数理解析研究所講究録
325巻 1978年 143-150

Report on a 1 hour talk at the Kyoto Permutation Groups Meeting, January, 1978.

Elements of prime order in primitive permutation groups.

Cheryl E. Praeger

In 1873 C. Jordan, and at the beginning of this century W.A. Manning investigated certain properties of an element of prime order in a primitive group which is not alternating or symmetric. They found that the number of fixed points of such an element is bounded by a function of the number of its cycles of prime length, provided that the number of cycles is small. Let us make the following assumptions.

(*) G is a primitive permutation group of degree n, and $G \not\geq A_n$. G contains an element of prime order p, where p divides $|G|$, which has q cycles of length p and $f = n - qp$ fixed points.

In 1873 and 1875 Jordan [2,3] showed (or claimed) that if $1 \leq q \leq 5$ and $q < p$ then $f \leq q + 1$. The proof for $q > 1$ was not published however until early this century, when Manning [4] I,II, published a proof of the result and obtained better bounds for f if $2 \leq q \leq p - 2$. In 1928 M. Weiss [11] obtained similar bounds for $q \in \{6,7\}$, $q < p$, and very recently Jan Saxl [8,9] improved Manning's bounds in the cases $q = 4$ and $q = 5$.

Now Manning was interested in finding a bound for f for a larger range of values of q. His first result in this direction was obtained in 1911 when he showed [5] that if $q \leq 2p + 3$ and G is not 2-transitive then $f \leq \max\{q^2 - q, 2q^2 - p^2\}$.

This bound is too large to be useful in practice although there are examples in which the value of f differs from this bound only by a small constant multiple. (If G is A_c or S_c permuting the set of $n = c(c-1)/2$ unordered pairs of distinct points, where $c = (5p + 7)/2$, then G is a simply transitive primitive group which contains an element of order p with $2p + 3$ cycles of length p and $f = (9p^2 + 36p + 35)/8$ fixed points, while the bound for f is $2q^2 - p^2 = 7p^2 + 24p + 18$.) Manning's main result [4] III was published in 1918 and gave very useful bounds on f as well as limiting the p-part of $|G|$. We state it below.

<u>Theorem 1.</u> (Manning) If (*) is true and $5 < q \leq (p + 1)/2$ then $f \leq 4q - 4$ and $|G|$ is not divisible by p^2. Moreover if G is not 2-transitive then $f \leq 4q - 7$.

It is easily checked that if $1 \leq q \leq 4$ and $q < p$, then again $|G|$ is not divisible by p^2. Thus if $1 \leq q \leq (p + 1)/2$ we have a good bound both on the degree of G and on the p-part of the order of G. One might ask if these bounds can be extended for larger values of q, and indeed a partial answer was given a few years ago by Michael O'Nan and myself in [6,7].

<u>Theorem 2.</u> (O'Nan, Praeger) If (*) is true and $q < p$ then one of the following is true.

(a) p^2 does not divide $|G|$.

(b) $ASL(2,p) \leq G \leq AGL(2,p)$, and G permutes the $n = p^2$ points of an affine plane of order p.

(c) $G = P\Gamma L(2,8)$ of degree $n = p^2 = 9$.

A similar result has been proved for $q \leq 2p - 2$, (see [7] II). The problem of extending Manning's bound on the number of fixed points f, even for the case $q < p$, is more difficult since the bound $f \leq 4q - 4$ does not hold in general. Indeed if $G = A_c$ or S_c permuting the $n = c(c - 1)/2$ unordered pairs of distinct points, where $p \leq c \leq (3p - 1)/2$, then G is a simply transitive primitive group which contains an element of order p with $q = c - (p + 1)/2$ cycles of length p, where $(p - 1)/2 \leq q < p$, and $f = ((p^2 - 1)/4 - q(p - q))/2$ fixed points, (and if $c = (3p - 1)/2$ then $f = q(q - 2)/8$.) I have been able to show very recently that these are the only groups which prevent Manning's bound holding for $q < p$, at least for simply transitive groups.

Theorem 3. If (*) is true, G is not 2-transitive, and $2 < q < p$, then p^2 does not divide $|G|$ and either $f \leq 4q - 7$, or G is A_c or S_c permuting the $n = c(c - 1)/2$ unordered pairs of distinct points, where $c = q + (p + 1)/2$.

By using an argument shown me by Peter M. Neumann together with the result above a similar bound can be obtained for 2-transitive groups.

Theorem 4. If (*) is true, G is 2-transitive, and $2 < q < p$, then $f \leq 4q - 3$.

It may be possible to reduce the bound on f in the 2-transitive case. (Notice that I have stated the results for $q > 2$, for the bounds of Jordan and Manning for $q = 3,4,5$ are even better than $4q - 7$.)

Discussion of the proof of Theorem 3.

Theorem 3 is proved by induction on the degree of G. The result for $p \le 7$ follows from the results of Jordan, Manning and Weiss, so we may assume that $p \ge 11$. We may use Jordan's or Manning's results to start the induction, so we assume that G is a group satisfying (*) which is not 2-transitive and is such that $2 < q < p$, and we assume inductively that the theorem is true for groups of degree less than n. Let A be a subgroup of G of order p, degree qp, and with f fixed points. Without loss of generality we may assume that $f > 0$, so suppose that α is a point fixed by A. By Theorem 2 A is a Sylow p-subgroup of G, and hence of G_α. If Γ is an orbit of G_α in $\Omega - \{\alpha\}$ then by [12] 18.4, A acts nontrivially on Γ. Thus G_α^Γ is a transitive group of degree $|\Gamma| < n$ with a subgroup A^Γ of order p and degree less than p^2. The next step is to find a primitive representation of degree less than n associated with this representation which either satisfies (*) or is alternating or symmetric. Suppose that A has q' orbits of length p and f' fixed points in Γ.

Lemma Associated with G_α^Γ is a primitive permutation group X of degree x, where $|\Gamma| = xy$, which contains an element of order p and degree $(q'/y)p$ with f'/y fixed points, for some $y \ge 1$.

Proof Let M be the largest normal subgroup of G_α such that $|G_\alpha:M|$ is not divisible by p, and let Σ be the set of M-orbits in Γ. Then Σ is a set of blocks of imprimitivity for G_α^Γ and $|\Sigma|$ is maximal such that $A^\Sigma = 1$, (for $A \subseteq M$). Let $B \in \Sigma$ and let H be the setwise stabilizer of B in G_α, (possibly $B = \Gamma$). Let $D \subset B$, $D \neq B$, be a block of imprimitivity for H^B such that $|D|$ is maximal, (possibly $|D| = 1$).

.../5

Then D is a block of imprimitivity for G_α^Γ . Let $\Delta = \{D^g; g \in G_\alpha\}$ and let $\Delta(B) = \{D^g; g \in H\}$.

Set $X = H^{\Delta(B)}$. Then by the maximality of $|D|$, X is a primitive group of degree $|\Delta(B)| = x$ say where $|\Gamma| = x|D|\cdot|\Sigma|$. By the maximality of $|\Sigma|$, A acts nontrivially on Δ , and as $q' < p$ it follows that A permutes $q'p/|D|$ elements of Δ and fixes $f'/|D|$ elements of Δ pointwise. Moreover as A is a Sylow p-subgroup of M , A permutes the same number of points in each element of Σ , and it follows that A permutes $q'p/|D|\cdot|\Sigma|$ elements of $\Delta(B)$ and fixes $f'/|D|\cdot|\Sigma|$ elements of $\Delta(B)$. Since $|\Gamma| = x|D|\cdot|\Sigma|$, the lemma is proved.

Before proceeding we note that $M^{\Delta(B)}$ is a transitive normal subgroup of X .

If $q'/y = 1$ then by Jordan's result either $f'/y \le 2$ or $X \supseteq A_x$, and in the latter case clearly $M^{\Delta(B)} \supseteq A_x$ so that A_x is a composition factor of G_α . If $2 \le q'/y \le (p + 1)/2$ then by Jordan's and Manning's results, $f'/y \le 4(q'/y) - 4$, (for $X \not\supseteq A_x$ since p^2 does not divide $|X|$) . Finally if $q'/y \ge (p + 3)/2$, then since $q' \le q < p$, $y = 1$ and so $X = G_\alpha^\Gamma$ is primitive. Since $q' > q/2$ this situation can arise for at most one orbit of G_α . Moreover since the number of nontrivial orbits of A in an orbit Γ' of G_α other than Γ is at most $q - q' \le (p - 1) - (p + 3)/2 \le q' - 2$, a small calculation shows that for every possibility $|\Gamma'| < 2|\Gamma|$. It follows from [1] that G_α^Γ is not 2-transitive. Thus by induction either $f' \le 4q' - 7$ or G_α^Γ is A_c or S_c on the set of $|\Gamma| = c(c - 1)/2$ unordered pairs of distinct points for some $c \ge p$. In the latter case A_c is a composition factor of G_α .

.../6

If G_α has no composition factors isomorphic to A_c for some $c \geq p$, then essentially by adding the bounds for the number of fixed points of A in each orbit of G_α we obtain the required bound on f. If G_α has a composition factor isomorphic to A_c for some $c \geq p$ then the result follows from the following proposition.

<u>Proposition</u> Let G be a primitive permutation group of degree n and suppose that G contains an element of prime order $p \geq 11$ and degree less than p^2. Then,

(a) if G has a composition factor A_c for some $c \geq p$, either $n = c$ and $G \supseteq A_n$, or $n = c(c-1)/2$ and G is A_c or S_c permuting the set of unordered pairs of distinct points, and

(b) if a one-point stabilizer in G has a composition factor A_c for some $c \geq p$, either $n = c + 1$ and $G \supseteq A_n$, or $n = (c+2)(c+1)/2$ and G is A_{c+2} or S_{c+2} permuting the set of unordered pairs of distinct points.

The proof of this proposition is very complicated. One half of the proof involves a combinatorial argument using ideas from graph theory. The other half involves an investigation of subgroups of prime power order (for some prime less than p), and exploits the methods of O'Nan's paper [6].

<u>Conclusion</u> I would like to improve these results in two ways. First, using an idea of Peter Neumann it may be possible to reduce Manning's bound to, perhaps, $f \leq 2q$. Second, I would like to obtain bounds on f for $q \leq 2p - 2$. To do this I need a generalization of the Proposition.

.../7

References:

1. P.J. Cameron, Permutation groups with multiply transitive suborbits, Proc. London Math. Soc. (3) 25 (1972) 427-440.

2. C. Jordan, Sur la limite de transitivité des groupes non alternés, Bull. Soc. Math. France 1 (1873) 40-71.

3. C. Jordan, Sur la limite du degré des groupes primitifs qui contiennent. une substitution donnée, J. fur reine angew. Math. 79 (1875) 248-258.

4. W.A. Manning, On the order of primitive groups I, II, III, Trans. American Math. Soc. 10 (1909) 247-258; 16 (1915) 139-147; 19 (1918) 127-142.

5. W.A. Manning, On the limit of the degree of primitive groups, Trans. American Math. Soc. 12 (1911) 375-386.

6. M. O'Nan, Estimation of Sylow subgroups in primitive permutation groups, Math. Z. 147 (1976) 101-111.

7. C.E. Praeger, Primitive permutation groups containing an element of order p of small degree, p a prime I, II, J. Algebra 34 (1975) 540-546; 42 (1976) 278-293.

8. J. Saxl, Permutation groups of degree $4p + 3$, J. London Math. Soc. (2) 15 (1977) 66-74.

9. J. Saxl, On a theorem of Jordan and Manning, J. London Math. Soc. (2) 15 (1977).

10. M.J. Weiss, Primitive groups which contain substituions of prime order p of degree 6p or 7p , Trans. American Math. Soc. 30 (1928) 333-359.

11. H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.

University of Western Australia
Nedlands, Australia 6009.