Алгебра и анализ
Том 29 (2017), № 4

St. Petersburg Math. J.
Vol. 29 (2018), No. 4, Pages 575–580
http://dx.doi.org/10.1090/spmj/1507
Article electronically published on June 1, 2018

# A FAMILY OF PERMUTATION GROUPS WITH EXPONENTIALLY MANY NONCONJUGATED REGULAR ELEMENTARY ABELIAN SUBGROUPS

S. EVDOKIMOV, M. MUZYCHUK, AND I. PONOMARENKO

Abstract. Given a prime $p$, a permutation group is constructed that contains at least $p^{p-2}$ nonconjugated regular elementary Abelian subgroups of order $p^3$. This gives the first example of a permutation group with exponentially many nonconjugated regular subgroups.

## §1. Introduction

A transitive permutation group is said to be *regular* if the one-point stabilizer of it is trivial. Regular subgroups of permutation groups arise in many natural contexts, for example, in group factorizations [4], Schur rings [6], Cayley graphs [1], etc. In the present paper, given a group $H$ and a permutation group $\Gamma$, we are interested in the number

(1)
$$b_H(\Gamma) := |\operatorname{Orb}(\Gamma, \operatorname{Reg}(\Gamma, H))|$$

of orbits in the action of $\Gamma$ by conjugation on the set $\operatorname{Reg}(\Gamma, H)$ of all its regular subgroups isomorphic to $H$. Using terminology and arguments of [1], one can see that if $\Gamma$ is the automorphism group of an object of a concrete category $\mathcal{C}$, then $b_H(\Gamma)$ equals the number of pairwise nonequivalent representations of this object as a Cayley object over $H$ in $\mathcal{C}$. As $\mathcal{C}$ one can take, for example, the category of finite graphs or other combinatorial structures.

Let $H$ be a cyclic group. Then, obviously, $b_H(\Gamma)$ is bounded from above by number $c(\Gamma)$ of the conjugacy classes of full cycles contained in $\Gamma$. It was proved in [5] that the latter number does not exceed $n = |H|$.[1] Thus, in this case $b_H(\Gamma) \leq n$.

The simplest noncyclic case appears when $H$ is an elementary Abelian group $E_{p^2}$. Here, $b_H(\Gamma) \leq b_H(P)$ by the Sylow theorem, where $P$ is a Sylow $p$-subgroup of the group $\Gamma$. To estimate $b_H(P)$, without loss of generality we may assume that $P$ is a transitive $p$-group of degree $p^2$ the action of which on some imprimitivity system induces a regular (cyclic) group of order $p$, i.e., $P$ belongs to the class defined in the same way as the class $\mathcal{E}_p$ in Theorem 1.1 below with $p^3$ replaced by $p^2$. With the help of the technique developed in §2, we can describe the set $\operatorname{Reg}(\Gamma, H)$ (cf. Theorem 2.2 and Lemma 2.4). Then applying [2, Theorem 6.1], one can prove that $b_H(P) \leq p$. Thus, in this case we also have $b_H(\Gamma) \leq n$.

2010 *Mathematics Subject Classification.* Primary 20B05.
*Key words and phrases.* Permutation group, regular subgroup, polynomial over finite field.
The first author, S. Evdokimov, is deceased.
[1]More exactly, under the Classification of Finite Simple Groups, $c(\Gamma) \leq \varphi(n)$, where $\varphi$ is the Euler function, ibid.

In the above two cases, the number $b_H(\Gamma)$ does not exceed $n$ for all $\Gamma$. The main result of the present paper (Theorem 1.1) shows that in the general case, neither this bound, nor even substantially weaker bounds are valid.

**Theorem 1.1.** *Let $H = E_{p^3}$, where $p$ is a prime. Denote by $\mathcal{E}_p$ the class of all transitive $p$-groups of degree $p^3$ the action of which on some imprimitivity system induces a regular group isomorphic to $E_{p^2}$. Then there exists a group $\Gamma \in \mathcal{E}_p$ such that $b_H(\Gamma) \geq p^{p-2}$.*

From Theorem 1.1, it follows that there is no function $f$ for which the inequality $b_H(\Gamma) \leq n^{f(r)}$ holds true for all Abelian groups $H$ of rank at most $r$ and all permutation groups $\Gamma$ of degree $n$. It would be interesting to find an invariant $t = t(\Gamma)$ such that

$$b_H(\Gamma) \leq n^{f(r,t)}$$

for a function $f$ of $r$ and $t$; for instance, one can try to take $t = t(\Gamma)$ to be the minimal positive integer $t'$ for which the group $\Gamma$ is $t'$-closed as a permutation group in the sense of [7][2].

The proof of Theorem 1.1 is given in §3. It is based on a representation of the groups belonging to the class $\mathcal{E}_p$ with the help of two-variable polynomials over the field $\mathbb{F}_p$. The details are presented in §2. It is of interest to note that the stabilizer of the imprimitivity system in every group $\Gamma \subset \mathcal{E}_p$ is, up to language, a Generalized Reed–Muller code [3].

**Notation.** As usual, $\mathbb{F}_p$ and $\mathrm{Sym}(V)$ denote the field of order $p$ and the symmetric group on the set $V$. An elementary Abelian $p$-group of order $p^n$ is denoted by $E_{p^n}$.

## §2. Permutation groups and polynomials

Let $p$ be a prime. Denote by $R_p$ the factor ring of the polynomial ring $\mathbb{F}_p[X,Y]$ modulo the ideal generated by the polynomials $X^p - 1$ and $Y^p - 1$. The images of the variables $X$ and $Y$ are denoted by $x$ and $y$, respectively. Denote by $V$ the disjoint union of the one-dimensional subspaces

$$V_{i,j} = \{\alpha x^i y^j \,:\, \alpha \in \mathbb{F}_p\}, \quad i,j = 0,\dots,p-1,$$

of the ring $R_p$ viewed as a linear space over $\mathbb{F}_p$.

Every element $f = \sum_{i,j} \alpha_{i,j} x^i y^j$ of $R_p$ yields a permutation

$$\sigma_f \colon \alpha x^i y^j \mapsto (\alpha + \alpha_{i,j}) x^i y^j$$

of the set $V$. This produces a permutation group on $V$ with $p^2$ orbits $V_{i,j}$ that is isomorphic to the additive group of the ring $R_p$. For a subgroup $I$ of the latter group, the corresponding subgroup of $\mathrm{Sym}(V)$ is denoted by $\Delta(I)$. Also, we define two commuting permutations

$$\tau_x \colon \alpha x^i y^j \mapsto \alpha x^{i+1} y^j, \quad \tau_y \colon \alpha x^i y^j \mapsto \alpha x^i y^{j+1}.$$

Clearly, each of them commutes with the permutation $s = \sigma_{f_0}$, where $f_0 = \sum_{i,j} x^i y^j$. The following statement is straightforward.

**Lemma 2.1.** *In the above notation, we have*

(1) $\tau_x^{-1} \sigma_f \tau_x = \sigma_{fx}$ *and* $\tau_y^{-1} \sigma_f \tau_y = \sigma_{fy}$ *for all* $f \in R_p$,

(2) $G_0 := \langle s, \tau_x, \tau_y \rangle$ *is a regular group on* $V$ *isomorphic to* $E_{p^3}$.

Set $\Gamma(I)$ to be the group generated by $\Delta(I)$ and $\tau_x, \tau_y$. If $I$ is an ideal of $R_p$, then, by statement (1) of Lemma 2.1,

$$\Delta(I) \trianglelefteq \Gamma(I) \quad \text{and} \quad \Gamma(I)/\Delta(I) \cong E_{p^2}. \tag{2}$$

If $I$ is not an ideal, then $\Gamma(I) = \Gamma(I')$, where $I'$ is the ideal of $R_p$ generated by $I$.

[2]Here for groups $\Gamma \in \mathcal{E}_p$, the upper bound in inequality (8) could be useful.

**Theorem 2.2.** *Let $p$ be a prime. Then*

(1) *for every ideal $I \neq 0$ of the ring $R_p$, the group $\Gamma(I)$ belongs to the class $\mathcal{E}_p$,*
(2) *every group $\Gamma \in \mathcal{E}_p$ with $b_H(\Gamma) > 0$ is permutation isomorphic to the group $\Gamma(I)$ for some ideal $I$ of $R_p$.*

*Proof.* To prove statement (1), let $I \neq 0$ be an ideal of $R_p$. Then at least one of the sets $V_{i,j}$ is an orbit of the group $\Delta(I)$. Since $\tau_x$ and $\tau_y$ commute, the group $\langle \tau_x, \tau_y \rangle$ acts regularly on the set $S = \{V_{i,j} \,:\, i,j = 0,\dots,p-1\}$. This implies that the group $\Gamma(I)$ is transitive and $S$ is an imprimitivity system of it. The action of $\Gamma(I)$ on this system induces a regular group isomorphic to $E_{p^2}$ that is generated by the images of $\tau_x$ and $\tau_y$ with respect to this action. Thus, $\Gamma(I) \in \mathcal{E}_p$.

Let $\Gamma \in \mathcal{E}_p$. Then $\Gamma$ is a transitive $p$-group of degree $p^3$, the action of which on some imprimitivity system $S'$ induces a regular group isomorphic to $E_{p^2}$. Without loss of generality, we may assume that $\Gamma \leq \mathrm{Sym}(V)$ with $V$ as above. Furthermore, since $b_H(\Gamma) > 0$, the group $\Gamma$ contains a regular subgroup $G'$ isomorphic to $H = E_{p^3}$. Choose an element $s' \in G'$ such that $\mathrm{Orb}(\langle s' \rangle, V) = S'$. Then there exists a group isomorphism

$$\varphi\colon G' \to G_0$$

taking $s'$ to $s$ (see statement (2) of Lemma 2.1). Since $\varphi$ is induced by a permutation of $V$, we may assume that $S' = S$ and $G_0 \in \mathrm{Reg}(\Gamma, E_{p^3})$. Note that the permutation $s$ belongs to the stabilizer $\Delta$ of the blocks $V_{i,j}$ in $\Gamma$. Therefore, $\mathrm{Orb}(\Delta, V) = S$. Since the restriction of $\Delta$ to $V_{i,j}$ is a $p$-group of degree $p$ that contains the restriction of $s$ to $V_{i,j}$ for all $i,j$, this implies that

$$\Delta \leq \Delta(R_p).$$

It follows that $\Delta = \Delta(I)$ for a subgroup $I$ of $R_p$. Taking into account that $\Delta$ is normalized by $\tau_x$ and $\tau_y$, we conclude that $I$ is an ideal of $R_p$ by statement (1) of Lemma 2.1. $\square$

Any maximal element in the class $\mathcal{E}_p$ is permutation isomorphic to the (imprimitive) wreath product of regular groups isomorphic to $E_p$ and $E_{p^2}$. One of these maximal elements equals the group $\Gamma_p := \Gamma(R_p)$; set also $\Delta_p = \Delta(R_p)$. We need two auxiliary lemmas.

**Lemma 2.3.** *Let $g,h \in R_p$. Then the order of the permutation $t_{g,x} = \sigma_g \tau_x$ (respectively, $t_{h,y} = \sigma_h \tau_y$) equals $p$ if and only if $g \in aR_p$ (respectively, $h \in bR_p$), where $a = x-1$ and $b = y-1$.*

*Proof.* Let $g = \sum_{i,j} \alpha_{i,j} x^i y^j$, and let $v = \alpha x^i v^j$ be a point of $V$. Then by the definition of $t_{g,x}$, we have

$$v^{t_{g,x}} = (\alpha + \alpha_{i,j}) x^{i+1} y^j.$$

This implies that the order of $t_{g,x}$ equals $p$ if and only if the following condition is satisfied:

$$\sum_{i=0}^{p-1} \alpha_{i,j} = 0, \quad j = 0,\dots,p-1. \tag{3}$$

Note that this is always true whenever $g \in aR_p$. Conversely, suppose that relations (3) are fulfilled for some $g \in R_p$. Then

$$\alpha_{0,j} = \alpha'_{1,j} - \alpha'_{0,j}, \dots, \alpha_{p-1,j} = \alpha'_{0,j} - \alpha'_{p-1,j},$$

where $\alpha'_{i,j} = \sum_{k=0}^{i-1} \alpha_{k,j}$ for all $i,j$. It follows that $g = ag'$ with $g' = \sum_{i,j} \alpha'_{i,j} x^i y^j$. This completes the proof of the first statement. The second statement (on the order of $t_{h,y}$) is proved similarly. $\square$

**Lemma 2.4.** *A permutation group $G$ belongs to the set* $\mathrm{Reg}(\Gamma_p, E_{p^3})$ *if and only if there exist elements $g \in aR_p$ and $h \in bR_p$ such that*

$$G = \langle s, t_{g,x}, t_{h,y} \rangle \quad \textit{and} \quad ah = bg. \tag{4}$$

*Proof.* To prove the "only if" part, suppose that $G \in \mathrm{Reg}(\Gamma_p, E_{p^3})$. Then $G$ is a self-centralizing subgroup of $\mathrm{Sym}(V)$. On the other hand, the centralizer of $G$ in $\mathrm{Sym}(V)$ contains the central element $s$ of the group $\Gamma_p$. Thus, $s \in G$. The other two generators of $G$ can obviously be chosen so that their images with respect to the epimorphism $\Gamma_p \to \Gamma_p/\Delta_p$ coincide with $x$ and $y$. By Lemma 2.3, this implies that there exist $g \in aR_p$ and $h \in bR_p$ for which the first identity in (4) holds true. Next, since the group $G$ is Abelian, the definition of $t_{g,x}$ and $t_{h,y}$ implies that

$$\sigma_g \tau_x \, \sigma_h \tau_y = t_{g,x} t_{h,y} = t_{h,y} t_{g,x} = \sigma_h \tau_y \, \sigma_g \tau_x.$$

Each of the permutations on the left- and right-hand sides takes the point $\alpha x^i y^j \in V_{i,j}$ to a certain point $\alpha' x^{i+1} y^{j+1} \in V_{i+1,j+1}$. Calculating the images of the former point with respect to them, we obtain

$$\alpha + g_{i,j} + h_{i+1,j} = \alpha' = \alpha + h_{i,j} + g_{i,j+1}$$

or equivalently, $h_{i+1,j} - h_{i,j} = g_{i,j+1} - g_{i,j}$ for all $i, j$. Therefore, $ah = xh - h = yg - g = bg$, as required.

Conversely, let $G$ be the group defined by relations (4). Then the above argument shows that the permutations $s$, $t_{g,x}$, and $t_{h,y}$ pairwise commute. Therefore, the group $G$ is Abelian. Moreover, the definition of $s$ and Lemma 2.3 imply that $G$ is elementary Abelian and transitive. Thus, $G \in \mathrm{Reg}(\Gamma_p, E_{p^3})$, as required. □

## §3. Proof of Theorem 1.1

By statement (1) of Theorem 2.2, we may restrict ourselves to looking for a group $\Gamma$ of the form $\Gamma(I)$, where $I$ is an ideal of the ring $R_p$.

For every integer $k \geq 0$, set

$$I_k = \mathrm{span}_{\mathbb{F}_p}\{a^i b^j \; : \; i + j \geq k\},$$

where the elements $a$ and $b$ are as in Lemma 2.4. Clearly, $I_k$ is an ideal of $R_p$, and $I_{k+1} \subseteq I_k$ for all $k$, and also $I_k = 0$ for $k > 2(p-1)$. Below, the kernels of the mappings $I_k \to aI_k$ and $I_k \to bI_k$ induced by the multiplication by $a$ and $b$ are denoted by $A_k$ and $B_k$, respectively.

**Lemma 3.1.** *Suppose that $p \leq k \leq 2(p-1)$. Then*

(1) $\dim(I_k) = \binom{2p-k}{2}$,
(2) $aI_k = bI_k = I_{k+1}$,
(3) $\dim(A_k) = \dim(B_k) = 2p - k - 1$.

*Proof.* The leading monomials of the polynomials

$$(x-1)^i (y-1)^j, \quad 0 \leq i, j \leq p-1,$$

are obviously linearly independent. Therefore, the polynomials $a^i b^j$ with $i + j \geq k$ form a linear basis of the ideal $I_k$. This immediately proves statement (1). To prove statement (2), we note that, obviously, $aI_k \subseteq I_{k+1}$. Conversely, let $c \in I_{k+1}$. Since $k \geq p$, we have $c = abu$ for some $u \in I_{k-1}$, which proves the reverse inclusion. The rest of statement (2) is proved similarly. Finally, statement (3) follows, because the linear space $A_k$ (respectively, $B_k$) is spanned by the monomials $a^{p-1} b^i$ (respectively, $a^i b^{p-1}$) with $k - p + 1 \leq i \leq p - 1$. □

In what follows, for a subgroup $G$ of a group $\Gamma$ we denote by $G^\Gamma$ the set of all $\Gamma$-conjugates of $G$.

**Lemma 3.2.** *Let $\Gamma_{k,p} = \Gamma(I_k)$, where $k$ is as in Lemma 3.1. Then*

(1) $|\Gamma_{k,p}| = p^{2+\dim(I_k)}$,

(2) $|\operatorname{Reg}(\Gamma_{k,p}, E_{p^3})| = p^{\dim(A_k)+\dim(B_k)+\dim(I_{k+1})-2}$,

(3) $p^{\dim(I_k)-4} \le |G^{\Gamma_{k,p}}| \le p^{\dim(I_k)-1}$ *for all* $G \in \operatorname{Reg}(\Gamma_{k,p}, E_{p^3})$.

*Proof.* Obviously, $|\Delta(I_k)| = p^{\dim(I_k)}$. Therefore, statement (1) follows from the right-hand side of formula (2). Next, from Lemma 2.4 it follows that

$$\operatorname{Reg}(\Gamma_{k,p}, E_{p^3}) = \{G_{g,h} \,:\, (g,h) \in M\},$$

where $G_{g,h} = \langle s, t_{g,x}, t_{h,y}\rangle$ and

$$M = \{(g,h) \in (I_k \cap aR_p) \times (I_k \cap bR_p) \,:\, ah = bg\}. \tag{5}$$

However, $I_k \cap aR_p = I_k \cap bR_p = I_k$, because $k \ge p$. So by statement (2) of Lemma 3.1, the element $ah = bg$ runs over the ideal $I_{k+1}$, whenever $(g,h)$ runs over the set $M$. By the definition of $A_k$ and $B_k$, this implies that

$$|M| = p^{\dim(A_k)+\dim(B_k)+\dim(I_{k+1})}.$$

Thus, to complete the proof of statement (2), it suffices to verify that $G_{g,h} = G_{g',h'}$ if and only if $t_{g,x} = s^i t_{g',x}$ and $t_{h,y} = s^j t_{h',y}$ for some $0 \le i,j \le p-1$. However, this is true, because $G_{g,h} = G_{g',h'}$ if and only if $\varphi(G_{g,h}) = \varphi(G_{g',h'})$, where $\varphi$ is the quotient epimorphism of $\Gamma_{k,p}$ modulo the group $\langle s\rangle$.

To prove statement (3), we note that, by statement (1),

$$|G^\Gamma| = \frac{|\Gamma|}{|N|} = \frac{p^{2+\dim(I_k)}}{|C|\cdot|N/C|}, \tag{6}$$

where $\Gamma = \Gamma_{k,p}$, and $N$ and $C$ are, respectively, the normalizer and centralizer of $G$ in $\Gamma$. Since $G$ is a regular elementary Abelian group and the quotient $N/C$ is isomorphic to a subgroup of a Sylow $p$-subgroup $P$ of the group $\operatorname{Aut}(G) \cong \mathrm{GL}(3,p)$ (here we use the fact that $\Gamma$ is a $p$-group), we conclude that

$$|C| = |G| = p^3 \quad \text{and} \quad 1 \le |N/C| \le |P|.$$

However, $|P| = p^3$. Thus, statement (3) follows from formula (6). □

To complete the proof of Theorem 1.1, we note that $\operatorname{Reg}(\Gamma_k, E_{p^3})$ is the disjoint union of distinct sets $G^{\Gamma_k}$, where $\Gamma_k = \Gamma_{k,p}$ as in Lemma 3.2 and $G \in \operatorname{Reg}(\Gamma_k, E_{p^3})$. Therefore, setting $m_k$ and $M_k$ to be, respectively, the minimum and maximum of the numbers $|G^{\Gamma_k}|$, we obtain

$$\frac{|\operatorname{Reg}(\Gamma_k, E_{p^3})|}{m_k} \ge b_H(\Gamma_k) \ge \frac{|\operatorname{Reg}(\Gamma_k, E_{p^3})|}{M_k}. \tag{7}$$

However, by statement (3) of Lemma 3.2, $m_k \ge p^{\dim(I_k)-4}$ and $M_k \le p^{\dim(I_k)-1}$. By statement (2) of Lemma 3.2, this implies that

$$\frac{|\operatorname{Reg}(\Gamma_k, E_{p^3})|}{m_k} \le p^{d+2} \quad \text{and} \quad \frac{|\operatorname{Reg}(\Gamma_k, E_{p^3})|}{M_k} \ge p^{d-1},$$

where $d = \dim(A_k)+\dim(B_k)+\dim(I_{k+1})-\dim I_k$. Moreover, by statements (1) and (3) of Lemma 3.1, we have $d = 2p-k-1$. Thus,

$$p^{2p-k+1} \ge b_H(\Gamma_k) \ge p^{2p-k-2}. \tag{8}$$

This lower bound for $b_H(\Gamma_k)$ with $k = p-1$ proves Theorem 1.1.

## References

[1] L. Babai, *Isomorphism problem for a class of point symmetric structures*, Acta Math. Acad. Sci. Hungar. **29** (1977), no. 3, 329–336. MR0485447 (58:5281)

[2] S. A. Evdokimov and I. N. Ponomarenko, *Polynomial time recognition and verification of isomorphism of circular graphs*, Algebra i Analiz **15** (2003), no. 6, 1–34; English transl., St. Petersburg Math. J. **15** (2004), no. 6, 813–835. MR2044629 (2005g:68053)

[3] T. Kasami, S. Lin, and W. W. Peterson, *New generalizations of the Reed–Muller codes.* I. *Primitive codes*, IEEE Trans. Information Theory **IT-14** (1968), 189–199. MR0275989 (43:1742)

[4] M. W. Liebeck, C. Praeger, and J. Saxl, *Regular subgroups of primitive permutation groups*, Mem. Amer. Math. Soc. **203** (2010), no. 952, 1–88. MR2588738 (2011h:20001)

[5] M. Muzychuk, *On the isomorphism problem for cyclic combinatorial objects*, Discrete Math. **197/198** (1999), 589–606. MR1674890

[6] H. Wielandt, *Finite permutation groups*, Acad. Press, New York–London, 1964. MR0183775 (32:1252)

[7] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lecture Notes, Dept. Math., Ohio St. Univ., Columbus, 1969.

Netanya Academic College, Netanya, Israel

Netanya Academic College, Netanya, Israel
*Email address*: muzy@netanya.ac.il

St. Petersburg Branch, Steklov Institute of Mathematics, Russian Academy of Sciences, Fontanka 27, 191023 St. Petersburg, Russia
*Email address*: inp@pdmi.ras.ru

Received 6/FEB/2017
Originally published in English