A FAMILY OF PERMUTATION GROUPS WITH
EXPONENTIALLY MANY NON-CONJUGATED REGULAR
ELEMENTARY ABELIAN SUBGROUPS

SERGEI EVDOKIMOV, MIKHAIL MUZYCHUK, AND ILIA PONOMARENKO

Abstract. Given a prime $p$, we construct a permutation group containing at least $p^{p^2-2}$ non-conjugated regular elementary abelian subgroups of order $p^3$. This gives the first example of a permutation group with exponentially many non-conjugated regular subgroups.

1. Introduction

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 of $\Gamma$-orbits

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

in the action of $\Gamma$ by conjugation on the set $\text{Reg}(\Gamma, H)$ 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 non-equivalent representations of this object as a Cayley object over $H$ in $\mathcal{C}$. Note that $H$ is a CI-group with respect to the category $\mathcal{C}$ if and only if $b_H(\Gamma) = 1$ for every group $\Gamma = \text{Aut}(X)$, where $X$ is 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, $b_H(\Gamma) \leq c(\Gamma)$, where $c(\Gamma)$ is the number of the conjugacy classes of full cycles contained in $\Gamma$. It was proved in [5] that the latter number does not exceed $n = |H|$. Thus, in this case $b_H(\Gamma) \leq n$.

The simplest non-cyclic 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 one can 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 $E_p$ in Theorem [7] below with $p^3$ replaced by $p^2$. With the help of the technique developed in Section [2] one can describe the set $\text{Reg}(\Gamma, H)$ (cf. Theorem [2] and Lemma [2]). Then applying [2] Theorem 6.1], one can prove that $b_H(P) \leq p$. Thus, in this case $b_H(\Gamma) \leq n$ too.

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

The proof of Theorem 1.1 is given in Section 3. It is based on a representation of the groups belonging to the class $E_p$ with the help of two-variable polynomials over the field $F_p$. The details are presented in Section 2. It is interesting to note that for every group $\Gamma$ from Theorem 1.1, the stabilizer of the imprimitivity system is, up to language, a Generalized Reed-Muller code [3].

**Notation.** As usual, $F_p$ and $\text{Sym}(V)$ 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 $F_p[X, Y]$ modulo the ideal generated by 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 one-dimensional subspaces $V_{i,j} = \{\alpha x^i y^j : \alpha \in F_p\}$, $i, j = 0, \ldots, p-1$, of the ring $R_p$ considered as a linear space over $F_p$.

Every element $f = \sum_{i,j} \alpha_{i,j} x^i y^j$ of $R_p$ yields a permutation $\sigma_f : \alpha x^i y^j \mapsto (\alpha + \alpha_{i,j})x^i y^j$ 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 $\text{Sym}(V)$ is denoted by $\Delta(I)$. In addition, we define two commuting permutations $\tau_x : \alpha x^i y^j \mapsto \alpha x^{i+1} y^j$, $\tau_y : \alpha x^i y^j \mapsto \alpha x^i y^{j+1}$. 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. $\tau_x^{-1} \sigma_f \tau_x = \sigma_{f_x}$ and $\tau_y^{-1} \sigma_f \tau_y = \sigma_{f_y}$ for all $f \in R_p$.  

---

2Here for groups $\Gamma \in E_p$, the upper bound in inequality (8) could be useful.
(2) $G_0 := (s, \tau_x, \tau_y)$ 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 in view of statement (1) of Lemma 2.1:

\[ \Delta(I) \subseteq \Gamma(I) \quad \text{and} \quad \Gamma(I)/\Delta(I) \cong E_{p^2}. \]

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

**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 $S = \{V_{i,j} : i, j = 0, \ldots, p-1\}$. 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 $\Gamma \leq \text{Sym}(V)$ 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 $\text{Orb}(s', V) = S'$. Then there exists a group isomorphism

\[ \varphi : G' \to G_0 \]

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 $G_0 \in \text{Reg}(\Gamma, E_{p^3})$. Note that the permutation $s$ belongs to the stabilizer $\Delta$ of the blocks $V_{i,j}$ in $\Gamma$. Therefore, $\text{Orb}(\Delta, V) = S$. 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. \qed

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 $t_{g,x} = \sigma_g \tau_x$ (resp. $t_{h,y} = \sigma_h \tau_y$) equals $p$ if and only if $g \in aR_p$ (resp. $h \in bR_p$), where $a = x - 1$ and $b = y - 1$.

**Proof.** Let $g = \sum_{i,j} \alpha_{i,j} x^i y^j$, and let $v = \alpha x^i y^j$ 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:

\[
\sum_{i=0}^{p-1} \alpha_{i,j} = 0, \quad j = 0, \ldots, p - 1.
\]

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

\[
\alpha_{0,j} = \alpha'_{0,j} - \alpha_{0,j}, \quad \alpha_{p-1,j} = \alpha'_{0,j} - \alpha'_{p-1,j},
\]

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 \( \text{Reg}(\Gamma_p, E_{p^3}) \) if and only if there exist elements \( g \in aR_p \) and \( h \in bR_p \) such that

\[
G = \langle s, t_{g,x}, t_{h,y} \rangle \quad \text{and} \quad ah = bg.
\]

**Proof.** To prove the “only if” part, suppose that \( G \in \text{Reg}(\Gamma_p, E_{p^3}) \). Then \( G \) is a self-centralizing subgroup of \( \text{Sym}(V) \). On the other hand, the centralizer of \( G \) in \( \text{Sym}(V) \) 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 equality in (4) holds.

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, \( G \in \text{Reg}(\Gamma_p, E_{p^3}) \), as required. \( \square \)

3. Proof of Theorem 1.1

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

For every integer \( k \geq 0 \), set

\[
I_k = \text{span}_{R_p} \{ a^i b^j : i + j \geq k \},
\]

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. $\dim(I_k) = (2p^2 - k)$,
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 $a^ib^j$ 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 $A_k$ (resp. $B_k$) is spanned by the monomials $ap^{-1}b^i$ (resp. $a^ib^{p-1}$) 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. $|\Reg(\Gamma_{k,p}, E_{p^3})| = p^{\dim(A_k) + \dim(B_k) + \dim(I_{k+1}) - 2}$,
3. $p^{\dim(I_k) - 4} \leq |G^\Gamma| \leq p^{\dim(I_k) - 1}$ for all $G \in \Reg(\Gamma_{k,p}, E_{p^3})$.

**Proof.** Obviously, $|\Delta(I_k)| = p^{\dim(A_k)}$. Therefore, statement (1) follows from the right-hand side of formula (2). Next, from Lemma 3.1 it follows that

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

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

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

However, $I_k \cap aR_p = I_k \cap bR_p = I_k$, because $k \geq p$. 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 $t_{g,x} = s^it_{g',x}$ and $t_{h,y} = s^jt_{h',y}$ for some $0 \leq i, j \leq p - 1$. 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 in view of statement (1),

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

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 $\Aut(G) \cong GL(3, p)$ (here we use the fact that $\Gamma$ is a $p$-group), we conclude that

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

However, $|P| = p^3$. Thus, statement (3) follows from formula (6). □
To complete the proof of Theorem 1.1, we note that \( \text{Reg}(\Gamma_k, E_p^3) \) is the disjoint union of distinct sets \( G^{\Gamma_k} \), where \( \Gamma_k = \Gamma_{k,p} \) as in Lemma 3.2 and \( G \in \text{Reg}(\Gamma_k, E_p^3) \). Therefore, setting \( m_k \) and \( M_k \) to be, respectively, the minimum and maximum of the numbers \( |G^{\Gamma_k}| \), we obtain

\[
\frac{|\text{Reg}(\Gamma_k, E_p^3)|}{m_k} \geq b_H(\Gamma_k) \geq \frac{|\text{Reg}(\Gamma_k, E_p^3)|}{M_k}.
\]

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

\[
\frac{|\text{Reg}(\Gamma_k, E_p^3)|}{m_k} \leq p^{d+2} \quad \text{and} \quad \frac{|\text{Reg}(\Gamma_k, E_p^3)|}{M_k} \geq p^{d-1}.
\]

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

\[
p^{2p-k+1} \geq b_H(\Gamma_k) \geq p^{2p-k-2}.
\]

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. Hung., 29, No. 3, 329–336 (1977).
[2] S. Evdokimov and I. Ponomarenko, Recognizing and isomorphism testing circulant graphs in polynomial time, Algebra and Analysis, 15, No. 6, 1–34 (2003).
[3] T. Kasami, S. Lin, and W. W. Peterson, New generalisations of the Reed-Muller codes, EEE Trans. Information Theory, IT-14, 189–199 (1968).
[4] M. W. Liebeck, C. Praeger, and J. Saxl, Regular subgroups of primitive permutation groups, Memoirs Amer. Math. Soc., 203, No. 952, 1–88 (2010).
[5] M. Muzychuk, On the isomorphism problem for cyclic combinatorial objects, Discr. Math., 197/198, 589–606 (1999).
[6] H. Wielandt, Finite permutation groups, Academic press, New York - London (1964).
[7] H. Wielandt, Permutation groups through invariant relations and invariant functions, Lect. Notes Dept. Math. Ohio St. Univ., Columbus (1969).

Steklov Institute of Mathematics at St. Petersburg, Russia
E-mail address: evdokim@pdmi.ras.ru

Netanya Academic College, Netanya, Israel
E-mail address: muzy@netanya.ac.il

Steklov Institute of Mathematics at St. Petersburg, Russia
E-mail address: inp@pdmi.ras.ru