TRANSITIVE PERMUTATION GROUPS WITH ELEMENTS OF MOVEMENT m OR $m-1$

MEHDI ALAEIYAN and BAHMAN ASKARI

Let G be a permutation group on a set Ω with no fixed point in Ω and let m be a positive integer. If for each subset Γ of Ω the size $|\Gamma^g \setminus \Gamma|$ is bounded, for $g \in G$, we define the movement of g as the max $|\Gamma^g \setminus \Gamma|$ over all subsets Γ of Ω, and the movement of G is defined as the maximum of move(g) over all non-identity elements of $g \in G$. In this paper we will classify all transitive permutation groups G with bounded movement equal to m, such that G is not a 2-group but in which every non-identity element has the movement m or $m-1$.

AMS 2010 Subject Classification: 20B05.

Key words: permutation group, transitive, bounded movement, fixed point free element.

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 each subset Γ of Ω and each element $g \in G$, the size $|\Gamma^g \setminus \Gamma|$ is bounded, we define the *movement* of Γ as $\mathrm{move}(\Gamma) = \max_{g\in G} |\Gamma^g \setminus \Gamma|$. If $\mathrm{move}(\Gamma) \leqslant m$ for all $\Gamma \subseteq \Omega$, then G is said to have *bounded movement* and the *movement* of G is defined as the maximum of move(Γ) over all subsets Γ. This notion was introduced in [11]. Similarly, for each $1 \neq g \in G$, we define the movement of g as the max $|\Gamma^g \setminus \Gamma|$ over all subsets Γ of Ω. If all non-identity elements of G have the same movement, then we say that G has *constant movement*.

Clearly, every permutation group in which every non-identity element has movement m or $m-1$, is a permutation group with bounded movement equal to m. Further, by [11, Theorem 1], if G has movement equal to m, then Ω is finite, and its size is bounded by a function of m.

For each transitive permutation group G on a set Ω with bounded movement equal to m, where G is not a 2-group, the maximum bounds of Ω were obtained in [7, 11] as follows:

Lemma 1.1 [11, Lemma 2.2]. *Let G be a transitive permutation group on a set Ω such that G has movement equal to m. Suppose G is not a 2-group and*

p is the least odd prime dividing $|G|$, then $|\Omega| \leqslant \lfloor 2mp/(p-1) \rfloor$. (For $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.).

We will see that every transitive permutation group G with bounded movement equal to m, such that G is not a 2-group but in which every non-identity element has the movement m or $m-1$, the bound of Lemma 1.1 is not attained. For example, if we consider $G := \mathbb{Z}_{2p}$ as a permutation group on a set of size $n = 2p$, where p is an odd prime, then we see that every non-identity element has the movement p or $p-1$ (see Lemma 3.2).

The purpose of this paper is to classify all transitive permutation groups G with bounded movement equal to m, such that G is not a 2-group but in which every non-identity element has the movement m or $m-1$. It follows that $m \geq 2$. We denote by $K \rtimes P$ a semi-direct product of K by P with normal subgroup K.

We now have the following main theorem:

Theorem 1.2. *Let m be a positive integer, and let G be a transitive permutation group on a set Ω with no fixed point in Ω and bounded movement equal to m, in which every non-identity element has movement m or $m-1$. Suppose G is not a 2-group and p is the least odd prime dividing $|G|$. Then G is one of the following groups:*

(1) $G \in \{S_4, A_4\}$, $|\Omega| = 4$ *and* $m = 2$;
(2) $G \in \{S_5, A_5\}$, $|\Omega| = 5$ *and* $m = 2$;
(3) $G \in \{D_{18}, \mathbb{Z}_9\}$, $|\Omega| = 9$ *and* $m = 4$;
(4) $G = D_{2n}$, $|\Omega| = n$, *where* $n = 2p$, *and* $m = p$;
(5) $G = \mathbb{Z}_{2p}$, $|\Omega| = 2p$ *and* $m = p$;
(6) $G = AGL(1, q)$, *where* $q := 2p+1$ *is an odd prime,* $|\Omega| = q$ *and* $m = p$.

2. PRELIMINARIES

Let G be a transitive permutation group on a finite set Ω. Then by [13, Theorem 3.26], which we shall refer to as Burnside's lemma, the average number of fixed points in Ω of elements of G is equal to the number of G-orbits in Ω, namely 1, and since 1_G fixes $|\Omega|$ points and $|\Omega| > 1$, it follows that there is some element of G which has no fixed points in Ω. We shall say that such elements are fixed point free on Ω.

Let $1 \neq g \in G$ and suppose that g in its disjoint cycle representation has t nontrivial cycles of lengths $l_1, l_2, \ldots, l_t$, say. We might represent g as

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

Let $\Gamma(g)$ denote a subset of Ω consisting of $\lfloor l_i/2 \rfloor$ points from the i-th cycle, for each i, chosen in such a way that $\Gamma(g)^g \cap \Gamma(g) = \varnothing$. For example, we could choose

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

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 down. 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

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

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

Lemma 2.1 [7, Lemma 2.1]. *Let G be a permutation group on a set Ω and suppose that $\Gamma \subseteq \Omega$. Then for each $g \in G$, $|\Gamma^g \setminus \Gamma| \leq \sum_{i=1}^{t} \lfloor l_i/2 \rfloor$ where l_i is the length of the i-th cycle of g and t is the number of nontrivial cycles of g in its disjoint cycle representation. This upper bound is attained for $\Gamma = \Gamma(g)$ defined above.*

Let m be a positive integer, and let G be a permutation group on a set Ω of size n with bounded movement equal to m, in which every non-identity element has the movement m or $m-1$. Then we have the following basic result:

Proposition 2.2. *Let m be a positive integer, and let G be a permutation group on a set Ω of size n with bounded movement equal to m, in which every non-identity element has the movement m or $m-1$. Further, suppose that $1 \neq g \in G$ and $g = c_1 \dots c_s$ is the decomposition of g into its disjoint non-trivial cycles such that $|c_i| = l_i$ for $1 \leq i \leq s$. Then either*

(i) *$l := l_1 = l_2 = \dots = l_s$, where l is an odd prime or a power of 2;*

(ii) *$s = 2$, $l_i = 2$ and $l_j = 3$ for $1 \leq i, j \leq 2$ and $i \neq j$;*

(iii) *$s = 2$, $l_i = 3$ and $l_j = 6$ for $1 \leq i, j \leq 2$ and $i \neq j$;*

(iv) *g has a cycle of length 2 and $(s-1)$ cycles of length a power of 2 for $s \geq 2$.*

Moreover, the order of g is either an odd prime, a power of 2 or 6. Otherwise, g is a cycle of length 9 or $2p$, where p is an odd prime.

Proof. Let $1 \neq g \in G$. Then by Lemma 2.1, the movement of g, move(g), is the size of the subset $\Gamma(g)$ consisting of every second point of every cycle g, that is, move$(g) = \sum_{i=1}^{s} \lfloor l_i/2 \rfloor$. For each $1 \leq t \leq s$, we consider the element $h = g^{l_t}$ of G and compare the movement of h with the movement of g. As above, we have

$$\mathrm{move}(h) \leq \sum_{j \neq t} \lfloor l_j/2 \rfloor < \sum_{i=1}^{s} \lfloor l_i/2 \rfloor = \mathrm{move}(g).$$

We now consider the following two cases:

Case 1. Let $\mathrm{move}(g) = m - 1$, then $h = 1$.

Hence, we must have $l := l_1 = l_2 = \cdots = l_s$. Suppose now that l is not a power of 2, and let p be an odd prime such that $l = pk$ for some positive integer k. Then by comparing the movement of g and its power g^k we obtain

$$s\lfloor l/2 \rfloor = \mathrm{move}(g) = \mathrm{move}(g^k) = sk\frac{p-1}{2}.$$

It can be easily verified that $\lfloor \frac{kp}{2} \rfloor = k(p-1)/2$ if and only if $k = 1$, and so $l = p$.

Case 2. Let $\mathrm{move}(g) = m$, then $\mathrm{move}(h) = m - 1$ or $h = 1$.

We first suppose that $\mathrm{move}(h) = m - 1$. Then with new enumeration we can assume that $h = c_1 c_2 \ldots c_{s'}$, where $s' < s$ and $s' + 1 \leq t \leq s$. Therefore,

$$\mathrm{move}(g) = \mathrm{move}(h) + \sum_{i=s'+1}^{s} \left\lfloor \frac{l_i}{2} \right\rfloor.$$

Since $\mathrm{move}(g) = \mathrm{move}(h) + 1$, we must have $t = s = s' + 1$ and also $l_t = 2$ or 3. Again with suitable enumeration we can suppose that $h = c_1 \ldots c_{t-1} c_{t+1} \ldots c_s$, where $\mathrm{move}(h) = m - 1$. By Case 1, we have $l := l_1 = \cdots = l_{t-1} = l_{t+1} = \cdots = l_s$ where l is an odd prime or a power of 2. It is straightforward to verify that $s = 2$, $l_i = 2$ and $l_j = 3$ for $1 \leq i, j \leq 2$ and $i \neq j$.

In the second case we may assume that $h = 1$. Then we must have $l := l_1 = l_2 = \cdots = l_s$. Suppose now that l is not a power of 2, and let p be an odd prime such that $l = pk$ for some positive integer k. Then we obtain that

$$\mathrm{move}(g) = s\left\lfloor \frac{pk}{2} \right\rfloor, \quad \mathrm{move}(g^k) = sk\frac{p-1}{2}.$$

It can be easily shown that $\mathrm{move}(g^k) < m - 1$ for $k \geq 4$, a contradiction. So, we may assume that $k < 4$. For $k = 1$, we have $\mathrm{move}(g) = \mathrm{move}(g^k)$ and $l = p$. Now, if $k = 2$, then we have $\mathrm{move}(g) = sp$ and $\mathrm{move}(g^k) = s(p-1)$. This implies that $s = 1$ and $l = 2p$, that is, g is a cycle of length $2p$. Finally, if $k = 3$ and $p \neq 3$, then $\mathrm{move}(g^p) < m - 1$, a contradiction. Thus $p = 3$. It follows that $\mathrm{move}(g) = 4s$ and $\mathrm{move}(g^k) = 3s$, and this implies that $s = 1$ and $l = 9$, that is, g is a cycle of length 9.

In the second case we may assume that $\mathrm{move}(h) = \mathrm{move}(g^{l_i}) = m - 1$ and $h = g^{l_j} = 1$ for some $1 \leq i, j \leq t$ and $i \neq j$. As above, we can conclude that g is either $(s-1)$ cycles of length a power of 2 and a cycle of length

2 for $s \geq 2$, or a cycle of length 6 and a cycle of length 3. The result now follows. $\square$

3. THE PROOF OF THEOREM 1.2

In this section we suppose that m is a positive integer and G is a transitive permutation group on a set Ω of size n with bounded movement equal to m, such that G is not a 2-group but in which every non-identity element has the movement m or $m-1$. If for every $1 \neq g \in G$, $\text{move}(g) = m$ then G has constant movement were classified in [2]. So, in the rest of this section we can assume that G has at least one element of movement $m-1$. We also suppose that p is the least odd prime dividing $|G|$.

Lemma 3.1. *The groups $G = D_{18}$ and $G = \mathbb{Z}_9$ act transitively on a set of size $n = 9$ and in this action every non-identity element has movement 4 or 3.*

Proof. Let $M := \langle \alpha \rangle$ and $N := \langle \beta \rangle$ be two cyclic permutation groups on the set $\Omega = \{1, 2, \ldots, 9\}$, where $\alpha = (1\ 2\ \ldots\ 9)$ is a cycle of length 9 and $\beta = (1\ 3)(4\ 9)(5\ 8)(6\ 7)$ is four cycles of length 2. It is straightforward to verify that $M \cong \mathbb{Z}_9$ and $D_{18} \cong \langle M, N \rangle$. Since $M \leqslant G$ act transitively on a set Ω, so G is a transitive permutation group on a set Ω. Let $1 \neq g \in M$, then it is easy to see that g has order 3 or 9. Suppose that $\Gamma(g)$ consist of every second point of every cycle of g. If $o(g) = 9$ then g is a cycle of length 9 and hence $|\Gamma(g)^g \setminus \Gamma(g)| = 4$, that is, $\text{move}(g) = 4$. Now, if $o(g) = 3$ then g has three cycles of length 3 and hence $|\Gamma(g)^g \setminus \Gamma(g)| = 3$, that is, $\text{move}(g) = 3$. Let $1 \neq g \in \langle M, N \rangle$, $g \notin M$ and $g \notin N$. Then g has four cycles of length 2 and similarly, $\text{move}(g) = 4$. Also we know that $\text{move}(\beta) = 4$. This implies that every non-identity element of G has movement 4 or 3. $\square$

Lemma 3.2. *The group $G = \mathbb{Z}_{2p}$ act transitively on a set of size $2p$, where p is an odd prime, and in this action every non-identity element has movement p or $p-1$.*

Proof. Let $1 \neq g \in G$. Then it can be easily shown that g has order 2, p or $2p$. Suppose that $\Gamma(g)$ consist of every second point of every cycle of g. If $o(g) = 2$ then g has p cycles of length 2 and hence $|\Gamma(g)^g \setminus \Gamma(g)| = p$, that is, $\text{move}(g) = p$. If $o(g) = p$ then g has two cycles of length p and hence $|\Gamma(g)^g \setminus \Gamma(g)| = 2\frac{p-1}{2} = p-1$, that is, $\text{move}(g) = p-1$. Finally, if $o(g) = 2p$ then g is a cycle of length $2p$ and similarly, $\text{move}(g) = p$. It follows that every non-identity element of G has movement p or $p-1$. $\square$

Lemma 3.3. *The group $G = D_{2n}$ act transitively on a set of size $n = 2p$, where p is an odd prime, and in this action every non-identity element has movement p or $p-1$.*

Proof. Let $M := \langle\alpha\rangle$ and $N := \langle\beta\rangle$ be two cyclic permutation groups on the set $\Omega = \{1, 2, \dots, 2p\}$, where $\alpha = (1\ 2 \dots 2p)$ is a cycle of length $2p$ and $\beta = (1\ 3)(4\ 2p)\dots(p{+}1\ p{+}3)$ is $(p-1)$ cycles of length 2. It is straightforward to verify that $G = D_{2n} \cong \langle M, N\rangle$. Since $M \leqslant G$ act transitively on a set Ω, so G is a transitive permutation group on a set Ω. Suppose now that $M_1 \subset M$ consists precisely of those elements whose form is a cycle of length $2p$, $M_2 \subset M$ consists precisely of those elements whose form is two cycles of length p and $M_3 \subset M$ consists precisely of those elements whose form is p cycles of length 2. Consequently, M_1, M_2 and M_3 are a partition of $M \setminus \{1\}$. By Lemma 3.2, every element of M_1 and M_3 has the movement equal to p and every element of M_2 has the movement equal to $p-1$ and also $\mathrm{move}(\beta) = p-1$. Let $1 \neq g \in G$, $g \notin M$ and $g \notin N$. Then either $g \in M_1\beta$ or $g \in M_2\beta$ and or $g \in M_3\beta$. If $g \in M_1\beta$ or $g \in M_3\beta$, then g has p cycles of length 2, that is, $\mathrm{move}(g) = p$. If $g \in M_2\beta$, then g has $(p-1)$ cycles of length 2, that is, $\mathrm{move}(g) = p-1$. These implies that every non-identity element of G has movement p or $p-1$. $\square$

Let H be cyclic of order n and $K = \langle k\rangle$ be cyclic of order m and suppose r is an integer such that $r^m \equiv 1 (\mathrm{mod}\ n)$. For $i = 1, \dots, m$, let $(k^i)\theta : H \to H$ be defined by $h^{(k^i)\theta} = h^{r^i}$ for h in H. It is straightforward to verify that each $(k^i)\theta$ is an automorphism of H, and that θ is a homomorphism from K to $\mathrm{Aut}(H)$. Hence the semi-direct product $G = H \rtimes K$ (with respect to θ) exists and if $H = \langle h\rangle$, then G is given by the defining relations:

$$h^n = 1, \quad k^m = 1, \quad k^{-1}hk = h^r, \quad \text{with } r^m \equiv 1 (\mathrm{mod}\ n).$$

Here every element of G is uniquely expressible as $h^i k^j$, where $0 \le i \le n-1$, $0 \le j \le m-1$. Certain semi-direct products of this type (as a permutation group on a set Ω of size n) also provide examples of transitive permutation groups where every non-identity element has the movement m or $m-1$, and the bound in Lemma 1.1, is not attained (as the following lemma). We note that, if $n = q$, a prime, then by [15, Theorem 3.6.1] this group G is a subgroup of the Frobenius group $AGL(1, q) = \mathbb{Z}_q \rtimes \mathbb{Z}_{q-1}$.

LEMMA 3.4. *Let G be a semi-direct product of the Frobenius group $G = \mathbb{Z}_q \rtimes \mathbb{Z}_{q-1}$, where $q := 2p+1$ is an odd prime, denote a group defined as above of order $q(q-1)$. Then G act transitively on a set of size $n = q$ and in this action every non-identity element has movement p or $p-1$.*

Proof. By the above statement, the group G is a Frobenius group and has up to a permutational isomorphism a unique transitive representation of degree q on a set Ω. Let $g \in G$; $o(g) = q$. If $\Gamma(g)$ consists of every second point of the unique cycle of g, then $\mathrm{move}(g) = \frac{q-1}{2} = p$. Since the order of each element of G is either $2, p, q$ or $2p$, so by Lemma 3.2, every non-identity element has movement p or $p-1$. $\square$

Now, we are ready to complete the proof of the main theorem:

Let G, Ω and m be as in Theorem 1.2 with $n := |\Omega|$ and $\mathrm{move}(G) = m$. Now, we consider two cases:

Case 1. n is the maximum possible degree as in Lemma 1.1.

A transitive permutation group of degree $3m$ (which is the bound of Lemma 1.1, for $p = 3$) with bounded movement equal to m, were classified in [10] and the examples are as follows:

(a) $G = S_3, m = 1$;

(b) $G = A_4$ or $A_5, m = 2$;

(c) G is a 3-group of exponent 3.

It can be easily verified that the movements of all of these groups are not two consecutive integers, which contradicts our hypothesis.

But for $p \geq 5$, by [7, Theorem 1.2], one of the following holds:

(1) $|\Omega| = p, m = (p-1)/2$ and $G = \mathbb{Z}_p \rtimes \mathbb{Z}_{2^a}$, where $2^a|(p-1)$ for some $a \geq 1$;

(2) $|\Omega| = 2^s p$, $m = 2^{s-1}(p-1)$, $1 < 2^s < p$, and $G = K \rtimes P$ with K a 2-group and $P = \mathbb{Z}_p$ is fixed point free on Ω; K has p-orbit of length 2^s, and each element of K moves at most $2^s(p-1)$ point of Ω;

(3) G is a p-group of exponent bounded in terms of p only.

By [2, Theorem 1.1], all group in part (1), part (3) and the part (2), when p is a Mersenne prime and each non-identity element of K moves exactly $2^s(p-1)$ point of Ω, are examples in which every non-identity element has the same movement equal to m. We will show that the other groups in part (2) have some elements whose movement are less than $m-1$, which contradicts our hypothesis. In part(2), with $s \geq 2$, when p is not a Mersenne prime and each element of K moves at most $2^s(p-1)$ point of Ω, since every non-identity element of $G = K.P$ has movement m or $m-1$, there exist $k \in K$ with $(p-1)$ cycles of length 2^s. We consider the element kk^g of K. This element is fixed point free on Ω and so has movement $p.2^{s-1}$, which is a contradiction. Also, for $s = 1$, according to the [7, Lemma 3.3] we can easily achieve the same contradiction.

Case 2. n is not the maximum possible degree as in Lemma 1.1.

By Proposition 2.2, each non-trivial permutation of G in its disjoint cycle representation has either a cycle of length $2p$, a cycle of length 9, a cycle of length 2 and a cycle of length 3, a cycle of length 3 and a cycle of length 6, $(s-1)$ cycles of length a power of 2 and a cycle of length 2 for $s \geq 2$, multiple cycles of length p, or multiple cycles of length a power of 2, namely g_{2p}, g_9, $g_{2,3}$, $g_{3,6}$, $g_{2^a,2}$, g_p, g_{2^a}, respectively.

If G consists precisely of those elements whose form is g_{2^a} or g_p, then by [2], n is the maximum possible except the case when the groups S_4, A_4 and

A_5 act transitively on a set of size 4 and 5, respectively. We may only consider some of the cases which are satisfy in our assumptions. For example, if G is a cyclic group generated by g_{2p} or g_9, then by Lemma 3.1 and Lemma 3.2, we have $G = \mathbb{Z}_{2p}$ or $\mathbb{Z}_9$. If G consists precisely of those elements whose form is either g_9, g_p, or g_{2^a}, then it can be easily verified that $G = D_{18}$. If G consists precisely of those elements whose form is either g_{2p}, g_p or g_{2^a}, then G is the groups as in Lemma 3.3 and Lemma 3.4. Finally, if G consists precisely of those elements whose form is either $g_{2,3}$, g_{2^a} or g_p, then it can be easily shown that $G = S_5$. These completes the proof of Theorem 1.2. $\square$

REFERENCES

[1] M. Alaeiyan, *Improvement on the bounds of permutation groups with bounded movement.* Bull. Aust. Math. Soc. **67** (2003), 246–257.
[2] M. Alaeiyan and H.A. Tavallaee, *Permutation groups with the same movement.* Carpathian J. Math. **25** (2009), 147–156.
[3] M. Alaeiyan and S. Yoshiara, *Permutation groups of minimal movement.* Arch. Math. **85** (2005), 211–226.
[4] R. Brandl, *Finite groups all of whose elements are of prime power order.* Bull. U. M. I. **5** (1981), 491–493.
[5] J.R. Cho, P.S. Kim and C.E. Praeger, *The maximal number of orbits of a permutation groups with bounded movement.* J. Algebra **214** (1999), 625–630.
[6] B. Fein, W. Kantor and M. Schacher, *Relative Brauer groups.* J. Reine Angew. Math. **328** (1981), 39–57.
[7] A. Hassani, M. Alaeiyan (Khayaty), E.I. Khukhro and C.E. Praeger, *Transitive permutation groups with bounded movement having maximal degree.* J. Algebra **214** (1999), 317–337.
[8] G. Higman, *Finite groups in which every element has prime power order.* J. Lond. Math. Soc. **32** (1957), 335–342.
[9] B. Huppert, *Endliche Gruppen* I. Springer-Verlag, Berlin–New York, 1967.
[10] A. Mann and C.E. Praeger, *Transitive permutation groups of minimal movement.* J. Algebra **181** (1996), 903–911.
[11] C.E. Praeger, *On permutation groups with bounded movement.* J. Algebra **144** (1991), 436–442.
[12] C.E. Praeger, *Movement and separation of subsets of points under group action.* J. Lond. Math. Soc. **56**(2) (1997), 519–528.
[13] J.J. Rotman, *An Introduction to the Theory of Groups.* 3rd ed., Allyn and Bacon, Boston, 1984.
[14] M. Suzuki, *On a class of doubly transitive groups.* Ann. of Math. **75** (1962), 105–145.
[15] T. Tsuzuku, *Finite Groups and Finite Geometries.* Cambridge University Press, 1982.

Received 8 March 2011

Karaj Branch, Islamic Azad University
Department of Mathematics
Karaj, Iran
alaeiyan@iust.ac.ir
bahman_askari2003@yahoo.com