Silesian J. Pure Appl. Math.
vol. 8, is. 1 (2018), 57–64

Bartłomiej PAWLIK

Institute of Mathematics, Silesian University of Technology, Gliwice, Poland

A NOTE ON INVOLUTIVE BASES OF SYLOW 2-SUBGROUPS OF SYMMETRIC GROUPS

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).

2010 Mathematics Subject Classification: 20B35, 20D20, 20E22.
Keywords: Sylow p-subgroups, group base, wreath product of groups.
Corresponding author: B. Pawlik (bartlomiej.pawlik@polsl.pl).
Received: 02.10.2018.

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]):

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

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

$$f = [f_1, f_2(X_1), \ldots, f_n(X_n)], \tag{1}$$

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 $\mathbb{Z}_p[X_i]/\langle x_1^p - x_1, \ldots, x_i^p - x_i\rangle$. We call such element f as a *tableau*. By $[f]_i$ we denote the i-th coordinate of tableau f:

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

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

$$\begin{aligned} fg = \big[&f_1 + g_1,\ f_2(X_1) + g_2(x_1 + f_1),\ \ldots, \\ &f_n(X_{n-1}) + g_n\big(x_1 + f_1, x_2 + f_2(X_1), \ldots, x_{n-1} + f_{n-1}(X_{n-2})\big)\big], \end{aligned} \tag{2}$$

and

$$\begin{aligned} f^{-1} = \Big[&-f_1,\ -f_2(x_1 - f_1),\ \ldots, \\ &-f_n\big(x_1 - f_1, x_2 - f_2(x_1 - f_1), \ldots, x_{n-1} - f_{n-1}(x_1 - f_1, \ldots)\big)\Big]. \end{aligned}$$

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

$$u^f = \big[u_1 + f_1, u_2 + f_2(u_1), \ldots, u_n + f_n(u_1, u_2, \ldots, u_{n-1})\big],$$

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 tablaeu f.

It is known that every base of group $P_n(p)$ contains exactly n elements. Moreover, the set $\mathfrak{B} = \{B_1, \ldots, B_n\}$ 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

$$\left(\prod_{i \in I} x_i\right)^f = \prod_{i \in I} \big(x_i + f_i(X_{i-1})\big), \tag{3}$$

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 $\overline{x_n}$ and $\overline{x_n/x_1}$.*

Proof. By (3) we have

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

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

$$\begin{aligned}
(\overline{x_n})^f &= \prod_{i=1}^{n} \Big(x_i + f_i(X_{i-1})\Big) = \\
&= (x_1 + 1) \cdot \prod_{i=2}^{n} \Big(x_i + f_i(X_{i-1})\Big) = \\
&= x_1 \cdot \prod_{i=2}^{n} \Big(x_i + f_i(X_{i-1})\Big) + \prod_{i=2}^{n} \Big(x_i + f_i(X_{i-1})\Big).
\end{aligned}$$

We cannot obtain a monomial $\overline{x_n/x_1}$ from the polynomial

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

so we have to investigate polynomial

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

Let us notice that

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

The polynomial

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

does not contain a variable x_n, so the monomial $\overline{x_n/x_1}$ can occur only in the polynomial

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

Similarly

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

where the polynomial

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

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

By the induction we establish that in the polynomial $(\overline{x_n})^f$, the monomial $\overline{x_n/x_1}$ can be <u>uniquely</u> obtain as a product of 1 from the component $(x_1 + 1)$ and x_i-s from the components $\Big(x_i + f_i(X_{i-1})\Big)$ for $i = 2, \ldots, n$.

Thus

$$(\overline{x_n})^f = \overline{x_n} + \overline{x_n/x_1} + v(X_{i-1}),$$

where the polynomial v does not contain monolials $\overline{x_n}$ and $\overline{x_n/x_1}$. □

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

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

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

Proof. Let us assume that k is the biggest integer from set $\{1, \dots, n\}$ such that $k \notin I$. Thus $I = \{i_1, i_2, \dots, i_s, k+1, k+2, \dots, n\}$, where $i_1 < i_2 < \dots < i_s < k$. By the induction (similarly to the induction in the proof of Lemma 1 we show that

$$\left(\prod_{i\in I} x_i\right)^f = x_n \cdot x_{n-1} \cdot \ldots \cdot x_{k+1} \cdot \prod_{j=1}^{s} \Big(x_{i_j} + f(X_{i_j-1})\Big) + v(X_{n-1}),$$

where polynomial v does not contain a variable x_n. Thus polynomial v does not contain a monomial $\overline{x_n/x_1}$. On the other hand polynomial

$$x_n \cdot x_{n-1} \cdot \ldots \cdot x_{k+1} \cdot \prod_{j=1}^{s} \Big(x_{i_j} + f(X_{i_j-1})\Big)$$

does not contain a variable x_k, so it also does not contain a monomial $\overline{x_n/x_1}$. □

Now we can establish the Main Theorem of this paper:

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

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

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

and

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

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

$$\begin{aligned} [B^2]_k = &\overline{x_{k-1}} + \alpha \cdot \overline{x_{k-1}/x_1} + f'_k(X_{k-1}) + \\ &+ \prod_{i=1}^{k-1}(x_i + f_i(X_{i-1})) + \alpha \cdot \prod_{i=2}^{k-1}(x_i + f_i(X_{i-1})) + f'_k(X^B_{k-1}). \end{aligned} \tag{4}$$

From Lemma 1 and Colloray 2 we have

$$\begin{aligned} \prod_{i=1}^{k-1}(x_i + f_i(X_{i-1})) &= \overline{x_{k-1}} + \overline{x_{k-1}/x_1} + v_1(X_{k-1}), \\ \prod_{i=2}^{k-1}(x_i + f_i(X_{i-1})) &= \overline{x_{k-1}/x_1} + v_2(X_{k-1}), \end{aligned}$$

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

$$\begin{aligned} [B^2]_k &= \overline{x_{k-1}} + \alpha \cdot \overline{x_{k-1}/x_1} + f'_k(X_{k-1}) + \\ &+ \overline{x_{k-1}} + \overline{x_{k-1}/x_1} + v_1(X_{k-1}) + \alpha \cdot \Big(\overline{x_{k-1}/x_1} + v_2(X_{k-1})\Big) + f'_k(X^B_{k-1}) = \\ &= \overline{x_{k-1}/x_1} + f'_k(X_{k-1}) + v_1(X_{k-1}) + \alpha \cdot v_2(X_{k-1}) + f'_k(X^B_{k-1}) = \\ &= \overline{x_{k-1}/x_1} + w(X_{k-1}), \end{aligned}$$

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

To show the uniqueness of such generator, let us assume that there are two different generators $B, B' \in \mathfrak{B}$ such that $\varphi(B) = \varphi(B') = [1, 0, \dots, 0]$. 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 $P_n(2)$. □

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 $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_2$:

$[f]_1$	$[f]_2$	$[f]_3$	$[f]_4$
1	0	0	$\alpha x_2x_3 + \beta x_2 + \gamma x_3 + \delta$
		1	$\alpha(x_1x_2 + x_2x_3) + \beta(x_1 + x_3) + \gamma x_2 + \delta$
		x_2	$\alpha(x_1x_2 + x_3) + \beta(x_2x_3 + x_3) + \gamma x_2 + \delta$
		$x_2 + 1$	$\alpha(x_1x_2 + x_1 + x_3) + \beta x_2x_3 + \gamma x_2 + \delta$
	1	0	$\alpha(x_1x_3 + x_2x_3) + \beta(x_1 + x_2) + \gamma x_3 + \delta$
		1	$(\alpha + \beta + \gamma)(x_1x_2 + x_1x_3 + x_2x_3) + \alpha x_1 + \beta x_2 + \gamma x_3 + \delta$
		$x_1 + x_2$	$(\alpha + \beta + \gamma)(x_1x_2 + x_1x_3 + x_2x_3) + \alpha x_1 + \beta x_2 + \gamma(x_1x_2 + x_3) + \delta$
		$x_1 + x_2 + 1$	$\alpha(x_1x_2 + x_3) + \beta(x_1x_3 + x_2x_3) + \gamma(x_1 + x_2) + \delta$

References

1. Bier A., Sushchansky V.: *Kaluzhnins representations of Sylow p-subgroups of automorphism groups of p-adic rooted trees.* Algebra Discrete Math. **19**, no. 1 (2015), 19–38.
2. Dixon J., Mortimer B.: *Permutation Groups*, Springer-Verlag, New York 1996.
3. Dmitruk Ju.V.: *The structure of a Sylow 2-subgroup of the symmetric group of degree* 2^n. Ukr. Math. Zhurn. **30**, no. 2 (1978), 155–164 (in Russian).
4. Kaluzhnin L.: *Sur les p-group de Sylow du groupe symetricque du degree* p^m. C.R. Acad. Sci. Paris **221** (1945), 222–224 (in French).
5. Kaluzhnin L.: *La structure des p-groupes de Sylow des groupes symetriques finis.* Ann. Sci. l'Ecole Norm. Sup. **65** (1948), 239–272 (in French).
6. Pawlik B.: *The action of Sylow 2-subgroups of symmetric groups on the set of bases and the problem of isomorphism of their Cayley graphs.* Algebra Discrete Math. **21**, no. 2 (2016), 264–281.
7. Pawlik B.: *The Girth of Cayley graphs of Sylow 2-subgroups of symmetric groups* S_{2^n} *on diagonal bases* (under review).
8. Slupik A.J., Sushchansky V.I.: *Minimal generating sets and Cayley graphs of Sylow p-subgroups of finite symmetric groups.* Algebra Discrete Math. **8**, no. 4 (2009), 167–184.