \\ h_g = (i,j), i,j \in \{5,6,7\}, \ if \ g|_{X^2} \in syl_2 S_7 \setminus syl_2 A_7. \end{cases} \tag{2}$$

The generators of the group H_7 have the form $(g, h), \ g \in syl_2(S_4), \ h \in C_2$, namely: $\{\beta_0; \beta_1, \tau\} \cup \{(5,6)\}$. An element h_g can't be a product of two transpositions of the set: $(i,j), (j,k), (i,k)$, where $i,j,k \in \{5,6,7\}$, because $(i,j)(j,k) = (i,k,j)$ but $ord(i,k,j) = 3$, so such element doesn't belong to 2-subgroup. In general elements of $syl_2 A_{4k+3}$ have the structure (2), where $h_g = (i,j), \ i,j \in \{4k+1, 4k+2, 4k+3\}$ and $g \in syl_2 S_{4k}$.

Also $|syl_2(S_8)| = 2^7$, $|syl_2(S_4)| = 2^3$, so $|syl_2(S_8) \times syl_2(S_4)| = 2^{10}$ and $|H_{12}| = 2^9$, because its index in $syl_2(S_8) \times syl_2(S_4)$ is 2. The structure of $syl_2(A_6)$ is the same as of $H_6 < Syl_2(S_4) \times (C_2)$.
Here $H_6 = \{(g, h_g) | g \in syl_2(S_4), h_g \in C_2\}$.

The orders of this groups are equal. Indeed

$$|syl_2(A_7)| = 2^{[7/2]+[7/4]-1} = 2^3 = |H_7|.$$

In case $g|_{L_2} \in S_7 \setminus A_7$ we have C_3^2 ways to construct one transposition that is direct factor in H which complete $syl_2 S_4$ to H_7 by one transposition : $\{(5,6); (6,7); (5,7)\}$.

The structure of $syl_2(A_{2^k+2^l})$ $(k > l)$ is the same as of the subgroup $H_{2^k+2^l} < syl_2(S_{2^k}) \times syl_2(S_{2^l})$, for that $[syl_2(S_{2^k}) \times syl_2(S_{2^l}) : H] = 2$. $|syl_2(A_{2^k+2^l})| = 2^{[(2^k+2^l)!/2]+[(2^k+2^l)!/4]+....-1}$.
Here $H = \{(g, h_g) | g \in syl_2(S_2^k), h_g \in syl_2(S_2^l\}$, where

$$\begin{cases} h \in A_{2^l}, \ \ if \ g|_{X^{k-1}} \in A_{2^k}, \\ h : h|_{X^2} \in syl_2(S_{2^l}) \setminus syl_2 A_{2^l}, \ if \ g|_{X^k} \in syl_2 S_{2^k} \setminus syl_2 A_{2^k}. \end{cases} \tag{3}$$

The generators of the group H_7 have the form $(g, h), \ g \in syl_2(S_4), \ h \in C_2$, namely: $\beta_0; \beta_1, \tau \cup (5,6)$.

I.e. for element $\beta_\sigma(2i-1) = 2\sigma(i) - 1, \ \beta_\sigma(2i) = 2\sigma(i), \ \sigma_i \in \{1, 2, ..., 2^{k-1}\}$.

Let us present new operation $\boxtimes$ (similar to that is in [1]) that is an even subdirect product of $sylS_{2^i}$, $n = 2^{k_0} + 2^{k_1} + ... + 2^{k_m}$, $0 \leq k_0 < k_1 < ... < k_m$ and $m \geq 0$, i.e.,

$$syl_2S_{2^{k_1}} \boxtimes syl_2S_{2^{k_2}} \boxtimes ... \boxtimes syl_2S_{2^{k_l}} = Par(syl_2S_{2^{k_1}} \times syl_2S_{2^{k_2}} \times ... \times syl_2S_{2^{k_l}}),$$

where $Par(G)$ – set of all even permutations of G. Note, that $\boxtimes$ is not associated operation, for instance $ord(G_1 \boxtimes G_2 \boxtimes G_3) = |G_1 \times G_2 \times G_3| : 2$ but $ord((G_1 \boxtimes G_2) \boxtimes G_3) = |G_1 \times G_2 \times G_3| : 4$. For cases $n = 4k + 1$, $n = 4k + 3$ it follows from Legendre's formula.

It is well known that the $syl_2S_{2^{k_i}} \simeq \wr_{j=1}^{k_i} C_2$. Since Sylow p-subgroup of direct product is direct product of Sylow p-subgroups and fact that automorphism of rooted tree keeps an vertex-edge incidence relation then we have $AutX^{[k_0]} \times AutX^{[k_1]} \times ... \times AutX^{[k_m]} \simeq syl_2S_n$, $n = 2^{k_1} + 2^{k_2} + ... + 2^{k_l}$, $k_i \geq 0$, $k_i < k_{i-1}$. Let us denote a subgroup, that consists of all even substitutions from syl_2S_n as $AutX^{[k_0]} \boxtimes AutX^{[k_1]} \boxtimes ... \boxtimes AutX^{[k_m]}$, where a states of v.p. on $X^{k_0-1} \sqcup X^{k_1-1} \sqcup ... \sqcup X^{k_m-1}$ are related by congruence:

$$\sum_{i=0}^{m} \sum_{j=1}^{2^{k_i-1}} s_{k_i-1,j}(\alpha_i) \equiv 0 \,(\mathrm{mod} 2). \tag{4}$$

Lemma 4.1. *If number of active states on a last level of $AutX^{[k_i]}$ from $AutX^{[k_0]} \boxtimes ... \boxtimes AutX^{[k_m]}$ is odd, then it is subdirect product of groups $AutX^{[k_0]}$, ... , $AutX^{[k_m]}$.*

Proof. It is a quotient group which is a homomorphic image obtained by a mapping from $AutX^{[k_0]} \times AutX^{[k_1]} \times ... \times AutX^{[k_m]} \simeq syl_2S_n$ to this quotient group. A kernel of φ consists of all automorphisms which satisfy a congruence $\sum_{i=0}^{m} \sum_{j=1}^{2^{k_i-1}} s_{k_i-1,j}(\alpha_i) \equiv 1 \,(\mathrm{mod} 2)$. At once from definition follows, that if number of states on last level of $AutX^{[k_i]}$ is odd, then a subgroup from the condition is subdirect product of groups $AutX^{[k_0]}$, ... , $AutX^{[k_m]}$. Actually for every state of automorphism α from $AutX^{[k_i]}$ on X^l, $l < k_i - 1$ we have that $(e, ..., e, \alpha_i, e, ..., e)$ belongs to $AutX^{[k_0]} \times AutX^{[k_1]} \times ... \times AutX^{[k_m]}$. An arbitrary state from X^{k_i-1} is included in $AutX^{[k_0]} \boxtimes AutX^{[k_1]} \boxtimes ... \boxtimes AutX^{[k_m]}$ together with even number of states from last levels of $X^{[k_0]}$, ... , $X^{[k_m]}$. Analogous fact was proved in [1] for a direct sum of permutations groups and for their subgroups which consists of all even permutations. Our statement is a restiction on a syl_2S_n. ∎

The Sylow subgroup $syl_2(A_n)$ has index 2 in $syl_2(S_n)$ and it's structure: $syl_2S_{2^{k_1}} \boxtimes syl_2S_{2^{k_2}} \boxtimes ... \boxtimes Syl_2S_{2^{k_l}}$.

Lemma 4.2. *If $n = 4k+2$, then the subgroup syl_2A_n is isomorphic to syl_2S_{4k}, where $k \in \mathbb{N}$.*

Proof. Let us consider the subgroup $H_{4k+2} = \{(g, h_g)|g \in syl_2(S_{4k}), h_g \in S_2\}$, where

$$\begin{cases} h_g = e, \ \ if \ g|_{X^k} \in syl_2(A_{4k+2}), \\ h_g = (4k+1, 4k+2), \ if \ g|_{X^k} \in syl_2(S_{4k+2}) \setminus syl_2(A_{4k+2}). \end{cases} \tag{5}$$

For instance the structure of $syl_2(A_6)$ is the same as subgroup $H_6 : H_6 < syl_2(S_4) \times (C_2)$, where $H_6 = \{(g, h)|g \in syl_2(S_4), h \in AutX\}$. So last bijection determined by (5) give us $syl_2A_6 \simeq syl_2S_4$. As a corollary we have $syl_2A_{2^k+2} \simeq syl_2S_{2^k}$.

Bijection correspondence between set of elements of $syl_2(A_n)$ and $syl_2(S_{4k})$ we have from (5). Let's consider a mapping $\phi : syl_2(S_{4k}) \to syl_2(A_{4k+2})$ if $\sigma \in syl_2(S_{4k})$ then $\phi(\sigma) = \sigma \circ (4k+1, 4k+2)^{\chi(\sigma)} = (\sigma, (4k+1, 4k+2)^{\chi(\sigma)})$, where $\chi(\sigma)$ is number of transposition in σ by module 2. So $\phi(\sigma) \in syl_2(A_{4k+2})$. If $\phi(\sigma) \in A_n$ then $\chi(\sigma) = 0$, so $\phi(\sigma) \in syl_2(A_{n-1})$. Check that ϕ is homomorphism. Assume that $\sigma_1 \in syl_2(S_{4k} \backslash A_{4k})$, $\sigma_2 \in syl_2(A_{4k})$, then $\phi(\sigma_1)\phi(\sigma_2) = (\sigma_1, h^{\chi(\sigma_1)})(\sigma_2, e) = (\sigma_1\sigma_2, h) = \sigma_1\sigma_2 \circ (4k+1, 4k+2)$, where $(\sigma_i, h) = \sigma_i \circ h^{\chi(\sigma_i)} \in syl_2(A_{4k+2})$. If $\sigma_1, \ \sigma_2 \in S_{2^k} \backslash A_{2^k}$, then $\phi(\sigma_1)\phi(\sigma_2) = (\sigma_1, h^{\chi(\sigma_1)})(\sigma_2, h^{\chi(\sigma_2)}) = (\sigma_1\sigma_2, \ e) = (a, \ e)$, where $\sigma_1\sigma_2 = a \in A_{4k+2}$. So it is isomorphism. ∎

Let $n_m = 2^{k_0} + 2^{k_1} + ... + 2^{k_m}$, where $0 \leq k_0 < k_1 < ... < k_m$ and $m \geq 0$.

Theorem 4.1. *If $n_m = 4k+2$, then the minimal set of generators for $syl_2A_{n_m}$ has $\sum_{i=1}^{m} k_i$ elements.*

Proof. Actually, according to Lemma 4.2, syl_2A_{4k+2} is isomorphic to syl_2S_{4k}. It is well known (see Chapter 10, especially Section 10.4.) [20] that $syl_2S_{4k} \simeq syl_2S_{2^{k_1}} \times ... \times syl_2S_{2^{k_m}}$, where $4k = 2^{k_1} + ... + 2^{k_m}$, $k_1 < ... < k_m$. On the other hand, $syl_2S_{2^{k_i}} \simeq AutX^{[k_i]}$, so there exists the homomorphism φ from every factor $syl_2S_{2^{k_i}}$ onto $C_2^{k_i}$. Such homomorphism was defined in Corollary 3.3 and in [11]. And what is more it is known that $AutX^{[k_i]}$ has a minimal generating set of k_i generators [11]. Thus, there exists the homomorphism from $AutX^{[k_1]} \times \ ... \ \times AutX^{[k_m]}$ onto $C_2^{k_1} \times ... \times C_2^{k_m}$, so the rank of syl_2A_{4k+2} is $\sum_{i=1}^{m} k_i$, where $k_1 = 1$. ∎

This result was confirmed by the algebraic system GAP. Actually, it was founded by GAP that the minimal generating set for syl_2A_{14}, $syl_2A_{14} \simeq syl_2S_{12} \simeq syl_2S_{2^2} \times Syl_2S_{2^3}$, of 5 elements:
$(11, 12)(13, 14), (9, 11)(10, 12), (7, 8)(9, 10), (1, 5)(2, 6)(3, 7)(4, 8), (1, 3)(2, 4)$.

Lemma 4.3. *If $n_m \equiv 1(\mathrm{mod}2)$, then there exists a point n from tuple M of n_m points indexed by numbers from 1 to n_m, such that $St_{syl_2S_{n_m}}(n)$ is isomorphic to $syl_2S_{n_m}$ acting on a tuple M.*

Proof. If S_{n_m} acts on M, then one of a Sylow 2-subgroups $H < S_{n_m}$ is isomorphic to $AutX^{[k_0]} \times AutX^{[k_1]} \times ... \times AutX^{[k_m]}$, that acts on tuple of n_m points, where $n_m = 2^{k_0} + 2^{k_1} + ... + 2^{k_m}$, $k_0 < k_1 < ... < k_m$. By virtue of the fact that $n_m \equiv 1(\mathrm{mod}2)$, then $k_0 = 0$. Thus vertex with number n from $X^{[k_0]}$ has a stabilizer $St_H(n) \simeq syl_2S_{n_m}$, because the group of automorphisms of such group keeps an vertex-edge incidence relation of $X^{[k_i]}$, $i \in \{0, ..., m\}$. Thus, action of every Sylow 2-subgroup of S_{n_m}, where $n_m \equiv 1(\,\mathrm{mod}\,2)$, fix one element from $\{1, 2, ..., n_m\}$. ∎

According to the Sylow theorem all Sylows p-subgroups are conjugated so their actions are isomorphic. In particular, a Sylow 2-subgroup of S_{2^r} is self-normalizing. The number of Sylow 2-subgroups of S_{2^r} is $2^r! : 2^e$ where $e = 1 + 2 + ... + 2^{r-1}$ [16].

Remark 1. *The mentioned in Lemma 4.2 isomorphism may be extended to $syl_2A_{4k+3} \simeq syl_2A_{4k+2} \simeq syl_2S_{4k+1} \simeq syl_2S_{4k}$.*

Proof. Since in accordance with Lemma 4.3 an action of syl_2A_{4k+3} on the set of $4k + 3$ elements fixes one point, then this group as group of action is isomorphic to syl_2A_{4k+2}. For a similar reason $syl_2A_{4k+1} \simeq syl_2A_{4k}$. As well as it was proved in Lemma 4.2 that $syl_2A_{4k+2} \simeq syl_2S_{4k}$. ∎

Proposition 4.1. *If $n = 4k$, then index $syl_2(A_{n+3})$ in A_{n+3} is equal to $[S_{4k+1} : syl_2(A_{4k+1})](2k + 1)(4k + 3)$, index $syl_2(A_{n+1})$ in A_{n+1} as a subgroup of index 2^{m-1}, where m is the maximal natural number, for which $4k!$ is divisible by 2^m.*

Proof. For $syl_2(A_{n+3})$ its cardinality equal to maximal power of 2 which divide $(4k + 3)!$. This power on 1 grater then correspondent power in $(4k + 1)!$ because $(4k + 3)! = (4k + 1)!(4k + 2)(4k + 3) = (4k + 1)!2(2k + 1)(4k + 3)$ so $\mid syl_2A_{n+3} \mid = 2^m \cdot 2 = 2^{m+1}$. As a result of it indexes of A_{n+3} and A_{n+1} are following: $[S_{4k+1} : syl_2(A_{4k+1})] = \frac{(4k+1)!}{2^m}$ and $[S_{4k+3} : syl_2(A_{4k+3})] = [S_{4k+1} : syl_2(A_{4k+1})](2k + 1)(4k + 3) = \frac{(4k+1)!}{2^m}(2k + 1)(4k + 3)$. ∎

Proposition 4.2. *If $n = 2k$ then $[syl_2(A_n) : syl_2(S_{n-1})] = 2^{m-1}$ and $syl_2(S_{n-1}) \hookrightarrow syl_2(A_n)$, where m is the maximal power of 2 in factorization of n.*

Proof. Let $t = |syl_2(S_{n-1})|$ therefore t is a maximal power of 2 in $(n - 1)!$. $|syl_2(A_n)|$ is equal to the maximal power of 2 in $(n!/2)$. Since $n = 2k$ then $(n/2)! = (n - 1)!\frac{n}{2}$. Therefore $\frac{|syl_2(A_n)|}{|syl_2(S_{n-1})|} = \frac{2^{m-1}}{2^t}2^t = 2^{m-1}$. Note that for odd

$m = n-1$ the group $syl_2(S_m) \simeq syl_2(S_{m-1})$ i.e., $syl_2(S_{n-1}) \simeq syl_2(S_{n-2})$. The group $syl_2(S_{n-2})$ contains the automorphism of correspondent binary subtree with last level X^{n-2} and this automorphism realizes the permutation σ on X^{n-2}. For every $\sigma \in syl_2(S_{n-2})$ let us set in correspondence a permutation $\sigma(n-1,n)^{\chi(\sigma)} \in syl_2(A_n)$, where $\chi(\sigma)$ – number of transposition in σ by $mod\,2$, so it is bijection $\phi(\sigma) \longmapsto \sigma(n-1,n)\chi(\sigma)$ that has property of homomorphism, see Lemma 4.2. Thus, we prove that $syl_2(S_{n-1}) \hookrightarrow syl_2(A_n)$ and its index is 2^{m-1}. ∎

Proposition 4.3. *The ratio of* $|syl_2(A_{4k+3})|$ *and* $|syl_2(A_{4k+1})|$ *is equal to 2 and ratio of indexes* $[A_{4k+3} : Syl_2(A_{4k+3})]$ *and* $[A_{4k+1} : syl_2(A_{4k+1})]$ *is equal to* $(2k+1)(4k+3)$.

Proof. The ratio $|syl_2(A_{4k+3})| : |syl_2(A_{4k+1})| = 2$ holds because Legendre's formula gives us new one power of 2 in $(4k+3)!$ in compering with $(4k+1)!$. Second part of statement follows from theorem about p-subgroup of H, $[G : H] \neq kp$ then one of p-subgroups of H is Sylow p-group of G. In this case $p = 2$ but $|syl_2(A_{4k+3})| : |syl_2(A_{4k+1})| = 2$ so we have to divide ratio of indexes $\frac{(4k+3)!|syl_2(A_{4k+1})|}{(4k+1)!|syl_2(A_{4k+3})|}$ on 2. Really it is so because $\frac{|syl_2(A_{4k+1})|}{|syl_2(A_{4k+3})|} = \frac{1}{2}$. ∎

Let $n = 2^{k_0} + 2^{k_1} + ... + 2^{k_m}$, where $0 \leq k_0 < k_1 < ... < k_m$ and $m \geq 0$. Also recall that $syl_2S_n = syl_2S_{2^{k_0}} \times ... \times syl_2S_{2^{k_m}}$.

Property 2. *Relation between sizes of the Sylows subgroup for* $n = 4k-2$ *and* $n = 4k$ *is given by* $|Syl_2(A_{4k-2})| = 2^i\,|Syl_2(A_{4k})|$, *where value* i *depends only of power of 2 in decomposition of prime number of* k.

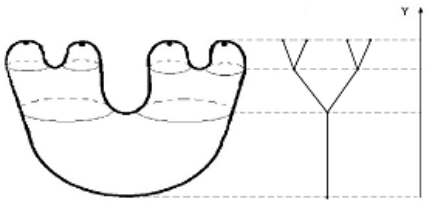
Proof. Really $|A_{4k-2}| = \frac{(4k-2)!}{2}$, therefore $|A_{4k}| = \frac{(4k-2)!}{2}(4k-1)4k$, it means that i determines only by k and is not bounded. ∎

Also it can be deduced from Lemma 8, Corollary 3 and Corollary 4 that derived length of $syl_2A_2^k$ is not always equal to k as it was said in Lemma 3 of [1] because in case A_{2^k} if $k = 2$ its $syl_2A_4 \simeq K_4$ but K_4 is abelian group so its derived length is 1.

5. SOME APPLICATIONS OF CONSTRUCTED GENERATING SET

Let us consider a function of Morse [25] $f : D^2 \to \mathbb{R}$ that painted at pict. 2 and graph of Kronrod-Reeb [26] that obtained by contraction every set's component of level of $f^{-1}(c)$ in point. Group of automorphism of this graph is isomorphic to $syl_2S_{2^k}$, where $k = 2$ in general case we have regular binary rooted tree for arbitrary $k \in \mathbb{N}$.

According to investigations of [27] for D^2 we have that $syl_2S_{2^k} > G_k \simeq syl_2A_{2^k}$ is quotient group of diffeomorphism group that stabilize a function



and isotopic to identity. Analogously to investigations of [26, 27, 28] there is the short exact sequence $0 \to \mathbb{Z}^m \to \pi_1 O_f(f) \to G \to 0$, where G is the group of automorphisms Reeb's (Kronrod-Reeb) graph [26] that has the main property

$$G \simeq syl_2 S_{2^k}$$

if a function of Morse has 2^k points of local maximum, and $O_f(f)$ is the orbit under the action of diffeomorphism group, so it could be way to transfer it for a group $syl_2(S_{2^k})$, where m in $\mathbb{Z}^m$ is number of inner vertices in Reeb's graph, in case for $syl_2 S_4$ we have $m = 3$.

Higher half of projection of manifold from pic. 2 can be determed by product of the quadratic forms $-((x+4)^2+y^2)((x+3)^2+y^2)((x-3)^2+y^2)((x-4)^2+y^2) = z$ in points $(-4,0)(-3,0)(3,0)(4,0)$ it reachs a maximum value 0. Generally there is $-d_1^2 d_2^2 d_3^2 d_4^2 = z$.

6. CONCLUSION

The proof of minimality of constructed generating sets was done, also the description of the structure $syl_2 A_{2^k}$, $syl_2 A_{4m+2}$, $syl_2 A_{4m+3}$, $syl_2 S_{4m}$, $syl_2 S_{4m+1}$ and its properties were founded. The structure of Sylow 2-subgroups $syl_2 A_{2^k}$, $syl_2 A_n$, where $n = 4k+2$, were founded. The centralizer structures of $syl_2 A_{2^k}$ and $syl_2 S_{2^k}$ were described.

The total number of minimal generating sets for $syl_2 A_{2^k}$ and $syl_2 S_{2^k}$ was obtained.

References

[1] *U. Dmitruk, V. Suschansky,* Structure of 2-sylow subgroup of alternating group and normalizers of symmetric and alternating group. UMJ. 3(1981), 304-312.

[2] *R. Skuratovskii,* "Corepresentation of a Sylow p-subgroup of a group Sn". Cybernetics and systems analysis, 1(2009), 27-41.

[3] *B. Pawlik,* The action of Sylow 2-subgroups of symmetric groups on the set of bases and the problem of isomorphism of their Cayley graphs. Algebra and Discrete Mathematics, **21**, 2(2016), 264-281.

[4] V. Ivanchenko, *System of generators for 2-Sylow subgroup alternating group*, The forth ukraine conference of young scientists. Kiev: *KPI* 2015, (http://matan.kpi.ua/uk/ysmp4conf.html), pg. 60.

[5] R.V. Skuratovskii, Y.A. Drozd, *Generators and and relations for wreath products of groups*, Ukr Math J., **60**, 7(2008), 11681171.

[6] R. Grigorchuk, V. Nekrashevich, V. Sushchanskii, *Automata, Dynamical Systems, and Groups*, Trudy mat. inst. imeny Steklova, 231(2000) 134–214.

[7] V. Nekrashevych, *Self-similar groups*, International University Bremen, American Mathematical Society, 2005, Monographs, vol. 117.

[8] D. Gorenstein, *Finite groups*, 2nd edition, Chelsea New York, 1980.

[9] Martin Isaacs, *Finite Group Theory*, American Mathematical Society. 15 Nov 2008.

[10] I.V. Bondarenko, I.O. Samoilovych *On finite generation of self-similar groups of finite type*, International Journal of Algebra and Computation, **23**, 1(2013), 69-79.

[11] R.I. Grigorchuk, *Solved and unsolved problems around one group*, Infinite Groups: Geometric, Combinatorial and Dynamical Aspects. asel, Progress Math., **248**(2005), 117-218.

[12] V. Magnus, A. Karras, D. Soliter, *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*, New York, Dover Books on Mathematics, INC. Miniola, 1976.

[13] V.S. Sikora, V. I. Suschanskii, *Operations on groups of permutations* Chernivci: Ruta, 2003.

[14] R. V. Skuratovskii, *Generators and relations of Sylow p-subgroups of symmetric groups* S_n. Naukovi visti KPI, pp. 93-101, 2014.

[15] M. I. Kargapolov, J. I. Merzljakov, *Fundamentals of the Theory of Groups Springer*, Softcover reprint of the original 1st ed. 1979 edition. Springer. 1st ed. 1979,

[16] Louis Weisner, *On the Sylow Subgroups of the Symmetric and Alternating Groups*, American Journal of Mathematics, **47**, 2(1925), 121-124.

[17] Oleg Bogopolski, *An Introduction to the Theory of Groups*, European Mathematical Society. 2008.

[18] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer, New York, Fourth Ed., 1995.

[19] A.G. Myasnikov, V. Shpilrain, A. Ushakov, *A practical attack on some braid group based cryptographic protocols*, Crypto 2005, Springer Lect., Notes Comp. (2005), Sc. 3621, pp. 86-96.

[20] Hall, Marshall, *The theory of groups*, New York, N.Y.: Macmillan. (1959). 434 pp.

[21] Nikolay Nikolov, *On the commutator width of perfect groups*, Bull. London Math. Soc., **36**(2004),3036.

[22] L. Kaloujnine, *"La structure des p-groupes de Sylow des groupes symetriques finis"*, Annales Scientifiques de l'Ecole Normale Superieure, Troisieme Serie, **65**(1948), 239276.

[23] J.D.P. Meldrum, *Wreath Products of Groups and Semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematic English. Publisher, Longman, 1st Edition, Jun (1995).

[24] Roger C. Lyndon, Paul E. Schupp, *Combinatorial group theory*, Springer, (2001) Series: Classics in Mathematics 339 P.

[25] V. V. Sharko, *Smooth topological equivalence of functions of surfaces*, Ukrainian Mathematical Journal, May, **55**, Issue 5(2003), 832846.

[26] S. I. Maksymenko, *Homotopy types of stabilizers and orbits of Morse functions on surfaces*, Annals of Global Analysis and Geometry., **29**, 3(2006), 241285.

[27] S. I. Maksymenko, *Path-components of Morse mappings space Some problems of contemporary mathematics*, Proceedings of Institute of Mathematics of Ukrainian NAS. 1998, vol. 25, pp. 135-153.

[28] R. V. Skuratovskii, *Minimal generating systems and properties of $Syl_2A_{2^k}$ and Syl_2A_n*, X International Algebraic Conference in Odessa dedicated to the 70th anniversary of Yu. A. Drozd. (2015), p. 104.

[29] R. V. Skuratovskii, *Minimal generating systems and structure of $Syl_2A_{2^k}$ and Syl_2A_n*, International Conference and PhD-Master Summer School on Graphs and Groups, Spectra and Symmetries. (2016), source: http://math.nsc.ru/conference/g2/g2s2/exptext/Skuratovskii-abstract-G2S2+.pdf.

[30] R. V. Skuratovskii, *Structure and minimal generating sets of Sylow 2-subgroups of alternating groups and their centralizers*, 11th International Algebraic Conference in Ukraine, Kiev, (2017), p. 154. https://www.imath.kiev.ua/ algebra/iacu2017/participants

[31] V. Shpilrain, A. Ushakov, *A new key exchange protocol on the decomposition problem*, Contemp. Math. Volume 418. (2006), pp. 161-167.

[32] J. Hughes, A. Tannenbaum, *Length-based attacks for certain group based encryption rewriting systems*, Inst. for Mathematics and Its Applic. (Minneapolis MN) 2002, Springer Lect. Notes in Comput. Sci. 2384 (2002) pp. 176189. Avalilable at http: //front.math.ucdavis.edu/0306.6032