Advances in Pure and Applied Mathematics
2025, vol. 16, n° 3, 20-25 pages, DOI: 10.21494/ISTE.OP.2025.1315 ISTE OpenScience

Permutation groups with two orbits having constant movement

Groupe de permutations avec deux orbites à mouvement constant

Mehdi Rezaei*[,1] and Mehdi Alaeiyan[2]

[1]Mehdi Rezaei, Department of Mathematics, Buein Zahra Technical University, Buein Zahra, Qazvin, Iran
mehdrezaei@gmail.com,m_rezaei@bzte.ac.ir
ORCID iD: 0000-0001-6999-9703
[2]Mehdi Alaeiyan, Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran 16846, Iran.
alaeiyan@iust.ac.ir
ORCID iD: 0000-0003-2185-5967

ABSTRACT. Let G be a permutation group on a set Ω with no fixed points in Ω, and let m be a positive integer. If for each subset Γ of Ω the size $|\Gamma^g - \Gamma|$ is bounded, for $g \in G$, the movement of g is defined as move$(g) := \max |\Gamma^g - \Gamma|$ over all subsets Γ of Ω, and move(G) is defined as the maximum of move(g) over all non-identity elements of $g \in G$. Suppose that G is not a 2-group. It was shown by Praeger that $|\Omega| \leqslant \lceil \frac{2mp}{p-1} \rceil + t - 1$, where t is the number of G-orbits on Ω and p is the least odd prime dividing $|G|$. In this paper, we classify all permutation groups with maximum possible degree $|\Omega| = \lceil \frac{2mp}{p-1} \rceil + t - 1$ for $t = 2$, in which every non-identity element has constant movement m.
2000 Mathematics Subject Classification. 20B05
KEYWORDS. Intransitive permutation groups; orbits; bounded movement; constant movement.

1 Introduction

Let G be a permutation group on a set Ω with no fixed points in Ω and let m be a positive integer. If for a subset Γ of Ω the size $|\Gamma^g - \Gamma|$ is bounded, for $g \in G$, the *movement of* Γ is defined as:

$$\text{move}(\Gamma) := \max_g |\Gamma^g - \Gamma|.$$

If move$(\Gamma) \leq m$ for all $\Gamma \subseteq \Omega$, then G is said to have *bounded movement* m and the *movement of* G is defined as:

$$\text{move}(G) := \max_{\Gamma, g} |\Gamma^g - \Gamma|.$$

In [7], the concept of the movement of elements in a group is introduced. For any element $g \in G$, we define the *movement of* g as follows:

$$\text{move}(g) := \max_{\Gamma} |\Gamma^g - \Gamma|.$$

If all non-identity elements of G have the same movement, then G is said to have *constant movement*. It is evident that every permutation group with constant movement has bounded movement. According to Theorem 1 in [7], if G has a bounded movement equal to m, then the set Ω is finite. Furthermore, both the number of G-orbits in Ω and the length of each G-orbit are bounded above by linear functions of m. Specifically, Lemma 2.2 in [7] demonstrates that if G is not a 2-group and p is the least odd prime dividing $|G|$, then each G-orbit has a length at most $\lceil \frac{2mp}{p-1} \rceil + 1$ and $n := |\Omega| \leq \lceil \frac{2mp}{p-1} \rceil + t - 1$, where t represents the number of G-orbits on Ω. The case when $t = 1$ is verified and classified in [3].

Corresponding author.

Throughout this paper, we consider a positive integer m and an intransitive permutation group G acting on a set Ω of size n with movement m and t $(= 2)$ orbits, such that $n = \lceil \frac{2mp}{p-1} \rceil + t - 1$. The main objective of this paper is to classify all intransitive permutation groups of degree $n = \lceil \frac{2mp}{p-1} \rceil + t - 1$, for $t = 2$.

It's important to note that for $x \in \mathbb{R}$, $\lfloor x \rfloor$ represents the integer part of x, and $\lceil x \rceil$ denotes the least integer greater than or equal to x. Additionally, $K \rtimes H$ denotes the semi-direct product of K and H with normal subgroup K.

Theorem 1.1. *Let G be a permutation group on a set Ω with $t = 2$ orbits which has no fixed points in Ω. Suppose further that m is a positive integer such that G has constant movement m and $n = \lceil \frac{2mp}{p-1} \rceil + 1$. Then G is one of the following:*
(I) $G \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$;
(II) $G \cong \mathbb{Z}_q \rtimes \mathbb{Z}_p$, where $q = p(p-1) + 1$.

The structure of the groups in Theorem 1.1 will be explained in Example 2.2 and Example 2.3, respectively.

2 Examples and Preliminaries

Let $1 \neq g \in G$. Suppose that g has a disjoint cycle representation with s nontrivial cycles of lengths $l_1, ..., l_s$. We can represent g as

$$g = (a_1 a_2 ... a_{l_1})(b_1 b_2 ... b_{l_2})...(z_1 z_2 ... z_{l_s}).$$

Let $\Gamma(g)$ be a subset of Ω that consists of $\lfloor l_i/2 \rfloor$ points from the i^{th} cycle, for each i, chosen in a way that $\Gamma(g)^g \cap \Gamma(g) = \emptyset$. For example, we could choose

$$\Gamma(g) = \{a_2, a_4, \ldots, a_{k_1}, b_2, b_4, \ldots, b_{k_2}, ..., z_2, z_4, \ldots, z_{k_s}\},$$

where $k_i = l_i - 1$ if l_i is odd and $k_i = l_i$ if l_i is even.

Note that $\Gamma(g)$ is not uniquely determined as it depends on the way each cycle is written. For any set $\Gamma(g)$ of this kind, we say that $\Gamma(g)$ *consists of every second point of every cycle of g*. From the definition of $\Gamma(g)$ we see that

$$|\Gamma(g)^g - \Gamma(g)| = |\Gamma(g)| = \sum_{i=1}^{s} \lfloor l_i/2 \rfloor.$$

The next lemma shows that this quantity is an upper bound for $|\Gamma^g - \Gamma|$ for an arbitrary subset Γ of Ω.

Lemma 2.1. *(Lemma 2.1 of [5]) Let G be a permutation group on a set Ω and suppose that $\Gamma \subseteq \Omega$. Then for each $1 \neq g \in G$, $|\Gamma^g - \Gamma| \leq \Sigma_{i=1}^{s} \lfloor l_i/2 \rfloor$, where l_i is the length of the i^{th} cycle of g and s is the number of nontrivial cycles of g in its disjoint cycle representation. This upper bound is attained for $\Gamma = \Gamma(g)$ defined above.*

Now in the following examples, we explain the structure of groups mentioned in Theorem 1.1.

Example 2.2. Let $G_1 := \mathbb{Z}_2^2$ and $G_2 := \mathbb{Z}_3$ be permutation groups on the sets $\Omega_1 = \{1, 2, 3, 4\}$ and $\Omega_2 = \{1', 2', 3'\}$ respectively, where $\mathbb{Z}_2^2 \cong < (1\,2)(3\,4), (1\,3)(2\,4) >$ and $\mathbb{Z}_3 \cong < (1\,2\,3)(1'2'3') >$. Set $\Omega := \Omega_1 \cup \Omega_2$. Then $G := G_1 \rtimes G_2$ is a permutation group on Ω which has $t = 2$ orbits, and since each non-identity element of G has two cycles of length 2 or two cycles of length 3, so $m =$move$(G) = 2$. It follows that $n = \lceil \frac{2mp}{p-1} \rceil + t - 1 = 7$, which meets the upper bound in Theorem 1.1 for $p = 3$. □

Let g be an element of a permutation group G on a set Ω. Assume that the set Ω is the disjoint union of G-invariant sets Ω_1 and Ω_2. Then every subset Γ of Ω is a disjoint union of subsets $\Gamma_i = \Gamma \cap \Omega_i$ for $i = 1, 2$. Let g_i be the permutation on Ω_i induced by g for $i = 1, 2$. Since $|\Gamma^g - \Gamma| = |\Gamma_1^{g_1} - \Gamma_1| + |\Gamma_2^{g_2} - \Gamma_2|$, we have:

$$\text{move}_\Omega(g) = \sum_{i=1}^{2} \max\{|\Gamma_i^{g_i} \setminus \Gamma_i| | \Gamma_i \subseteq \Omega_i\} = \text{move}_{\Omega_1}(g_1) + \text{move}_{\Omega_2}(g_2).$$

The second example is as follows.

Example 2.3. Let p and q be two prime numbers such that $q := p(p-1) + 1$, r is an integer such that $r^p \equiv 1 (\text{mod } q)$, and $\mathbb{Z}_q =< \alpha >$, $\mathbb{Z}_p =< \beta >$ be permutation groups on sets Ω_1 and Ω_2 of sizes q and p, respectively. Assume that K is the group generated by $\gamma := \beta\gamma_1 ... \gamma_{p-1}$, where the cycles γ_i $(1 \le i \le p-1)$ are of length p from Ω_1. Thus $K \cong \mathbb{Z}_p$ and the group $G := \mathbb{Z}_q \rtimes K$ given by the defining relations:

$$\alpha^q = \gamma^p = 1, \quad \gamma^{-1}\alpha\gamma = \alpha^r, \quad r^p \equiv 1 (\text{mod } q).$$

is a permutation group on $\Omega := \Omega_1 \cup \Omega_2$ with $t = 2$ orbits such that $\mathbb{Z}_q$ acts regularly on Ω_1. Since each non-identity element of G has either p cycles of length p or one cycle of length q, we have $m =$move$(G) = \frac{p(p-1)}{2}$. It follows that $n = \lceil \frac{2mp}{p-1} \rceil + 1 = p^2 + 1$, which meets the upper bound in Theorem 1.1.

In particular, for $p = 3$ we can consider $\Omega_1 = \{1, ..., 7\}$, $\Omega_2 = \{1', 2', 3'\}$, $\alpha = (1...7)$ and $\gamma = (1'2'3')(2\,3\,5)(4\,7\,6)$. Then $G :=< \alpha, \gamma >\cong \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ is a permutation group with $t = 2$ orbits on a set $\Omega := \Omega_1 \cup \Omega_2$ of size 10, in which every $1 \ne g \in G$ has 3 cycles of size 3 or is a cycle of size 7 and therefore in both cases have movement 3. It follows that $n = \lceil \frac{2mp}{p-1} \rceil + t - 1 = 10$. This example is one of the groups mentioned in example above for $p = 3$. □

3 The Proof of Theorem 1.1

Before starting the proof of Theorem 1.1, we give some basic notions and results.

Definition 3.1. A group G is called a CP-group if every non-identity element of G has prime power order.

Definition 3.2. A finite group G is called 2-Frobenius if there exists a normal series $1 \lhd N \lhd K \lhd G$ of G such that N is the Frobenius kernel of K and $\frac{K}{N}$ is the Frobenius kernel of $\frac{G}{N}$.

The following lemma (Lemma 0.4 of [8]), presents a complete classification of finite CP-groups.

Lemma 3.3. *Let G be a finite CP-group. Then*

(1) G is nilpotent if and only if G is a p-group.

(2) If G is solvable and non-nilpotent, then $|G| = p^\alpha q^\beta$. Suppose P (or Q) is the Sylow p(or q)-subgroups of G, and P_1 is the maximal normal p-subgroup of G.

(a) If the Sylow 2-subgroup of G is a quaternion group, then $p \neq 2$, $q = 2$, and G is a Frobenius group with Frobenius complement Q. Moreover, G has the chief factors $\underbrace{2,\ldots,2}_{\beta}$; $p^{b_1},\ldots,p^{b_k}$, $b_i > 1$, $b \mid b_i$, $i = 1,\ldots,k$, where b is the exponent of p(mod $2^{\alpha-1}$).

(b) Suppose the order of G is odd or the Sylow 2-subgroup of G is not a quaternion group. Then G/P_1 is cyclic $(P_1 = P)$ or metacyclic $(P_1 < P)$ and G is Frobenius or 2-Frobenius, respectively.

(b1) $P_1 = P$ and G is a Frobenius group with Frobenius kernel P and cyclic complement Q. Moreover, G has the chief factors $\underbrace{q,\ldots,q}_{\beta}$; $\underbrace{p^b,\ldots,p^b}_{k}$, $\alpha = kb$, where b is the exponent of p(mod q^β). In this case, the nilpotent class of P is less than or equal to k.

(b2) $P_1 < P$ and G is a 2-Frobenius group. If $|G/P_1| = p^\gamma q^\beta$, then $p^\gamma|(q-1)$. G has the chief factors $\underbrace{p,\ldots,p}_{\gamma}$; $\underbrace{q,\ldots,q}_{\beta}$; $p^{b_1},\ldots,p^{b_k}$, $b_i > 1$, $b \mid b_i$, $i = 1,\ldots,k$, $\gamma < b$, where b is the exponent of p(mod q^β).

(3) If G is simple, then $G \cong L_2(q)$, $q = 5, 7, 8, 9, 17$; $L_3(4)$, $Sz(8)$ or $Sz(32)$ (Theorem 16 of [10]).

(4) If G is non-solvable and non-simple, $G \cong M_{10}$, or G has an elementary abelian 2-subgroup P, P is normal in G and $G/P \cong L_2(q)$, $q = 5, 8$; $Sz(8)$ or $Sz(32)$ (Theorem 3 of [4]; Theorem 3.1 of [9]).

Lemma 3.4. *(Lemma 3.6 of [3]) Let G be a permutation group on a set Ω of size n with constant movement m, and let $1 \neq g \in G$. Then all non-trivial cycles of g have the same size and the order of g is either an odd prime or a power of 2.*

As a result of the above lemma we can say that if G is a permutation group with constant movement m on a set Ω of size n, then G is a CP-group. Also, one can see that there is no non-solvable CP-group with $t = 2$ orbits having constant movement. So, G is solvable and by Theorem 1 of [6], G has order divisible by at most two primes. So the order of G is of the form $p^\alpha q^\beta$, for some non-negative integers α and β. Therefore, by Lemma 3.3, G is either a p-group, a Frobenius group or a 2-Frobenius group. We now give an elementary but useful lemma.

Lemma 3.5. *With the above notations, if $n = \lceil \frac{2mp}{p-1} \rceil + 1$, then $m = \lfloor \frac{(n-1)(p-1)}{2p} \rfloor$.*

Proof. From the inequality

$$\frac{2mp}{p-1} \leq \lceil \frac{2mp}{p-1} \rceil < \frac{2mp}{p-1} + 1,$$

we have

$$\frac{p-1}{2p} + m \leq \frac{n(p-1)}{2p} < \frac{p-1}{p} + m < \frac{p-1}{2p} + m + 1.$$

So

$$m \leq \frac{n(p-1)}{2p} - \frac{p-1}{2p} < m + 1,$$

and therefore we can conclude that,

$$m = \lfloor \frac{(n-1)(p-1)}{2p} \rfloor.$$

□

To prove Theorem 1.1, we can introduce the following notation:

Let $r_p(a)$ be the number of G-orbits of length p on which G acts as $\mathbb{Z}_p \rtimes \mathbb{Z}_{2^a}$ with $0 \leq a \leq a_0$, where 2^{a_0} is the 2-part of $(p-1)$. We then define r_p as the sum of $r_p(a)$ for a ranging from 0 to a_0. This represents the total number of G-orbits of length p. Moreover, let Φ be the union of G-orbits of lengths 2^b, and let u be the number of orbits in Φ. Additionally, we define s as the number of G-orbits of length greater than p.

The orbits are labeled as follows: $\Omega_1, ..., \Omega_{r_p}$ are those of length p on which G acts as $\mathbb{Z}_p \rtimes \mathbb{Z}_{2^a}$ for some $a \geq 0$; $\Omega_{r_p+1}, ..., \Omega_{r_p+u}$ are those of length 2^b; and so on. We define t as r_p+u+s, representing the total number of G-orbits. As Φ is a union of u G-orbits whose lengths are powers of 2, we may express $|\Phi|$ as $2u + 2\delta$ for some non-negative integer δ. If $\delta = 0$, then Φ is the union of u G-orbits of length 2.

Finally, since Ω is the union of r_p G-orbits of length p, Φ, and Δ (the union of s G-orbits of lengths greater than p), we have $n := |\Omega| = pr_p + (2u + 2\delta) + |\Delta|$.

Suppose that G is a permutation group with constant movement m on a set Ω of size $n = \lceil \frac{2mp}{p-1} \rceil + 1$ having $t = 2$ orbits. Since p is the least odd prime dividing $|G|$ and G has constant movement with maximum possible degree, we can assume that $r_p \neq 0$. It follows that there are only the following possibilities:

$I)$ $r_p = 2, u = s = 0,$

$II)$ $r_p = 1, u = 1, s = 0$

$III)$ $r_p = 1, s = 1, u = 0$

We first consider the case (I). We have $n = 2p$ and therefore Lemma 3.5 implies that $m = \lfloor \frac{(2p-1)(p-1)}{2p} \rfloor = p-1+\lfloor \frac{-(p-1)}{2p} \rfloor = p-2$. But the movement of G (in this case) is $m = \frac{p-1}{2} + \frac{p-1}{2} = p-1$ (see Corollary 2.3 of [2], Lemma 3.2 of [5]). Thus this case does not occur.

Suppose that the case (II) holds. So we have $n = p + 2^b$. By Lemma 3.5, we conclude that $m = \lfloor \frac{(p+2^b-1)(p-1)}{2p} \rfloor = 2^{b-1} - 1 + \lfloor \frac{(p^2-2^b+1)}{2p} \rfloor = 2^{b-1} - 1 + \frac{p-1}{2}$. It follows that $n = 2m+3$. Comparing with $n = \lceil \frac{2mp}{p-1} \rceil + 1$, we have $n = p+4$ and $m = \frac{p+1}{2}$. Since G has constant movement, m is equal to $\frac{p-1}{2}$ or 2 and this is possible when $p = 3$, $m = 2$ and $n = 7$. Now Theorem 1.1. of [1] implies that the group mentioned in Example 2.2 is the only group satisfying in this case.

Finally, we consider the case (III). It is easy to see that the group in Example 2.3 satisfies in this case and we also will show that it is the only example satisfying in the case (III). In this case we have $n = p+|\Delta|$. Since $|G| = p^a q^b$, G has two elements of orders p and q, say x and y respectively. With respect to Lemma 3.4, we can represent x and y as $x = c_1...c_l$ and $y = e_1...e_k$, where $|c_i| = p$ and $|e_j| = q$ (for all $1 \leq i \leq l$ and $1 \leq j \leq k$). Since G has constant movement, we have move$(x) = \frac{l(p-1)}{2} = \frac{k(q-1)}{2}$=move$(y)$. With respect to equality $(l-1)p = q-1$, we have $kp(l-1) = l(p-1)$. The last equality holds if and only if $k = 1$ and $l = p$ and therefore $q = p(p-1)+1$, $m = \frac{p(p-1)}{2}$ and G has two orbits, one of them is of length $|\Delta| = p(p-1)+1$ and the other is of length p. Since G is a CP-group with constant movement m, we conclude that G is a Frobenius group with kernel $\mathbb{Z}_q$ and complement $\mathbb{Z}_p$, in which $\mathbb{Z}_p$ is generated with p cycles of length p that described in Example 2.3.

Now the proof of Theorem 1.1 is complete.

References

[1] Alaeiyan, M. and Rezaei, M., Intransitive permutation groups with bounded movement having maximum degree, *Math. Rep.*, **13(63)**(2), 2011, 109-115.

[2] Alaeiyan, M. and Tavallaee, H. A., Improvement on the Bound of Intransitive Permutation Groups with Bounded Movement, *Bull. Belg. Math. Soc. Simon Stevin*, **13(3)**, 2006, 471-477.

[3] Alaeiyan, M. and Tavallaee, H. A., Permutation groups with the same movement, *Carpathian. J. Math.*, **25**(2), 2009, 147-156.

[4] Brandl, R., Finite groups all of whose elements are of prime power order, *Boll. Un. Mat. Ital.*, A(5) **18**(3), 1981, 491-493.

[5] Hassani, A., Khayaty (Alaeiyan), M., Khukhro, E. I. and Praeger, C. E., Transitive permutation groups with bounded movement having maximal degree, *J. Algebra*, **214**, 1999, 317-337.

[6] Higman, G., Finite groups in which every element has prime power order, *J. London Math. Soc.*, **32**, 1957, 335-342.

[7] Praeger, C. E., On permutation groups with bounded movement, *J. Algebra*, **144**, 1991, 436-442.

[8] Shi, W. J. and Lv, H., A Note of CP_2 Groups, *Commun. Math. Stat.*, **5**, 2017, 447–451.

[9] Shi, W. J. and Yang, W. Z., The finite groups all of whose elements are of prime power order, *J. Yunnan Educ. Coll.*, **1**, 1986, 2–10. (in Chinese)

[10] Suzuki, M., On a class of doubly transitive groups. *Ann. Math.* **75**, 1962, 105–145.

