Algebra and Discrete Mathematics
Volume **21** (2016). Number 2, pp. 264–281 RESEARCH ARTICLE
© Journal "Algebra and Discrete Mathematics"

The action of Sylow 2-subgroups of symmetric groups on the set of bases and the problem of isomorphism of their Cayley graphs

Bartłomiej Pawlik

Communicated by V. I. Sushchansky

Abstract. Base (minimal generating set) of the Sylow 2-subgroup of S_{2^n} is called diagonal if every element of this set acts non-trivially only on one coordinate, and different elements act on different coordinates. The Sylow 2-subgroup $P_n(2)$ of S_{2^n} acts by conjugation on the set of all bases. In presented paper the stabilizer of the set of all diagonal bases in $S_n(2)$ is characterized and the orbits of the action are determined. It is shown that every orbit contains exactly 2^{n-1} diagonal bases and 2^{2^n-2n} bases at all. Recursive construction of Cayley graphs of $P_n(2)$ on diagonal bases ($n \geqslant 2$) is proposed.

Introduction

Let n be a positive integer greater then 1 and let p be a prime. By $P_n(p)$ we denote the Sylow p-subgroup of the symmetric group S_{p^n}. In this paper by *base of a group* we mean a minimal set of generators of this group (whitch further is simply called *a base*).

It is known that

$$P_n(p) \cong \underbrace{C_p \wr C_p \wr \ldots \wr C_p}_{n},$$

2010 MSC: 20B35, 20D20, 20E22, 05C25.

Key words and phrases: Sylow p-subgroup, group base, wreath product of groups, Cayley graphs.

where C_p is a cyclic permutation group of order p. For every finite p-group G the following equality holds:

$$\Phi(G) = G' \cdot G^p,$$

where $\Phi(G)$ is a Frattini subgroup of G (see e.g. [2]). If $G = P_n(p)$ then $G' = G^p$, thus

$$\Phi(P_n(p)) = (P_n(p))'.$$

So

$$P_n(p)/(P_n(p))' \cong \mathbb{Z}_p^n,$$

but $\mathbb{Z}_p^n$ is a vector space over $\mathbb{Z}_p$ and every basis of $\mathbb{Z}_p^n$ over $\mathbb{Z}_p$ induces a base of $P_n(p)$. Thus every base of $P_n(p)$ has exactly n elements. The group $P_n(p)$ acts on the set of bases of $P_n(p)$ by inner automorphisms. The purpose of this article is to investigate orbits of this action and the respective Cayley graphs of $P_n(p)$. We will consider the case $p = 2$, because group $P_n(2)$ is of particular interest. Namely group $P_n(2)$ is the full group of automorphisms of 2-adic rooted tree of height n (see eg. [3]) and the inverse limit of such groups is a group of automorphisms of 2-adic rooted tree, which is widely investigated because of its properties (for the survey, see e.g. [1]). On the other hand, $p = 2$ is also the only case for which considered diagonal bases generate undirected Cayley graphs.

In Section 2 we recall basic facts about Sylow p-subgroups of symmetric groups and the polynomial (Kaluzhnin) representation of such subgroups. Section 3 shows a special type of bases of Sylow 2-subgroups of S_{2^n} called diagonal bases and some of their properties (an exemplary construction of a diagonal base is presented in [5]). Also in this section we present some further investigations of these bases, which lead us to the definition of primal diagonal bases and characterize the orbits of the action of $P_n(2)$ by inner automorphisms on the set of all diagonal bases. In Section 4 we present a recursive algorithm for construction of Cayley graphs of $P_n(2)$ on diagonal bases. In Section 5 we give some examples of Cayley graphs constructed with the proposed algorithm and present two non-isomorphic Cayley graphs of $P_3(n)$.

1. Preliminaries

Let X_i be the vector of variables $x_1, x_2, \ldots, x_i$. Polynomial representation of group $P_n(p)$ (see e.g. [4], [6]) states that every element $f \in P_n(p)$ can be written in form

$$f = [f_1, f_2(X_1), f_3(X_2), \ldots, f_n(X_{n-1})], \tag{1}$$

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 $\mathbb{Z}_p[X_i]/\langle x_1^p - x_1, \ldots, x_i^p - x_i\rangle$. Following the original paper of L. Kaluzhnin ([4]) we call such element f a *tableau.* By $[f]_i$ we denote the i-th coordinate of tableau f and by $f_{(i)}$ we denote the table

$$f_{(i)} = [f_1, f_2(X_1), \ldots, f_i(X_{i-1})] \in P_i(p),$$

where $i \leqslant n$.

For tableaux $f, g \in P_n(p)$, where f has the form (1) and

$$g = [g_1, g_2(X_1), g_3(X_2), \ldots, g_n(X_{n-1})]$$

the product fg has the form

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

and the inverse

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

Let $\mathfrak{B}$ be the set of all bases of $P_n(p)$. $P_n(p)$ acts on the set $\mathfrak{B}$ by conjugation:

$$B^u = \langle u^{-1}B_1u,\ u^{-1}B_2u,\ \ldots,\ u^{-1}B_nu\rangle \tag{2}$$

for all $B = \{B_1, \ldots, B_n\} \in \mathfrak{B}$.

Lemma 1. *The center of group $P_n(p)$ has the form*

$$Z(P_n(p)) = \{[0, \ldots, 0, \alpha] :\ \alpha \in \mathbb{Z}_p\}.$$

Proof. See [4]. □

Proposition 1. *The action (2) of $P_n(p)$ on the set $\mathfrak{B}$ is semi-regular. The length of every orbit of this action is equal to $p^{\frac{p^n-1}{p-1}-1}$.*

Proof. An action of a group G on a set X is semi-regular, iff every orbit of G on X has the same length. Let $B = \{B_1, B_2, \ldots, B_n\}$ be a base of $P_n(p)$. For any $u \in P_n(p)$ we have $B^u = B$ if and only if $u^{-1}B_iu = B_i$ for every $i = 1, \ldots, n$. Since $\langle B_1, \ldots, B_n\rangle = P_n(p)$, it follows that for every

$g \in P_n(2)$, equality $u^{-1}gu = g$ holds if and only if $u \in Z(P_n(2))$. But following Lemma 1:

$$|Z(P_n(p))| = p,$$

hence the length of orbit containing B is equal to $\frac{|P_n(p)|}{p}$. Thus the length of every orbit is the same regardless of the choice of base B. Hence the action (2) is semi-regular. The length of every orbit is equal to

$$\frac{|P_n(p)|}{p} = p^{\frac{p^n-1}{p-1}-1}. \qquad \square$$

2. Diagonal bases of $P_n(2)$

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

2.1. Definitions and basic facts

Let $\overline{x_n}$ be the monomial $x_1 \cdot x_2 \cdot \ldots \cdot x_n$ and let $\overline{x_n}/x_i$ be the monomial $x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n$ for $i = 1, \ldots, n$.

In [6] the authors defined so-called triangular bases of group $P_n(p)$. In the following article we consider a special type of triangular bases, which we call diagonal. However, the notion of diagonal bases can be formulated independently of triangularity.

Definition 1. Base $B = \{B_1, \ldots, B_n\} \in \mathfrak{B}$ is called diagonal if for any i, $1 \leqslant i \leqslant n$, the table B_i is i-th coordinative, i.e. $[B_i]_j = 0$ for $j \neq i$.

It is well known that in every base B of $P_n(2)$ for every i there exists a tableaux $B' \in B$ which contains a monomial $\overline{x_{i-1}}$ on i-th coordinate. Thus, the nonzero coordinates of elements of diagonal base $B = \{B_1, \ldots, B_n\}$ have form $[B_1]_1 = 1$ and $[B_i]_i = b_i(X_{i-1})$, where b_i contains monomial $\overline{x_{i-1}}$ for every $i = 2, \ldots, n$.

Diagonal bases $B = \{B_1, \ldots, B_n\}$ and $C = \{C_1, \ldots, C_n\}$ of $P_n(2)$ are conjugate if there exists element $u \in P_n(2)$ such that $u^{-1}Bu = C$, i.e.

$$u^{-1}B_i u = C_i \tag{3}$$

for every $i = 1, \ldots, n$.

Definition 2. The length $l(m)$ of a nonzero monomial $m = x_{i_1} \ldots x_{i_k}$ is the number of variables of this monomial. We assume that $l(0) = -1$ and $l(1) = 0$. The length of the reduced polynomial is equal to the maximal length of its monomials.

For every polynomials f and g the following inequality holds:

$$l(f+g) \leqslant \max\{l(f), l(g)\}.$$

Definition 3. Reduced polynomial $f_n : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$ is called primal if

$$f_n = \overline{x_{n-1}} + \beta_n(X_{n-1}),$$

where $l(\beta_n) \leqslant n-3$.

Diagonal base $B = \{B_1, \ldots, B_n\}$ is called primal if $[B_n]_n$ is primal polynomial.

Let $\delta(P_n(2))$ and $\delta'(P_n(2))$ be the numbers of different diagonal bases and different primal diagonal bases of $P_n(2)$, respectively.

Theorem 1. *The following equalities holds:*

$$\delta(P_n(2)) = 2^{2^n-(n+1)} \quad \text{and} \quad \delta'(P_n(2)) = 2^{2^n-2n}.$$

Proof. Let $B = \{B_1, \ldots, B_n\}$ be a diagonal base of $P_n(2)$, i.e. every tableau B_i has on i-th coordinate a polynomial of length $i-1$ for $1 \leqslant i \leqslant n$. Every polynomial $[B_i]_i$ contains monomial $\overline{x_{i-1}}$. There are 2^{i-1} monomials on variables $x_1, \ldots, x_{i-1}$. Thus there are $2^{2^{i-1}-1}$ polynomials on $(i-1)$ variables, which length equal to $i-1$. So the number of diagonal bases of $P_n(2)$ is equal to

$$\prod_{i=0}^{n-1} 2^{2^i-1} = 2^{\gamma},$$

where $\gamma = \sum_{i=0}^{n-1}(2^i - 1) = 2^n - (n+1)$.

Let B be a primal diagonal base, i.e. $[B_n]_n$ be the primal polynomial. There are $2^{2^{n-1}-n}$ primal polynomials on $(n-1)$ variables. So the number of different primal diagonal bases of $P_n(2)$ is equal to

$$\left(\prod_{i=0}^{n-2} 2^{2^i-1}\right) \cdot 2^{2^{n-1}-n} = 2^{\gamma'},$$

where $\gamma' = \left(\sum_{i=0}^{n-2}(2^i-1)\right) + 2^{n-1} - n = 2^{n-1} - n + 2^{n-1} - n = 2^n - 2n$. $\square$

2.2. Properties of diagonal bases

Let

$$\Lambda = \{[\lambda_1, \ldots, \lambda_n] : \lambda_i \in \mathbb{Z}_2,\, 1 \leqslant i \leqslant n\}$$

be an maximal elementary abelian 2-subgroup of group $P_n(2)$. For any $\lambda = [\lambda_1, \ldots, \lambda_n] \in \Lambda$ and vector X_{n-1} we denote

$$X_{n-1} + \lambda = (x_1 + \lambda_1, \ldots, x_{n-1} + \lambda_{n-1}).$$

We can define the left and right actions of group Λ on the set of reduced polynomial on $(n-1)$ variables in the following way. For a reduced polynomial $f : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$ and $\lambda = [\lambda_1, \ldots, \lambda_n] \in \Lambda$ let

$$\lambda \star f(X_{n-1}) = f(X_{n-1} + \lambda) + \lambda_n \quad \text{and} \quad f(X_{n-1}) \star \lambda = f(X_{n-1}) + \lambda_n.$$

As we can can see, this actions resemble the multiplication of tables in $P_n(p)$.

Lemma 2. *Let $\lambda = [\lambda_1, \ldots, \lambda_n] \in \Lambda$ and let $f(X_{n-1}) = \overline{x_{n-1}}$. Then*

$$\lambda^{-1} \star f(X_{n-1}) \star \lambda = \overline{x_{n-1}} + \sum_{i=1}^{n-1} \lambda_i (\overline{x_{n-1}}/x_i) + h(X_{n-1}),$$

where h is some reduced polynomial such that $l(h) \leqslant n-3$.

Proof. We have

$$\begin{aligned}
\lambda^{-1} \star f(X_{n-1}) &= (x_1 + \lambda_1)(x_2 + \lambda_2) \ldots (x_{n-1} + \lambda_{n-1}) + \lambda_n \\
&= x_1 x_2 \ldots x_{n-1} + (\lambda_1 x_2 \ldots x_{n-1} + \lambda_2 x_1 x_3 \ldots x_{n-1} + \ldots + \lambda_{n-1} x_1 \ldots x_{n-2}) \\
&\quad + \ldots + \lambda_1 \lambda_2 \ldots \lambda_{n-1} + \lambda_n \\
&= \overline{x_{n-1}} + \sum_{i=1}^{n-1} \lambda_i (\overline{x_{n-1}}/x_i) + h(X_{n-1}) + \lambda_n,
\end{aligned}$$

where h is some reduced polynomial such that $l(h) \leqslant n-3$. Thus

$$\begin{aligned}
\lambda^{-1} \star f(X_{n-1}) \star \lambda &= \overline{x_{n-1}} + \sum_{i=1}^{n-1} \lambda_i (\overline{x_{n-1}}/x_i) + h(X_{n-1}) + \lambda_n + \lambda_n \\
&= \overline{x_{n-1}} + \sum_{i=1}^{n-1} \lambda_i (\overline{x_{n-1}}/x_i) + h(X_{n-1}). \qquad \square
\end{aligned}$$

There is also an important relation between polynomials of maximal length and the primal polynomials.

Lemma 3. *For every reduced polynomial $f : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$ such that $l(f) = n-1$, there exists a tableau $\lambda \in \Lambda$ such that $\lambda^{-1} \star f \star \lambda$ is the primal polynomial.*

Proof. Every polynomial $f(X_{n-1})$ such that $l(f) = n-1$ can be written in the form

$$f(X_{n-1}) = \overline{x_{n-1}} + \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + h(X_{n-1}),$$

where $\alpha_i \in \mathbb{Z}_2$ for $i = 1, \ldots, n-1$ and $l(h) \leqslant n-3$.

Let $f_1(X_{n-1}) = \overline{x_{n-1}}$ and $f_2^{(i)}(X_{n-1}) = \alpha_i(\overline{x_{n-1}}/x_i)$ for every $i = 1, \ldots, n-1$. Then

$$f = f_1 + \sum_{i=1}^{n-1} f_2^{(i)} + h$$

and

$$\lambda^{-1} \star f \star \lambda = \lambda^{-1} \star f_1 \star \lambda + \sum_{i=1}^{n-1} (\lambda^{-1} \star f_2^{(i)} \star \lambda) + \lambda^{-1} \star h \star \lambda. \quad (4)$$

We construct the tableau λ using coefficients α_i from the polynomial f in form $\lambda = [\alpha_1, \ldots, \alpha_{n-1}, u_n]$, where $u_n \in \mathbb{Z}_2$ is fixed. Let us investigate the form of sum (4). From Lemma 2 we have

$$\lambda^{-1} \star f_1(X_{n-1}) \star \lambda = \overline{x_{n-1}} + \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + h'(X_{n-1})$$

where h' is some reduced polynomial such that $l(h') \leqslant n-3$, and

$$\begin{aligned}\lambda^{-1} \star f_2^{(i)}(X_{n-1}) \star \lambda =& \alpha_i(\overline{x_{n-1}}/x_i) \\ &+ \alpha_i \sum_{j=1, j\neq i}^{n-1} \beta_j\big((\overline{x_{n-1}}/x_i)/x_j\big) + \alpha_i k^{(i)}(X_{n-1}),\end{aligned}$$

where $\beta_j \in \mathbb{Z}_2$ and $k^{(i)}$ is some reduced polynomial such that $l(k^{(i)}) \leqslant n-4$. Thus

$$\begin{aligned}&\sum_{i=1}^{n-1} \Big(\lambda^{-1} \star f_2^{(i)}(X_{n-1}) \star \lambda\Big) \\ &\quad = \sum_{i=1}^{n-1} \alpha_i \left(\overline{x_{n-1}}/x_i + \sum_{j=1, j\neq i}^{n-1} \beta_j\big((\overline{x_{n-1}}/x_i)/x_j\big) + k^{(i)}(X_{n-1})\right)\end{aligned}$$

$$= \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + h''(X_{n-1}),$$

where h'' is some reduced polynomial such that $l(h'') \leqslant n-3$.

The last element in sum (4) has the form

$$\lambda^{-1} \star h(X_{n-1}) \star \lambda = h'''_n(X_{n-1}),$$

where h''' is some reduced polynomial such that $l(h''') \leqslant n-3$. Thus finally

$$\begin{aligned}\lambda^{-1} \star f(X_{n-1}) \star \lambda = \overline{x_{n-1}} + \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + h'(X_{n-1}) \\ + \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + h''(X_{n-1}) + h'''(X_{n-1}) \\ = \overline{x_{n-1}} + h'(X_{n-1}) + h''(X_{n-1}) + h'''(X_{n-1}) \\ = \overline{x_{n-1}} + b(X_{n-1}),\end{aligned}$$

where $b = h' + h'' + h'''$ and $l(b) \leqslant n-3$. So $\lambda^{-1} \star f \star \lambda$ is a primal polynomial. □

Theorem 2. *Every*

$$f = [0, 0, \ldots, 0, f_n(X_{n-1})] \in P_n(2)$$

where $l(f_n) = n-1$, *is conjugate to a tableau*

$$b = [0, 0, \ldots, 0, b_n(X_{n-1})],$$

where b_n *is the primal polynomial.*

Proof. Similarly like in the proof of Lemma 3, tableau f can be written in form

$$f = \left[0,\ \ldots,\ 0,\ \overline{x_{n-1}} + \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + h_n(X_{n-1})\right],$$

where $\alpha_i \in \mathbb{Z}_2$ for $i = 1, \ldots, n-1$ and $l(h_n) \leqslant n-3$.

Let us construct the tableau u using coefficients α_i from tableau f. Let $u = [\alpha_1,\ \ldots,\ \alpha_{n-1}, u_n]$, where $u_n \in \mathbb{Z}_2$ is fixed. Notice that $u \in \Lambda$. Of course the equality

$$[u^{-1} f u]_j = 0$$

holds for every $j = 1, \ldots, n-1$. From Lemma 3 we get that $[u^{-1} f u]_n$ is the primal polynomial. □

Let us denote the set of all diagonal bases of $P_n(2)$ by $\mathfrak{D}$. Now we describe stabilizer of the set $\mathfrak{D}$ in the group $P_n(2)$ with respect to the action (2).

Theorem 3. *The stabilizer of the subset $\mathfrak{D} \subset \mathfrak{B}$ in the group $P_n(2)$ acting on the set $\mathfrak{B}$ according to (2) is equal to Λ. The kernel of this action coincide with the center of $P_n(2)$.*

Proof. To show that Λ is the stabilizer of $\mathfrak{D}$ we have to prove the following.

1) If $B = \{B_1, \dots, B_n\}$ is a diagonal base of $P_n(2)$ and $\lambda \in \Lambda$, then $\lambda^{-1} B \lambda$ is a diagonal base of $P_n(2)$.
2) For every diagonal bases $B = \{B_1, \dots, B_n\}$ and $C = \{C_1, \dots, C_n\}$ of $P_n(2)$ if there exists $u \in P_n(2)$ such that $u^{-1} B u = C$, then $u \in \Lambda$.

A set conjugate to a base is always a base. Let $1 \leqslant s \leqslant n$ and let $B_s \in P_n(2)$ be a tableau with the only nonzero element on its s-th coordinate. Let $j \neq s$. Then

$$[\lambda^{-1} B_s \lambda]_j = 0.$$

Thus the first condition is proved.

We now prove the second condition. Let $[B_1]_1 = 1$ and $[B_i]_i = b_i(X_{i-1})$ for $i = 2, \dots, n$. Base B is diagonal, so $b_i(X_{i-1}) \neq 0$ for every $i = 2, \dots, n$. Let

$$u = [\alpha_1, u_2(X_1), \dots, u_n(X_n)].$$

We will show that for every $s = 1, \dots, n-1$, the reduced polynomial u_i for $i = 2, \dots, n$ does not contain variable x_s. Variable x_s can be contained only in polynomials u_i for which $i > s$. Every such polynomial can be described as

$$u_i(X_{i-1}) = u_i'(X_{i-1}) \cdot x_s + u_i''(X_{i-1}),$$

where polynomials u_i' and u_i'' do not contain variable x_s. Equality $u^{-1} B_s u = C_s$ can be written in form $B_s u = u C_s$. Thus

$$[B_s u]_k = [u C_s]_k \tag{5}$$

for every $k = 1, \dots, n$. For $k > s$ we have $[B_s]_k = [C_s]_k = 0$, so in this case

$$\begin{aligned}[B_s u]_k &= 0 + u_i'(X_{i-1}) \cdot (x_s + b_i(X_{i-1})) + u_i''(X_{i-1}) \\ &= u_i'(X_{i-1}) \cdot x_s + u_i'(X_{i-1}) \cdot b_i(X_{i-1}) + u_i''(X_{i-1})\end{aligned}$$

and

$$[u C_s]_k = u_i'(X_{i-1}) \cdot x_s + u_i''(X_{i-1}) + 0 = u_i'(X_{i-1}) \cdot x_s + u_i''(X_{i-1}).$$

Thus

$$[B_s u]_k = [uC_s]_k,$$
$$u_i'(X_{i-1})\, x_s + u_i'(X_{i-1})\, b_i(X_{i-1}) + u_i''(X_{i-1}) = u_i'(X_{i-1})\, x_s + u_i''(X_{i-1}),$$
$$u_i'(X_{i-1})\, b_i(X_{i-1}) = 0.$$

We know that $b_i(X_{i-1}) \neq 0$, so $u_i'(X_{i-1}) = 0$ and hence

$$u_i = 0 \cdot x_s + u_i''(X_{i-1}) = u_i''(X_{i-1}),$$

where u_i'' does not contain variable x_s.

We have shown that any variable x_s for $1 \leqslant s \leqslant n$ is not contained in polynomials u_i for $i = 2, \dots, n$, so $u_i(X_{i-1}) = \alpha_i$, where α_i is constant and hence $u = [\alpha_1, \alpha_2, \dots, \alpha_n] \in \Lambda$. Thus indeed Λ is the stabilizer of σ on $\mathfrak{D}$. Lemma 1 implies that the center of $P_n(2)$ contains only the tableaux $[0, \dots, 0, 0]$ and $[0, \dots, 0, 1]$.

Let

$$b_n(X_{n-1}) = \overline{x_{n-1}} + \sum_{i=1}^{n-1} \alpha_i(\overline{x_{n-1}}/x_i) + \beta_n(X_{n-1}),$$

where β_n is some reduced polynomial such that $l(\beta_n) \leqslant n-3$. Thus

$$b_n(x_1+\lambda_1, \dots, x_{n-1}+\lambda_{n-1}) = \overline{x_{n-1}} + \sum_{i=1}^{n-1}(\alpha_i+\lambda_i)(\overline{x_{n-1}}/x_i) + \overline{\beta_n}(X_{n-1}),$$

where $\overline{\beta_n}$ is a reduced polynomial such that $l(\overline{\beta_n}) \leqslant n-3$. So the necessary condition for the equality $\lambda^{-1}B_n\lambda = B_n$ to hold is

$$\alpha_i = \alpha_i + \lambda_i$$

for all $i = 1, \dots, n-1$. So $\lambda_i = 0$ for all such i. It follows that $\overline{\beta_n} = \beta_n$. Hence

$$\lambda^{-1}B_n\lambda = B_n$$

if and only if $\lambda_1 = \ldots = \lambda_{n-1} = 0$. □

Corollary 1. *If B and C are two conjugated diagonal bases of $P_n(2)$ such that for tableaux $u, v \in \Lambda$ the following equalities hold:*

$$u^{-1}Bu = C \quad \textit{and} \quad v^{-1}Bv = C,$$

then

$$u = v + [0, \dots, 0, \alpha],$$

where $\alpha \in \mathbb{Z}_2$.

2.3. Properties of primal diagonal bases

Let $B = \{B_1, \dots, B_n\}$ be a diagonal base of $P_n(2)$. Theorem 2 implies that tableau B_n is conjugate with some tableau $C_n = [0, \dots, 0, c_n(X_{n-1})]$, where c_n is the primal polynomial. As we could see in the proof of Theorem 2, the tableau u which conjugate tableaux B_n and C_n belongs to the subgroup Λ. Thus, by Theorem 3 we can formulate

Corollary 2. *Every diagonal base of $P_n(2)$ is conjugate to some primal diagonal base.*

Primal diagonal bases have another important property.

Theorem 4. *If B and C are different primal diagonal bases of $P_n(2)$, then B and C are not conjugated.*

Proof. Let us assume that bases

$$B = \{B_1, \dots, B_n\} \quad \text{and} \quad C = \{C_1, \dots, C_n\}$$

are conjugated. Then according to Theorem 3 there exists tableau $u \in \Lambda$ such that

$$u^{-1} B u = C. \tag{6}$$

Let

$$B_n = [0, \dots, 0, \overline{x_{n-1}} + \beta_n(X_{n-1})], \quad \text{where } l(\beta_n) \leqslant n-3,$$

and

$$C_n = [0, \dots, 0, \overline{x_{n-1}} + \gamma_n(X_{n-1})], \quad \text{where } l(\gamma_n) \leqslant n-3.$$

From (6) we get the equality

$$[u^{-1} B_n u]_n = [C_n]_n. \tag{7}$$

By Lemma 2, we have

$$[u^{-1} B_n u]_n = \overline{x_{n-1}} + \sum_{i=1}^{n-1} u_i(\overline{x_{n-1}}/x_i) + h(X_{n-1}),$$

where $l(h) \leqslant n-2$. So equation (7) implies that

$$\overline{x_{n-1}} + \sum_{i=1}^{n-1} u_i(\overline{x_{n-1}}/x_i) + h(X_{n-1}) = \overline{x_{n-1}} + \gamma_n(X_{n-1}).$$

Thus $h(X_{n-1}) = \gamma_n(X_{n-1})$ and $u_i(\overline{x_{n-1}}/x_i) = 0$ for every $i = 1, \dots, n-1$, so $u_i = 0$ for every $i = 1, \dots, n-1$, that is, $u = [0, \dots, 0, u_n]$. But if $u = [0, \dots, 0, u_n]$ then $u^{-1}Bu = B$ and from (6) we get that $B = C$, which contradicts the assumption that B and C are different primal diagonal bases. □

The orbit of $P_n(2)$ on $\mathfrak{B}$ by action (2) which contains a diagonal base is called $\mathfrak{D}$-orbit. Summing up previous results we can formulate following

Theorem 5. *The following statement holds:*

1) *every $\mathfrak{D}$-orbit contains exactly one primal diagonal base;*
2) *every $\mathfrak{D}$-orbit contains exactly 2^{n-1} diagonal bases and 2^{2^n-2} bases at all;*
3) *the number of different $\mathfrak{D}$-orbits is equal to 2^{2^n-2n}.*

Proof. 1) Corollary 2 states that every diagonal base is conjugate with some primal diagonal base. Thus every $\mathfrak{D}$-orbit contains a primal diagonal base. From Theorem 4 we get that this primal diagonal base is unique in every $\mathfrak{D}$-orbit.

2) From Theorem 3 we know that the elements which conjugate diagonal bases are of form $u = [u_1, \dots, u_{n-1}, u_n]$, where $u_i \in \mathbb{Z}_2$ for $i = 1, \dots, n$. Theorem 3 also states that conjugation does not depend on u_n, so the number of conjugated diagonal bases is equal to the number of different tableaux of the form $[u_1, \dots, u_{n-1}, 0]$. There are 2^{n-1} such tableaux. The number of all bases in single $\mathfrak{D}$-orbit is determined by Theorem 1.

3) Every $\mathfrak{D}$-orbit contains exactly one primal diagonal base, so the number of $\mathfrak{D}$-orbits is equal to the number of different primal diagonal bases, which is equal to $2^{2^n} - 2n$ by Theorem 1. □

3. Cayley graphs of $P_n(2)$ on diagonal bases

We recall the definition of Cayley graphs.

Definition 4. Let G be a group and S be a set of generators of G. The Cayley graph of group G on set S is a graph $\mathrm{Cay}(G, S)$ in which vertex set is equal to G and two vertices u, v are connected by an edge iff there exists $s \in S$ such that $u = v \cdot s$. Such edge will be denoted as uv.

If $S = S^{-1}$, then $\mathrm{Cay}(G, S)$ is undirected. Thus Cayley graphs of $P_n(2)$ on diagonal bases are undirected.

From now on in this section we assume that $n > 2$.

Let $B = \{B_1, \ldots, B_n\}$ be a diagonal base of $P_n(2)$. By Theorem 5 base B is in the same orbit with some primal diagonal base $D = \{D_1, \ldots, D_n\}$, so

$$\mathrm{Cay}(P_n(2), B) \cong \mathrm{Cay}(P_n(2), D).$$

Thus investigation of Cayley graphs of $P_2(n)$ on diagonal bases is equivalent with investigation of Cayley graphs only on primal diagonal bases.

Let $B' = \{(B_1)_{(n-1)}, \ldots, (B_{n-1})_{(n-1)}\}$. Set B' is a diagonal base of group $P_{n-1}(2)$.

Theorem 6. *Let $D = \{D_1, \ldots, D_{n-1}, D_n\}$ be a diagonal base of $P_n(2)$ and let $D' = \{(D_1)_{(n-1)}, \ldots, (D_{n-1})_{(n-1)}\}$ be a diagonal base of $P_{n-1}(2)$. Let Γ be a graph obtained from $\mathrm{Cay}(P_n(2), D)$ by removing edges of form uD_n for every $u \in P_n(2)$. Then*

1) *Γ is not connected;*
2) *Γ contains $2^{2^{n-1}}$ connected components;*
3) *every connected component of Γ is isomorphic to the Cayley graph $\mathrm{Cay}(P_{n-1}(2), D')$.*

Proof. Let $(D_{j_1}, D_{j_2}, \ldots, D_{j_l})$ be a tuple of (not necessarily different) elements of $D \backslash \{D_n\}$, i.e. $D_{j_k} \in \{D_1, \ldots, D_{n-1}\}$ for every $k = 1, \ldots, l$. Thus

$$\left[\prod_{k=1}^{l} D_{i_k}\right]_n = 0. \tag{8}$$

We now prove stated properties.

1) Consider vertices $f_1 = [0, \ldots, 0]$ and $f_2 = [0, \ldots, 0, 1]$ of graph Γ. Equality (8) implies that

$$\left[f_1 \cdot \prod_{k=1}^{l} D_{i_k}\right]_n = 0.$$

Thus in Γ there is no path from vertex f_1 to vertex f_2, which implies that Γ is not connected.

2) Let $f = [0, \ldots, 0, f_n(X_{n-1})]$. Equality (8) implies that

$$\left[f \cdot \prod_{k=1}^{l} D_{i_k}\right]_n = f_n(X_{n-1}).$$

Thus if $g = [0, \ldots, 0, g_n(X_{n-1})]$ and $g_n \neq f_n$, then vertices f and g are contained in different connected components of Γ.

Let f' be a tableau for which $[f']_n = [f]_n$. Set D' is a base of $P_{n-1}(2)$, and there exists a set $\{D_{j_1}, D_{j_2}, \ldots, D_{j_l}\}$ of elements of $D \backslash \{D_n\}$ such that

$$f' \cdot \prod_{k=1}^{l} D_{i_k} = f.$$

Thus every vertex

$$f' = [f_1, \ldots, f_n(X_{n-1})]$$

of Γ is contained in the same connected component of Γ as vertices of the form

$$[0, \ldots, 0, f_n(X_{n-1})], \tag{9}$$

and different vertices of form (9) lays in different connected components of Γ, so the number of connected component of Γ is equal to the number of different reduced polynomials $f_n : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$, which is equal to $2^{2^{n-1}}$.

3) We have shown that every connected component of Γ contains a vertex made of tableaux with fixed last coordinate. Let V_{f_n} be the subgroup of $P_n(2)$ such that if $g \in V_{f_n}$ iff $[g_n] = f_n$. Thus $V_{f_n} \cong P_{n-1}(2)$, hence

$$\mathrm{Cay}(V_{f_n}, D') \cong \mathrm{Cay}(P_{n-1}(2), D'). \qquad \square$$

Theorem 6 implies the recurrent construction of Cayley graphs of $P_n(2)$ on primal diagonal bases. Let $D = \{D_1, \ldots, D_n\}$ be a primal diagonal base of $P_n(2)$. Graph $\mathrm{Cay}(P_n(2), D)$ can be constructed in following way.

1) We construct $2^{2^{n-1}}$ Cayley graphs $\mathrm{Cay}(P_{n-1}(2), D')$, where

$$D' = \{(D_1)_{(n-1)}, \ldots, (D_{n-1})_{(n-1)}\}.$$

Every such Cayley graph may be labeled with a different reduced polynomial $f_n : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$. Denote the Cayley graph corresponding to polynomial f_n by Cay_{f_n}.

2) In every graph Cay_{f_n} we replace the set of vertices $V(\mathrm{Cay}_{f_n}) = P_{n-1}(2)$ by the set of vertices $V' \subset P_n(2)$ in following way: we replace $u = [u_1, \ldots, u_{n-1}(X_{n-2})]$ by

$$u' = [u_1, \ldots, u_{n-1}(X_{n-2}), f_n(X_{n-1})]$$

for every $u \in V(\mathrm{Cay}_{f_n})$.

3) For every pair of vertices u', v' of obtained graph, if $u'B_n = v'$, then we add an edge $u'v'$.

So in the construction we need to start with the case $n = 2$, which is presented in the next section.

Above construction suggests the dependence between Cayley graphs and Schreier coset graphs on diagonal bases of $P_n(2)$.

Let us recall the definition of the latter graphs.

Definition 5. Let G be a group, S be a set of generators of G and H be a subgroup of finite index in G. The Schreier coset graph $\mathrm{Sch}(G, S, H)$ is a graph whose vertices are the right cosets of H in G and two vertices Hu and Hv are connected by an edge iff there exists $s \in S$ such that $Hu = Hv \cdot s$.

Let us notice that every Cayley graph of group G is a Schreier coset graph of G in which H is a trivial subgroup.

We consider a subgroup $\overline{P}_n(2)$ of group $P_n(2)$ in which in every tableuax the last coordinate is equal to 0, i.e. if $f \in \overline{P}_n(2)$,then

$$f = [f_1, f_2(X_1), \ldots, f_{n-1}(X_{n-2}), 0].$$

Of course $\overline{P}_n(2) \cong P_{n-1}(2)$.

Theorem 7. *Let $D = \{D_1, \ldots, D_n\}$ be a diagonal base of $P_n(2)$. Then the following conditions hold.*

1) *Two vertices $\overline{P}_n(2)u$ and $\overline{P}_n(2)v$ of graph $\mathrm{Sch}(P_n(2), D, \overline{P}_n(2))$ are connected by an edge, iff*

$$\overline{P}_n(2)u = \overline{P}_n(2)v \cdot D_n.$$

2) *Graph $\mathrm{Sch}(P_n(2), D, \overline{P}_n(2))$ is bipartite.*

Proof. If $i = 1, \ldots, n-1$, then $[D_i]_n = 0$. Thus in this case

$$\overline{P}_n(2)u \cdot D_i = \overline{P}_n(2)u,$$

so elements $D_1, \ldots, D_{n-1}$ do not generate edges of $\mathrm{Sch}(P_n(2), D, \overline{P}_n(2))$.

We now prove the second statement.

Vertex set $V(\mathrm{Sch})$ can be described as a sum of sets V_1 and V_2, where V_1 is made of cosets in which the last coordinate in all tableaux in this coset is a polynomial which contains a monomial $\overline{x_{n-1}}$ and V_2 is made of cosets in which the last coordinate in all tableaux are polynomials which do not contain such a monomial. $[D_n]_n$ contains a monomial $\overline{x_{n-1}}$, thus for every $\overline{P}_n(2)v_1 \in V_1$ and $\overline{P}_n(2)v_2 \in V_2$:

$$\overline{P}_n(2)v_1 \cdot D_n \in V_2 \text{ and } \overline{P}_n(2)v_2 \cdot D_n \in V_1. \qquad \square$$

Hence for diagonal base $D = \{D_1, \dots, D_n\}$ we can obtain a Cayley graph $\mathrm{Cay}(P_n(2))$ from a graph $\mathrm{Sch}(P_n(2), D, \overline{P}_n(2))$ by replacing every vertex of $\mathrm{Sch}(P_n(2), D, \overline{P}_n(2))$ by a graph $\mathrm{Cay}(P_{n-1}(2), D')$ and replacing every edge of $\mathrm{Sch}(P_n(2), D, \overline{P}_n(2))$ by a set of corresponding edges between elements $P_n(2)$ due to generator D_n (see point 3 of above construction).

4. Cayley graphs of $P_n(2)$ for small n

4.1. The case $n = 2$

Group $P_2(2)$ is isomorphic with the dihedral group D_4. It has two different diagonal bases and 12 different bases at all. The list of bases is as follows:

$$\begin{aligned} B_1 = D_1 &= \{[1,0],[0,x_1]\}, & B_2 = D_2 &= \{[1,0],[0,x_1+1]\},\\ B_3 &= \{[1,1],[0,x_1]\}, & B_4 &= \{[1,1],[0,x_1+1]\},\\ B_5 &= \{[1,0],[1,x_1]\}, & B_6 &= \{[1,0],[1,x_1+1]\},\\ B_7 &= \{[1,1],[1,x_1]\}, & B_8 &= \{[1,1],[1,x_1+1]\},\\ B_9 &= \{[0,x_1],[1,x_1]\}, & B_{10} &= \{[0,x_1],[1,x_1+1]\},\\ B_{11} &= \{[0,x_1+1],[1,x_1]\}, & B_{12} &= \{[0,x_1+1],[1,x_1+1]\}. \end{aligned}$$

The only primal diagonal base in $P_n(2)$ is B_1. The action on the set of all bases has 3 different orbits of length 4:

$$O_1 = \{D_1, D_2, B_3, B_4\}, \qquad O_2 = \{B_5, B_6, B_7, B_8\},$$
$$O_3 = \{B_9, B_{10}, B_{11}, B_{12}\}.$$

The orbit O_1 is the only $\mathfrak{D}$-orbit. Cayley graphs of $P_2(2)$ on bases from O_2 and O_3 are isomorphic (Fig. 1).

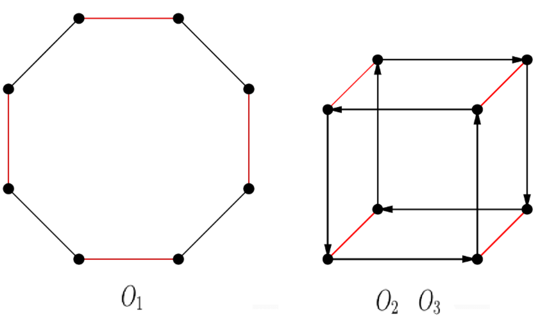

Figure 1. Cayley graphs of $P_2(2)$ in bases from respective orbits.

4.2. The case $n = 3$

There are four different primal diagonal bases of $P_3(2)$:

$$\begin{aligned}
D_1 &= \{[1,0,0],\ [0,x_1,0],\ [0,0,x_1x_2]\},\\
D_2 &= \{[1,0,0],\ [0,x_1,0],\ [0,0,x_1x_2+1]\},\\
D_3 &= \{[1,0,0],\ [0,x_1+1,0],\ [0,0,x_1x_2]\},\\
D_4 &= \{[1,0,0],\ [0,x_1+1,0],\ [0,0,x_1x_2+1]\},
\end{aligned}$$

Thus there are four different $\mathfrak{D}$-orbits and every such orbit contains exactly four diagonal bases and exactly 60 bases, which are not diagonal. Schreier coset graph $\mathrm{Sch}(P_3(2), D, \overline{P}_3(2))$ on bases from orbits $\mathfrak{D}$-orbits have form presented in Figure 2.

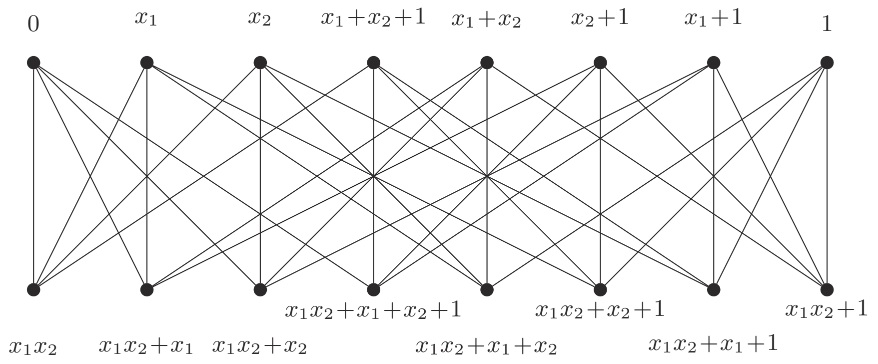

Figure 2. $\mathrm{Sch}(P_3(2), D, \overline{P}_3(2))$, where D is a diagonal base (vertex indexed by polynomials on last coordinate).

As we can see, $\mathrm{Sch}(P_3(2), D, \overline{P}_3(2))$ is a 4-regular bipartite graph. Every edge of this graph corresponds to connections with subgraphs isomorphic to $\mathrm{Cay}(P_2(2), D')$ (i.e. undirected cycle on 8 vertices, see 5.1). Every such connected cycles in $\mathrm{Cay}(P_3(2), D)$ are connected by two edges and form of connection depends of bases (Fig. 3)

Thus the length of the shortest cycle in graphs on bases D_1 and D_2 is equal to 8, and length of the shortest cycle in graphs on bases D_3 and D_4 is equal to 4. This means that these Cayley graphs of $P_3(2)$ on diagonal bases are not isomorphic.

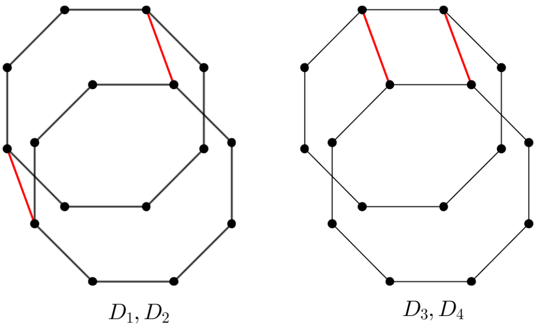

Figure 3. Connections between subgraphs of $\mathrm{Cay}(P_3(2), D)$ isomorphic with $\mathrm{Cay}(P_2(2), D')$ for different diagonal bases.

References

[1] A. Bier, V. Sushchansky *Kaluzhnin's representations of Sylow p-subgroups of automorphism groups of p-adic rooted trees* Algebra Discrete Math., 19:1 (2015), 19-38.

[2] D. Gorenstein, *Finite Groups*, Harper's series in modern mathematics, Now York, Harper & Row, 1968.

[3] R. I. Grigorchuk, V. V. Nekrashevych, V. I. Sushchanskii, *Automata, Dynamical Systems, and Groups*, Proc. Steklov Inst. Math. v.231 (2000), 134-214

[4] L. Kaluzhnin, *La structure des p-groupes de Sylow des groupes symetriques finis*, Ann. Sci. l'Ecole Norm. Sup. 65 (1948), 239–272.

[5] B. Pawlik, *Involutive bases of Sylow 2-subgroups of symmetric and alternating groups*, Zesz. Nauk. Pol. Sl., Mat. Stos. 5 (2015), 35–42.

[6] V. Sushchansky, A. Słupik, *Minimal generating sets and Cayley graphs of Sylow p-subgroups of finite symmetric groups*, Algebra Discrete Math., no. 4, (2009), 167–184.

Contact information

B. Pawlik

Institute of Mathematics
Silesian University of Technology
ul. Kaszubska 23, 44-100 Gliwice, Poland
E-Mail(s): `bartlomiej.pawlik@polsl.pl`

Received by the editors: 10.04.2016
and in final form 30.05.2016.