Abstract. The involutive base of a Sylow 2-subgroup $P_n(2)$ of symmetric group $S_{2^n}$ is a minimal generating set of this subgroup consisting of elements which are involutions. The Cayley graphs of group $P_n(2)$ on involutive bases may be naturally considered as the undirected ones. The exact number of such bases is not known. In presented paper the necessary condition for base $\mathfrak{B}$ of group $P_n(2)$ to be involutive is prooved.

1. Introduction

Over the past half-century, the theory of Sylow $p$-subgroups of symmetric and alternating groups has become a subject of extensive research in the field of group theory. It was specifically studied by L. Kaloujnine (e.g. [4, 5]), V. Sushchanskyy (e.g. [1, 8]) and their students (e.g. [3, 6, 7]).

The case of $p = 2$ is particularly distinguished from the others Sylow $p$-subgroups of symmetric groups. The initial study of the subgroups proved that due to their specificity, they require a completely separate approach and research methods than the general case (in the early works on Sylow $p$-subgroups of symmetric groups, Kaloujnine assumed that $p \neq 2$). One of the most important aspects distinguishing this case is the fact that as of today, the group of automorphisms of this group has not yet been characterized (for $p \neq 2$ full characterization is known).
By base of the group we mean a minimal set of generators of this group. In this paper we are particullary interested in those bases of $P_n(2)$ in which every generator is an involution (an element of order 2). The special case of involutive bases – so called diagonal bases – were considered in the articles [6] and [7], where they were used to discuss the isomorphism problem of Cayley graph of groups $P_n(2)$. In [6] the exact number of different diagonal bases of $P_n(2)$ was established. The number of different involutive bases of such groups is not known. The results from this paper may be considered a first step towards the general characterisation of such bases.

The outline of this paper is as follows. In the Section 2 we remind basic facts and definitions about Sylow $p$-subgroups $P_n(p)$ of symmetric groups $S_{p^n}$ and the polynomial representation of such subgroups. In Section 3 the necessary condition for base of $P_n(2)$ to be involutive is proved and the list of involutive generators of $P_n(2)$ with the first coordinate equals to 1 for small values of $n$ is presented.

2. Preliminaries

Let $P_n(p)$ be the Sylow $p$-subgroup of symmetric group $S_{p^n}$. It is well known that $P_n(p)$ is isomorphic to the wreath product of $n$ cyclic permutation groups of order $p$ (see, e.g. [2]):

$$P_n(p) \cong \bigast_{i=1}^{n} C_p^{(i)}.$$  

Let $X_i$ be the vector of variables $x_1, x_2, \ldots, x_i$.

In this paper we use polynomial (Kaloujnine) representation of groups $P_n(p)$ (see e.g. [5,6,8]). Every element $f$ of such group can be represented by a sequence

$$f = [f_1, f_2(X_1), \ldots, f_n(X_n)],$$  

(1)

where $f_1 \in \mathbb{Z}_p$ and $f_i : \mathbb{Z}_p^{i-1} \to \mathbb{Z}_p$ for $i = 2, \ldots, n$ are reduced polynomials from the quotient ring $\mathbb{Z}_p[X_i]/(x_1^{p_i} - x_1, \ldots, x_i^{p_i} - x_i)$. We call such element $f$ a tableau. By $[f]_i$ we denote the $i$-th coordinate of tableau $f$:

$$[f]_1 = f_1 \quad \text{and} \quad [f]_i = f_i(X_{i-1})$$

for $i = 2, \ldots, n.$
For tableaux $f, g \in P_n(p)$ where $f$ have form (1) and
\[ g = [g_1, g_2(X_1), \ldots, g_n(X_{n-1})] \]
we have
\[ fg = [f_1 + g_1, f_2(X_1) + g_2(x_1 + f_1), \ldots, f_n(X_{n-1}) + g_n(x_1 + f_1, x_2 + f_2(X_1), \ldots, x_{n-1} + f_{n-1}(X_{n-2}))], \quad (2) \]
and
\[ f^{-1} = [-f_1, -f_2(x_1 - f_1), \ldots, -f_n(x_1 - f_1, x_2 - f_2(x_1 - f_1), \ldots, x_{n-1} - f_{n-1}(x_1 - f_1, \ldots))] \]
The tableau $id = [0, 0, \ldots, 0]$ is the neutral element of the product (2).

The group $P_n(p)$ acts on the vector space $\mathbb{Z}_p^n$ in a natural way
\[ u^f = [u_1 + f_1, u_2 + f_2(u_1), \ldots, u_n + f_n(u_1, u_2, \ldots, u_{n-1})], \]
where $u = [u_1, u_2, \ldots, u_n] \in \mathbb{Z}_p^n$ and $f$ have form (1).

Let
\[ \overline{x_n} = x_1 \cdot x_2 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i \]
and
\[ \overline{x_n/ x_k} = x_1 \cdot \ldots \cdot x_{k-1} \cdot x_{k+1} \cdot \ldots \cdot x_n = \prod_{i=1,i\neq k}^{n} x_i \]
for every $k = 1, \ldots, n$.

We define a natural epimorphism $\varphi : P_n(p) \to \mathbb{Z}_p^k$ in the following way
\[ [\varphi(f)]_i = c([f]_i), \]
where $c(f)$ is a coefficient of the monomial $\overline{x_{i-1}}$ in the polynomial $f$. The vector $\varphi(f)$ we call a type of a tableau $f$.

It is known that every base of group $P_n(p)$ contains exactly $n$ elements. Moreover, the set $\mathcal{B} = \{B_1, \ldots, B_n\}$ is a base of group $P_n(p)$ if and only if the set $\{\varphi(B_1), \ldots, \varphi(B_n)\}$ is a basis of the linear space $\mathbb{Z}_p^k$ over $\mathbb{Z}_p$ (see [8] for details).
3. Main results

From now on we assume that $p = 2$.

Let $I \subset \{1, \ldots, n\}$ be some set of indexes. From the definition of the product of tableaux (2) arise a natural way of the action of a group $P_n(2)$ on the set of monomials

$$\left( \prod_{i \in I} x_i \right)^f = \prod_{i \in I} (x_i + f_i(X_{i-1})),$$

where $f$ have form (1).

**Lemma 1.** Let $f = [1, f_2(X_1), \ldots, f_n(X_{n-1})] \in P_n(2)$. Polynomial $(\overline{x_n})^f$ contains a monomials $x_n$ and $x_n/x_1$.

**Proof.** By (3) we have

$$(\overline{x_n})^f = \prod_{i=1}^n (x_i + f_i(X_{i-1})).$$

Of course the only way to obtain a monomial $x_n$ from the above product is to multiply $x_i$-s from every component $\left(x_i + f_i(X_{i-1})\right)$. On the other hand

$$(\overline{x_n})^f = \prod_{i=1}^n (x_i + f_i(X_{i-1})) =$$

$$= (x_1 + 1) \cdot \prod_{i=2}^n (x_i + f_i(X_{i-1})) =$$

$$= x_1 \cdot \prod_{i=2}^n (x_i + f_i(X_{i-1})) + \prod_{i=2}^n (x_i + f_i(X_{i-1})).$$

We cannot obtain a monomial $x_n/x_1$ from the polynomial

$$x_1 \cdot \prod_{i=2}^n (x_i + f_i(X_{i-1})),
$$

so we have to investigate polynomial

$$\prod_{i=2}^n (x_i + f_i(X_{i-1})).$$
Let us notice that

\[
\prod_{i=2}^{n} (x_i + f_i(X_{i-1})) = (x_n + f_n(X_{n-1})) \cdot \prod_{i=2}^{n-1} (x_i + f_i(X_{i-1})) = \\
= x_n \cdot \prod_{i=2}^{n-1} (x_i + f_i(X_{i-1})) + f_n(X_{n-1}) \cdot \prod_{i=2}^{n-1} (x_i + f_i(X_{i-1})).
\]

The polynomial

\[
f_n(X_{n-1}) \cdot \prod_{i=2}^{n-1} (x_i + f_i(X_{i-1}))
\]

does not contain a variable \(x_n\), so the monomial \(x_n/x_1\) can occur only in the polynomial

\[
x_n \cdot \prod_{i=2}^{n-1} (x_i + f_i(X_{i-1})).
\]

Similarly

\[
x_n \cdot \prod_{i=2}^{n-1} (x_i + f_i(X_{i-1})) = x_n \cdot (x_{n-1} + f_{n-1}(X_{n-2})) \cdot \prod_{i=2}^{n-2} (x_i + f_i(X_{i-1})) = \\
= x_n \cdot x_{n-1} \cdot \prod_{i=2}^{n-2} (x_i + f_i(X_{i-1})) + \\
+ x_n \cdot f_{n-1}(X_{n-2}) \cdot \prod_{i=2}^{n-2} (x_i + f_i(X_{i-1})),
\]

where the polynomial

\[
x_n \cdot f_{n-1}(X_{n-2}) \cdot \prod_{i=2}^{n-2} (x_i + f_i(X_{i-1}))
\]

does not contain a variable \(x_{n-1}\).

By the induction we establish that in the polynomial \((x_n)^f\), the monomial \(x_n/x_1\) can be uniquely obtain as a product of 1 from the component \((x_1 + 1)\) and \(x_i\)-s from the components \((x_i + f_i(X_{i-1}))\) for \(i = 2, \ldots, n\).
Thus
\[(x_n)^f = x_n + x_n/x_1 + v(X_{i-1}),\]
where the polynomial \(v\) does not contain monomials \(x_n\) and \(x_n/x_1\).

From the proof of above lemma we can easily obtain the following

**Corollary 2.** Let \(f = [1, f_2(X_1), \ldots, f_n(X_{n-1})] \in P_n(2)\). Polynomial \((x_n/x_1)^f\) contains a monomial \(x_n/x_1\).

**Lemma 3.** Let \(f = [1, f_2(X_1), \ldots, f_n(X_{n-1})] \in P_n(2)\). Let \(I\) be a proper subset of the set \(\{1, \ldots, n\}\) such that \(I \neq \{2, 3, \ldots, n\}\). Polynomial \((\prod_{i \in I} x_i)^f\) does not contain a monomial \(x_n/x_1\).

**Proof.** Let us assume that \(k\) is the biggest integer from set \(\{1, \ldots, n\}\) such that \(k \notin I\). Thus \(I = \{i_1, i_2, \ldots, i_s, k+1, k+2, \ldots, n\}\), where \(i_1 < i_2 < \ldots < i_s < k\).

By the induction (similarly to the induction in the proof of Lemma 1 we show that
\[\left(\prod_{i \in I} x_i\right)^f = x_n \cdot x_{n-1} \cdot \ldots \cdot x_{k+1} \cdot \prod_{j=1}^s \left(x_{i_j} + f(X_{i_j-1})\right) + v(X_{n-1}),\]
where polynomial \(v\) does not contain a variable \(x_n\). Thus polynomial \(v\) does not contain a monomial \(x_n/x_1\). On the other hand polynomial
\[x_n \cdot x_{n-1} \cdot \ldots \cdot x_{k+1} \cdot \prod_{j=1}^s \left(x_{i_j} + f(X_{i_j-1})\right)\]
does not contain a variable \(x_k\), so it also does not contain a monomial \(x_n/x_1\). \(\Box\)

Now we can establish the Main Theorem of this paper:

**Theorem 4.** If the base \(B = \{B_1, B_2, \ldots, B_n\}\) of group \(P_n(2)\) is involutive then there exists unique generator \(B \in B\) such that \([B]_1 = 1\). The type of this generator is \(\varphi(B) = [1, 0, 0, \ldots, 0]_{n-1}\).

**Proof.** Let us assume that there is a generator \(B \in B\) such that \([B]_1 = 1\) and \([B]_k\) contains a monomial \(x_{k-1}\) for some \(k \in \{2, \ldots, n\}\) (i.e. the type of this generator
have a property $[\varphi(B)]_1 = 1$ and $[\varphi(B)]_k = 1$ for some $k \in \{2, \ldots, n\}$. Let

$$B = [1, f_2(X_1), \ldots, f_n(X_{n-1})]$$

and

$$f_k(X_{k-1}) = \overline{x_{k-1}} + \alpha \cdot \frac{x_{k-1}}{x_1} + f_k'(X_{k-1}),$$

where $\alpha \in \{0, 1\}$ and $f$ does not contain monomials $x_{k-1}$ nor $x_{k-1}/x_1$. Thus

$$[B^2]_k = \overline{x_{k-1}} + \alpha \cdot \frac{x_{k-1}}{x_1} + f_k'(X_{k-1}) +$$

$$+ \prod_{i=1}^{k-1} (x_i + f_i(X_{i-1})) + \alpha \cdot \prod_{i=2}^{k-1} (x_i + f_i(X_{i-1})) + f_k'(X_{k-1})'. \tag{4}$$

From Lemma 1 and Corollary 2 we have

$$\prod_{i=1}^{k-1} (x_i + f_i(X_{i-1})) = \overline{x_{k-1}} + \frac{x_{k-1}}{x_1} + v_1(X_{k-1}),$$

$$\prod_{i=2}^{k-1} (x_i + f_i(X_{i-1})) = \frac{x_{k-1}}{x_1} + v_2(X_{k-1}),$$

where polynomials $v_1$ and $v_2$ do not contain monomials $x_{k-1}$ nor $x_{k-1}/x_1$. From Lemma 3 we also know that $f_k'(X_{k-1})$ does not contain such monomials. Thus equation (4) can be written as

$$[B^2]_k = \overline{x_{k-1}} + \alpha \cdot \frac{x_{k-1}}{x_1} + f_k'(X_{k-1}) +$$

$$+ \overline{x_{k-1}} + \frac{x_{k-1}}{x_1} + v_1(X_{k-1}) + \alpha \cdot \left(\frac{x_{k-1}}{x_1} + v_2(X_{k-1})\right) + f_k'(X_{k-1}) =$$

$$= \frac{x_{k-1}}{x_1} + f_k'(X_{k-1}) + v_1(X_{k-1}) + \alpha \cdot v_2(X_{k-1}) + f_k'(X_{k-1}) =$$

$$= \frac{x_{k-1}}{x_1} + w(X_{k-1}),$$

where polynomial $w$ does not contain a monomial $x_{k-1}/x_1$. Thus $[B^2]_k \neq id$, so $B$ is not an involution. We have shown that every involutive generator $B \in \mathcal{B}$ with the property $[B]_1 = 1$ have type $\varphi(B) = [1, 0, \ldots, 0]$.

To show the uniqueness of such generator, let us assume that there are two different generators $B, B' \in \mathcal{B}$ such that $\varphi(B) = \varphi(B') = [1, 0, \ldots, 0]$. In this case
the set \( \{ \varphi(B_1), \ldots, \varphi(B_n) \} \) is not a basis of the linear space \( \mathbb{Z}_2^k \) over \( \mathbb{Z}_2 \), so the set \( \mathfrak{B} \) does not form a base of the group \( P_n(2) \). \( \square \)

Let us notice that the inverse of Theorem 4 does not hold in general, i.e. not every tableau \( f \in P_n(2) \) with the property \( \varphi(f) = [1, 0, \ldots, 0] \) is involutive.

Finally, for \( n \leq 4 \) let us consider the table of involutive elements \( f \) of \( P_n(2) \) for which \( \varphi(f) = [1, 0, \ldots, 0] \). Let \( \alpha, \beta, \gamma, \delta \in \mathbb{Z}_2^2 \):

\[
\begin{array}{c|c|c|c}
0 & 0 & \alpha x_2 x_3 + \beta x_2 + \gamma x_3 + \delta \\
1 & 1 & \alpha (x_1 x_2 + x_2 x_3) + \beta (x_1 + x_3) + \gamma x_3 + \delta \\
x_2 & 0 & \alpha (x_1 x_2 + x_2 x_3) + \beta (x_1 + x_3) + \gamma x_2 + \delta \\
x_2 + 1 & 1 & \alpha (x_1 x_2 + x_1 + x_3) + \beta x_2 x_3 + \gamma x_2 + \delta \\
0 & x_1 + x_2 & \alpha + \beta + \gamma (x_1 x_2 + x_1 x_3 + x_2 x_3) + \alpha x_1 + \beta x_2 + \gamma x_3 + \delta \\
1 & x_1 + x_2 + 1 & \alpha (x_1 x_2 + x_3) + \beta (x_1 x_3 + x_2 x_3) + \gamma (x_1 + x_2) + \delta \\
\end{array}
\]

References

7. Pawlik B.: The Girth of Cayley graphs of Sylow 2-subgroups of symmetric groups \( S_{2^n} \) on diagonal bases (under review).