PERMUTATION GROUPS WITH BOUNDED MOVEMENT ATTAINING THE BOUNDS FOR ODD PRIMES

A. Hassani and M. Khayaty

Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran 16844, Islamic Republic of Iran

Abstract

Let G be a transitive permutation group on a set Ω and let m be a positive integer. If no element of G moves any subset of Ω by more than m points, then $|\Omega| \leqslant [2mp/(p-1)]$ where p is the least odd prime dividing $|G|$. When the bound is attained, we show that $|\Omega| = 2^{\alpha}p^{r}q_1^{\beta_1} \dots q_n^{\beta_n}$ where α is a non-negative integer with $2^{\alpha} < p$, $r \geqslant 1$ and q_i is a prime satisfying $p < q_i < 2p$, $\beta_i = 0$ or 1, $1 \leqslant i \leqslant n$. Furthermore, every 2-element of G fixes at least $[2m/(p-1)]$ points and each q_i-element of G fixes at least $[2m(q_i-p)/(p-1)(q_i-1)]$ points. Finally, we prove that if G is a p-group of exponent, at least p^2 and $|\Omega| = [2mp/(p-1)]$, then every fixed point free element of G has order p.

1. Introduction

Let G be a permutation group on a set Ω with no fixed points, and let m be a positive integer. For a subset Γ of Ω if the size of $|\Gamma^g - \Gamma|$ is bounded, for $g \in G$, we define the movement of Γ as $\mathbf{mov}(\Gamma) = \operatorname{Max}_{g \in G} |\Gamma^g - \Gamma|$. If $\mathbf{mov}(\Gamma) \leqslant m$ for all $\Gamma \subseteq \Omega$, then G is said to have bounded movement, and the movement of G is defined as the maximum of $\mathbf{mov}(\Gamma)$ over all subsets Γ of Ω. This notion was introduced in [1]. By [1, Theorem 1], if G has bounded movement m, then Ω is finite. Moreover, the number t of G-orbits in Ω is at most $2m-1$, and each G-orbit has a length at most $3m$, further $|\Omega| \leqslant t+3m-1$. In particular $|\Omega| \leqslant 5m-2$, and if G is transitive, then $|\Omega| \leqslant 3m$. Assume that G is not a 2-group, then by [1, Lemma 2.2], we have the following lemma.

Lemma 1.1. Let G be a transitive permutation group on a set Ω such that G has bounded movement equal to m. Suppose that G is not a 2-group and let p be the least odd prime dividing $|G|$. Then $|\Omega| \leqslant [2mp/(p-1)]$. (For $x \in R$, $[x]$ denotes the least integer greater than or equal to x).

Let us first consider the case of transitive groups of degree $[2mp/(p-1)]$ with movement bounded by m. There are various ways in which the bounds in Lemma 1.1 may be attained, and later we show that there are examples of transitive permutation groups of degree $[2mp/(p-1)]$ with movement bounded by m when $|\Omega| = p^r$ where $r \geqslant 1$. We are looking for an example of a group with movement bounded by m and in which $|\Omega|$ is divisible by a prime q or 2^{α} such that $q > p$ and $2^{\alpha} < p$ for $\alpha \geqslant 1$. Looking for these groups we have found the following result.

Theorem 1.2. (a) Any transitive permutation group of degree $2mp/(p-1) = p^r \geqslant p$ which has exponent p has bounded movement equal to m.

(b) Let G be a transitive permutation group of degree $[2mp/(p-1)]$ with bounded movement equal to m, where p

Keywords: Bounded movement; Permutation group; Transitive

is the least odd prime dividing $|G|$. Then $|\Omega| = 2^{\alpha} p^{r} q_1^{\beta_1} \dots q_n^{\beta_n}$ where α is a non-negative integer such that $2^{\alpha} < p$, $r \geqslant 1$, and q_i is a prime satisfying $p < q_i < 2p$, $\beta_i = 0$ or $1, 1 \leqslant i \leqslant n$.

(c) If G satisfies condition (b), then every 2-element of G fixes at least $[2m/(p-1)]$ points and every q_i-element of G fixes at least $[2m(q_i-p)/(p-1)(q_i-1)]$ points, $1 \leqslant i \leqslant n$.

Let $1 \neq g \in G$ be such that $g = (a_1 a_2 \dots a_{l_1})(b_1 b_2 \dots b_{l_2}) \dots (b_1 b_2 \dots b_{l_n})$. We can take the $[(l_i)/2]$ points α_{2j-1}, $1 \leqslant j \leqslant [(l_i)/2]$ from each cycle, that is, $\Gamma(g) = \{a_2, a_4, \dots, b_2, b_4, \dots, z_2, z_4, \dots\}$. Then we say that $\Gamma(g)$ consists of "every second point" of every cycle of g. Also, $\Gamma(g)$ satisfies $\Gamma(g)^g \cap \Gamma(g) = \phi$. It is obvious if G has bounded movement m, then $|\Gamma(g)| \leqslant m$.

For every positive integer n, we construct a permutation group of degree n with movement bounded by $[n(p-1)/2p]$ and with t orbits, in this case p is a possible bound for t.

The main aim of this paper is a generalization of Theorems in [1] and [2] for primes greater than 3. These are the types of works which were mentioned in [6].

2. Attaining the Bounds

Let G be a transitive permutation group on a finite set Ω. Then by [4, Theorem 3.26], 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. By proving the next Lemma, we find a general method to bound $|\Gamma^g - \Gamma|$.

Lemma 2.1. Let G be a permutation group on a set Ω and suppose that $\Gamma \subseteq \Omega$. Then for each $g \in G$ such that $g = c_1 c_2 \dots c_t$ the product of t disjoint cycles, $|\Gamma^g - \Gamma| \leqslant \sum_{i=1}^{t} [(l_i)/2]$ where l_i is the length of each cycle c_i of g, $1 \leqslant i \leqslant t$.

Proof. Let $g \in G$. Write g as a product of t disjoint cycles $c_1 c_2 \dots c_t$, where $c_i = (a_{i1} \dots a_{il_i})$, $1 \leqslant i \leqslant t$. We consider the sets $\overline{C_i} = \{a_{i1} \dots a_{il_i}\}$. Set $\Gamma_i = \Gamma \cap \overline{C_i}$, $1 \leqslant i \leqslant t$ and $\Gamma_{t+1} = \Gamma \cap \text{fix}(g)$. Then $\Gamma_i^g \subseteq \overline{C_i}^g$ thus, $\Gamma^g = \Gamma_1^g \cup \Gamma_2^g \cup \dots \cup \Gamma_t^g \cup \Gamma_{t+1}$.

It follows, $(\Gamma^g - \Gamma) = (\Gamma_1^g - \Gamma_1) \cup (\Gamma_2^g - \Gamma_2) \dots \cup (\Gamma_t^g - \Gamma_t)$. Select every second point of every cycle c_i of g. Clearly each l_i-cycle of g has at most $(l_i/2)$ points in Γ_i if l_i is even, and $(l_i - 1)/2$ points in Γ_i if l_i is odd, in any case $(\Gamma_i^g - \Gamma_i)$ has at most $[(l_i)/2]$ points. Hence $|\Gamma^g - \Gamma| \leqslant \Sigma_{i=1}^{t} [(l_i)/2]$.■

Lemma 2.2. Let $m = p^{a-1}(p-1)/2$ for some $a \geqslant 1$, where p is an odd prime, and suppose that G is a transitive permutation group of exponent p on a set Ω of size $p^a = 2mp/(p-1)$. Then Ω has bounded movement equal to m.

Proof. Let $1 \neq g \in G$ and let $\Gamma \subseteq \Omega$. For each cycle C of g of length p, $(\Gamma \cap C)^g - (\Gamma \cap C)$ has size at most $(p-1)/2$. Thus $|\Gamma^g - \Gamma|$ is at most the number of cycles of g of length p times $(p-1)/2$, that is $|\Gamma^g - \Gamma| \leqslant (|\Omega|/p).(p-1)/2 = m$. Thus G has movement at most m. Moreover, since G is transitive, then G contains a fixed point free element. For this element g, a subset $\Gamma(g)$ consisting of "every second point of every cycle g" has size m and $\Gamma(g)^g \cap \Gamma(g) = \phi$. Thus the movement of G is equal to m.■

The following Theorem, which is a generalization of Theorem 2 in [2], shows that possible values of $|\Omega|$ are highly restricted. We note that if $q < p$ is an odd prime divisor of $|\Omega|$ $(p \geqslant 5)$, since p is the least odd prime dividing $|G|$, then q certainly does not divide the order of G.

Theorem 2.3. Let G be a transitive permutation group on a set Ω of degree $[2mp/(p-1)]$ with movement bounded by m, where p is the least odd prime dividing $|G|$. Then $|\Omega| = 2^{\alpha} p^{r} q_1^{\beta_1} \dots q_n^{\beta_n}$ in which α is a non-negative integer such that $2^{\alpha} < p$, $r \geqslant 1$, q_i is a prime satisfying $p < q_i < 2p$ and $\beta_i = 0$ or 1, $1 \leqslant i \leqslant n$.

Proof. Let q be a prime dividing $|\Omega|$, and let P be a Sylow q-subgroup of G. For each $g \in P$, write g as a product of disjoint cycles and define $\Gamma(g)$, to be the set of every second point of every cycle of g. Let $|\text{fix}(g)|$ and O denote the number of fixed points (1-cycles) and the number of odd cycles (of length $\geqslant q$) of g. If q is odd, then each k-cycle of g contributes $(k-1)/2$ points to $\Gamma(g)$; and since $k \geqslant q$ we have $O.(q-1)/2 \leqslant |\Gamma(g)| \leqslant m$. For any q, g moves $(|\Omega| - |\text{fix}(g)|)$ points and $|\Gamma(g)| = (|\Omega| - |\text{fix}(g)| - O)/2 \leqslant m$; so $(|\Omega| - 2m) \leqslant |\text{fix}(g)| + O$.

For each $g \in P$ we have $|\text{fix}(g)| \geqslant (|\Omega| - 2m - O)$. When $q = 2$, O is zero, so $|\text{fix}(g)| \geqslant (|\Omega| - 2m)$ and the average number of fixed points of elements in p is $\geqslant (|\Omega| - 2m)$. When q is odd we have $O \leqslant 2m/(q-1)$, so the average number of fixed points of elements in P is $\geqslant (|\Omega| - 2m - 2m/(q-1))$. But the average number of fixed points of elements in P is equal to the number of P-orbits. Let q^a be the highest power of q which divides $|\Omega|$. Then each P-orbit has length $\geqslant q^a$, so P has at most $|\Omega|/q^a$ orbits. Hence $|\Omega|/q^a \geq (|\Omega| - 2m)$ when $q = 2$ and $|\Omega|/q^a \geqslant (|\Omega| - 2m - 2m/(q-1))$ when q is odd. The result follows.■

The existence of transitive permutation groups of degree $[2mp\ (p-1)]$ with movement bounded by m when $m > 2$ and $|\Omega|$ is not a power of p is not completely settled. We have the following information when $|\Omega|$ is even.

Lemma 2.4. Let G be a transitive permutation group on Ω of degree $[2mp/(p-1)]$ with movement bounded by m where $|\Omega|$ is even and p is the least odd prime dividing $|G|$. Then $|\Omega|$ is divisible by 2^a, for some $a \geqslant 1$ such that $2^a \leqslant p$ and every 2-element of G fixes at least $[2m/(p-1)]$ points.

Proof. Let $g \in G$ have order a power of 2, and let $\Gamma(g)$ consist of "every second point of every cycle of g". Then $\Gamma(g)$ is mapped by g to a set disjoint from $\Gamma(g)$ and hence $|\Gamma(g)| \leqslant m$. Thus $|\text{supp}(g)| \leqslant 2m$, where $\text{supp}(g) = \{a | a^g \neq a\}$. Consequently, $|\text{fix}(g)| \geqslant |\Omega| - 2m = [2m/(p-1)]$. Hence g fixes $[2m/(p-1)]$ points. The first part of the Lemma follows from the previous Theorem.■

We complete the proof of Theorem 1.2, by considering transitive groups of degree $[2mp(p-1)]$ with movement bounded by m, with $|\Omega|$ divisible by a prime greater than p.

Lemma 2.5. Let G be a transitive permutation group on a set Ω of $[2mp\ (p-1)$ points with movement bounded by m where p is the least odd prime dividing $|G|$. Then $|\Omega|$ is not divisible by q^2 where q is a prime satisfying $p < q < 2p$, neither by a prime greater than $2p$. If q satisfies $p < q < 2p$, such that divides $|\Omega|$, then $|\Omega| > q$ and every q-element in G fixes at least $[2m(q-p)/(p-1)(q-1)]$ points. Also, if $m > 1$ then G contains a p-element with no fixed points.

Proof. The first part follows from Theorem 2.3. Let q be a prime greater than p such that $q | |G|$ and let g be a q-element of G. Then by Theorem 2.3, $|\text{fix}(g)| \geqslant |\Omega| - 2m - 2m/(q-1)$. Hence we have $|\text{fix}(g)| \geqslant [2m(q-p)/(p-1)(q-1)]$. If $|\Omega| = q$ then, as the number of fixed points of a q-element is a multiple of q, each q-element fixes at least q points. It follows that $q < t_p \leqslant |\Omega|/q$ (where t_q is the number of orbits of a Sylow q-subgroup of G), which is a contradiction. Thus $|\Omega| > q$.

Finally, let $m > 1$. To establish that G contains a p-element with no fixed points we must use [3] which proves that G contains a fixed point free q-element for some prime q. By Lemma 2.4 and the argument above, q must be p.■

Question 1. Let p be the least odd prime dividing $|G|$ and m a positive integer. Is there a transitive permutation group of degree $[2mp/(p-1)]$ with movement bounded by m when $|\Omega|$ is divisible by a prime q satisifying $p < q < 2p$?

Now we shall consider intransitive groups with movement bounded by m which have t orbits and degrees close to $t + [2mp/(p-1)] - 1$. Let n be a positive integer, we construct such a group with m close to $[n(p-1)/2p]$.

Theorem 2.6. Let n be a positive integer. There is a permutation group of degree n with movement bounded by $[n(p-1)/2p]$ and with t orbits, where t is the sum of the coefficients of terms in the p-adic expansion of n (that is, $n = \sum_{i \geq 0} a_i p^i$ with each a_i equal to 0,1... or p-1 then $t = \sum a_i$).

Hence if $t - a_0$ is 1,2,... or p, then there is a permutation group of degree n with t orbits which has movement bounded by $[(p-1)(n-t+1)/2p]$.

Proof. Let $n = \sum_{i \geq 0} a_i p^i$ where each a_i is 0,1,... or p-1, and set $t = \sum a_i$. For each i, if $a_i > 0$, let $\Omega_{i1}, \ldots \Omega_{ia_i}$ be sets of size p^i and let Ω be the disjoint union of all the Ω_{ij}. For each Ω_{ij} let G_{ij} be the trivial permutation group on Ω_{ij} if $i = 0$, and a transitive permutation group of exponent p on Ω_{ij} if $i > 0$, and consider the direct product $G = \Pi G_{ij}$ of the G_{ij} acting on Ω with the sets Ω_{ij} as orbits. Let $\Gamma \subseteq \Omega$ and $1 \neq g \in G$. Then, arguing as in Lemma 2.2, $|\Gamma^g - \Gamma|$ is at most $(|\Omega|/p).(p-1)/2$, that is, $|\Gamma^g - \Gamma| \leqslant [n(p-1)/2p]$. Thus G has movement bounded by $[n(p-1)/2p]$ and has t orbits. We have $[n(p-1)/2p] = [(p-1)(n-t+1)/2p]$ if and only if $\sum_{i \geq 1} a_i$ is 1,2,... or p.■

The above Theorem contains a construction of such a group if p divides n and the p-adic expansion of n satisfies $1 \leqslant \sum_{i \geq 1} a_i \leqslant p$. The number t of nontrivial orbits in the construction is the sum of the coefficients of terms of the p-adic expansion, that is, $t = \sum_{i \geq 1} a_i$, and so the greatest value of t for this family is p.

Question 2. For which positive integers n is there a positive integer t and a permutation group G on a set of size n with t nontrivial orbits such that G has bounded movement equal to $[(p-1)(n-t+1)/2p]$?

3. Minimal Movement for Transitive Permutation Groups

In [5], transitive groups of degree $3m$ with movement bounded by m have been classified as follows:

Theorem 3.1. Let G be a transitive permutation group on a set Ω of size $3m$ such that G has movement m. Then either G is of exponent 3, or G is one of S_3, A_4 or A_5 of degree 3,6 and 6 respectively.

We are trying to generalize the above Theorem for transitive groups of degree $[2mp/(p-1)]$, where p is the smallest odd prime dividing $|G|$. As a first step for this goal we have found some information about Ω in Theorem 2.3. For example, according to Theorem 2.3 when $p = 5$ we have $|\Omega| = 2^a 5^r 7^\beta$, where $r \geqslant 1$, $a = 1$ or 2, and $\beta = 0$ or 1. It is clear that $|\Omega| = [5m/2]$ is of the form $2^a 5^r 7^\beta$ if m is even. For $m = 2$ we have $|\Omega| = 5$. In this case the transitive groups of degree 5 with movement bounded by 2 are z_5, z_5

$\times z_2$ and $z_5 \times z_4$. We hope to classify all transitive permutation groups of degree $[2mp/(p-1)]$ with movement bounded by m. Now we consider a transitive permutation group G on a set Ω of size $p^r (r \geqslant 1)$. If P is a Sylow p-subgroup of G, then by [7, Lemma 3.4] p^r divides the length of each P-orbit, that is, $|\alpha^P|$. Hence, $\alpha^P = \Omega$. It follows that P is transitive.

Proposition 3.2. If G is any group of exponent p, and $H \leqslant G$ with $H \cap Z(G) = 1$, then G acts transitively and faithfully on the cosets of H and has movement bounded by $(p^{a-1}(p-1)/2)$ for some $a \geqslant 1$, where $|G{:}H| = p^a$.

Proof. Let G be a group of exponent p, and $H \leqslant G$ with $H \cap Z(G) = 1$. Suppose Ω is the set of all right cosets of H in G. Then G acts on Ω by right multiplication.

It is obvious that this action is transitive. We know that the kernel of this action is core (H). If core $(H) \neq 1$, then, as core (H) is a normal subgroup of G and G is a p-group, we have,

$$1 \neq \text{core}(H) \cap Z(G) \subseteq H \cap Z(G)$$

which is a contradiction. Thus core $(H) = 1$. It follows that G acts transitively and faithfully on Ω. By Lemma 2.2, G has movement bounded by $(p^{a-1}(p-1)/2)$.■

Now we answer positively the open question posed in [5] after proposition 2. Let G be a transitive permutation group on a set Ω of size $[2mp/(p-1)]$, with movement bounded by m. Then we have the following Theorem.

Theorem 3.3. Let G be a transitive permutation group on a set Ω with movement m, and suppose that G is a p-group of exponent at least p^2, for some $p \geqslant 5$. Then all the elements of G which are fixed point free on Ω have order p.

Proof. Since G is a transitive p-group, then we have $|\Omega|\,|$ $|G|$. Let $|\Omega| = p^t$, where $t > 1$ and suppose that g is a fixed point free element of G. Then we show that any cycle of g has length p. Assume on the contrary, that there are r_i cycles of length p^{s_i} ($s_i \geqslant 2$) in the decomposition of g to the disjoint cycles where $1 \leqslant i \leqslant n$.

Let $\Gamma(g)$ be the set consisting of every second point of every cycle of g. Then by Lemma 2.1,

$$|\Gamma(g)| = \sum_{i=1}^{n} r_i(p^{s_i} - 1)/2 + ((p^t - \sum_{i=1}^{n} r_i p^{s_i})/p) \cdot (p-1)/2$$

Since G has bounded movement equal to m, we have $|\Gamma(g)| \leqslant m (= p^{t-1}(p-1)/2)$. Hence

$$\sum_{i=1}^{n} r_i(p^{s_i} - 1)/2 + ((p^t - \sum_{i=1}^{n} r_i p^{s_i})/p) \cdot (p-1)/2 \leqslant p^{t-1}(p-1)/2$$

This inequality implies $\Sigma_{i=1}^{n} r_i \, (p^{s_i - 2} + \ldots 1) \leqslant 0$ which is absurd. The result now follows.■

Now we conclude this section by posing the following conjecture.

Conjecture. Let G be a transitive permutation group on a set Ω with movement m and suppose that G is a p-group, where p is a prime at least 5. If all the elements of G which are fixed point free on Ω have order p, then G has exponent p.

Acknowledgements

The authors would like to thank Professor C. E. Praeger for pointing out this problem to them and for useful conversations. We specially thank her for showing us examples in Lemma 2.2, which helped us in the improvement of our paper. The first author would like to thank the Institute for Studies in Theoretical Physics and Mathematics for partial support.

References

1. Praeger, C.E. Movement and separation of subsets of points under group actions. *J. London Math. Soc.*, (to appear).
2. Gardiner, A. and Praeger, C.E. Transitive permutation groups with bounded movement. *J. Algebra*, **168**, 798-803, (1994).
3. Fein, B., Kantor, W.M. and Schacher, M. Relative Brauer Groups. II. *J Reine Angew. Math*, **328**, 39-57, (1981).
4. Rotman, J.J. *An introduction to the theory of groups*, (3rd edn). Allym and Bacon, (1984).
5. Mann, A. and Praeger, C.E. Transitive permutation groups of minimal movement. *J. Algebra*, 181, 903-911, (1996).
6. Praeger, C.E. The separation theorem for group actions. In *Ordered groups and infinite permutation groups*, (ed. W. C. Holland), pp. 195-219. Kluwer, Dordrecht, (1996).
7. Wielandt, H. *Finite permutation groups*. New York Academic Press, (1964).