FIXED-POINT-FREE PERMUTATIONS IN TRANSITIVE PERMUTATION GROUPS OF PRIME-POWER ORDER

By PETER J. CAMERON, L. G. KOVÁCS, M. F. NEWMAN and CHERYL E. PRAEGER

[Received 12th November 1984]

Introduction

THE problem of finding a useful lower bound for the number of fixed-point-free elements in a transitive p-group was suggested to us by a question of Kantor about the existence of fixed-point-free 2-elements in finite transitive groups.

THEOREM 1. *A transitive permutation group P of order a power of a prime p has at least $(p|P|-1)/(p+1)$ fixed-point-free elements.*

This theorem is a straightforward consequence of the following result on abstract groups of prime-power order (which is proved below). Take P to be G and a point stabiliser P_α to be H; note $\bigcap\{P_\alpha^x \mid x \in P\} = 1$.

THEOREM 2. *Let H be a proper subgroup of a group G of p-power order for a prime p, then*

$$(p+1)\,|\bigcup\{H^g \mid g \in G\}| \leqslant |G| + |\bigcap\{H^g \mid g \in G\}|.$$

Equality can hold in both theorems. Let R be a finite commutative ring with 1 such that the only ideals of R are powers of its radical J and $|R/J| = p$. For example, let R be the ring of integers modulo p^n or the polynomial ring $\mathbb{F}_p[y]$ modulo the ideal generated by y^n. Let P be the subgroup of the one-dimensional affine group over R consisting of mappings $(1+j, r)$ with j in J and r in R defined by

$$z(1+j, r) = z(1+j) + r \quad \text{for all } z \text{ in } R.$$

Then P is a transitive permutation group on the set R and P has order p^{2n-1}. Put $J^0 = R$; then $|J^i| = p^{n-i}$ for $0 \leqslant i \leqslant n$. For r in $J^i \setminus J^{i+1}$ the permutation $(1+j, r)$ has no fixed point if and only if $j \in J^{i+1}$. Hence the number of fixed-point-free elements in P is

$$\sum_{i=0}^{n-1} p^{n-i-1}(p^{n-i} - p^{n-i-1}) = (p^{2n}-1)/(p+1).$$

This gives equality in Theorem 1. Again taking G to be P and H to be the stabiliser of 0 gives equality in Theorem 2.

The above examples are not the only kinds of groups for which equality holds. Note they have soluble length 2. There are some quite different examples (for details see [1]) which are of maximal nilpotency class and have soluble length up to the integer part of $\log_2(p+1)$. These two types are the only examples we know. The analysis in the next section shows that there are quite severe restrictions on the possible structure of the groups with equality. Thus it seems reasonable to ask: given a prime p, is there a bound on the soluble length of transitive permutation groups of p-power order in which $(p|P|-1)/(p+1)$ elements act fixed-point-freely?

THEOREM 1E. *When equality holds in Theorem* 1 *and* P *acts on a set with* p^n *elements, then*

(a) $|P| = p^{2n-1}$,

(b) *the stabiliser* P_α *of a point* α *has* p *fixed points and* $p-1$ *orbits of length* p^i *for each* i *from* 1 *to* $n-1$,

(c) *the action of* P_α *on each such orbit is regular,*

(d) *for* β *in a* P_α*-orbit of length* p^i *the stabiliser* $P_{\alpha\beta}$ *fixes pointwise all* P_α*-orbits of length at most* p^i.

This result is a straightforward consequence of the corresponding result (Theorem 2E) which describes the situation when equality holds in Theorem 2. That requires more notation and is, therefore, given (in parts) during and after the proof of Theorem 2.

It is perhaps worth noting that conditions (a)–(d) characterise the equality case.

Proof of Theorem 2

Let p^n be the index, $|G: H|$, of H in G. Let $G = G_0 > G_1 > \cdots > G_n = H$ be a chain of proper subgroups; so $|G: G_i| = p^i$. Let $H_i = \bigcap \{H^g \mid g \in G_i\}$. Note H_0 is normal in G and $H_{n-1} = H$.

THEOREM 2E. *When equality holds in Theorem* 2, *then*

(a) $|H_i: H_0| = p^i$ *for* $0 \leq i \leq n-1$. (to be continued).

Theorem 2 and Theorem 2E (including (b) below) are proved together by induction on n. In the course of this we consider several cases; when in any one of these the inequality in Theorem 2 is proved to be strict, then Theorem 2E holds vacuously. For $n = 1$ everything is obvious. For $n \geq 2$ the inductive hypothesis applied to H as a proper subgroup of G_1 gives to begin with

$$(p+1)\,|\bigcup \{H^g \mid g \in G_1\}| \leq |G_1| + |H_1|. \qquad (*)$$

Clearly each term is divisible by $|H_1|$. When the inequality is strict

$$(p+1)\,|\bigcup \{H^g \mid g \in G_1\}| \leq |G_1|;$$

and hence, since G_1 has index p in G,

$$(p+1)\,|\bigcup\{H^g \mid g \in G\}| \leqslant p\,|G_1| = |G|$$

as required. So it remains to consider equality in (*). The inductive hypothesis gives in addition $|H_i\colon H_1| = p^{i-1}$ for $1 \leqslant i \leqslant n-1$; and it follows that $|G\colon H_1| = p^{2n-2}$. Let K denote G_{n-1} and $K_i = \bigcap\{K^g \mid g \in G_i\}$ for $0 \leqslant i \leqslant n-2$. The inductive hypothesis applied to K as a proper subgroup of G gives

$$(p+1)\,|\bigcup\{K^g \mid g \in G\}| \leqslant |G| + |K_0|.$$

Again when the inequality is strict

$$(p+1)\,|\bigcup\{K^g \mid g \in G\}| \leqslant |G|$$

and hence

$$(p+1)\,|\bigcup\{H^g \mid g \in G\}| \leqslant |G|.$$

With equality the inductive hypothesis gives $|K\colon K_0| = p^{n-2}$ and hence $|G\colon K_0| = p^{2n-3}$.

THEOREM 2E (continued).
(b) $H_1 \leqslant K_0$ *for* $n \geqslant 2$.

The proof is now divided into two cases,

(i) $H_1 \not\leqslant K_0$. Here we prove Theorem 2 with strict inequality. In this case $n \geqslant 3$ and the inductive hypothesis applied to H, K in G_1 yields $H_2 \leqslant K_1$. Put $D = H_1 \cap K_0$; note $|H_i\colon D| = p$ and $|K_0\colon D| = p^2$. It follows from the inductive hypothesis applied to H in G_2 that

$$(p+1)\,|\bigcup\{(H \setminus H_2)^g \mid g \in G_2\}| \leqslant |G_2| - p\,|H_2|;$$

so, since G_2 has index p^2 in G,

$$(p+1)\,|\bigcup\{(H \setminus H_2)^g \mid g \in G\}| \leqslant |G| - p^3\,|H_2| = |G| - p^5\,|D|.$$

Next consider $H_2 \setminus K_0$. It is a union of $p^2 - p$ cosets of D. Of these $p-1$ make up $H_1 \setminus K_0$ which is normalised by G_1, and the union of the other $p^2 - 2p + 1$ cosets is normalised by G_2 since H_2 is. Hence

$$|\bigcup\{H_2 \setminus K_0)^g \mid g \in G\}| \leqslant p(p-1)\,|D| + p^2(p-1)^2\,|D|.$$

Finally

$$\bigcup\{(H_2 \cap K_0)^g \mid g \in G\} \leqslant K_0,$$

so

$$|\bigcup\{(H_2 \cap K_0)^g \mid g \in G\}| \leqslant p^2\,|D|.$$

Combining the above three inequalities gives

$$(p+1)\,|\bigcup\{H^g \mid g \in G\}| \leqslant |G|$$

as claimed.

(ii) $H_1 \leqslant K_0$. It follows from (*) that

$$(p+1)\,|\bigcup\{(H\setminus H_1)^g \mid g \in G_1\}| \leqslant |G_1| - p\,|H_1|,$$

so

$$(p+1)\,|\bigcup\{(H\setminus H_1)^g \mid g \in G\}| \leqslant |G| - p^2\,|H_1|.$$

The indices of H_1, K_0 in G which have been determined yield that H_1 is maximal in K_0. Hence K_0/H_0, being a subdirect product of the K_0/H_1^g, is elementary abelian and centralised by G_1: so K_0/H_0 is acted on by the group G/G_1 of order p. No non-trivial element of the maximal subgroup H_1/H_0 of K_0/H_0 can be fixed by this action, since such an element would generate a non-trivial central subgroup of G/H_0 in H/H_0, which is impossible. The following lemma with $V = K_0/H_0$, $W = H_1/H_0$ and $\langle x\rangle = G/G_1$ yields

$$(p+1)\,|\bigcup\{H_1^g \mid g \in G\}| \leqslant p^2\,|H_1| + |H_0|$$

with equality only if $|H_1 : H_0| = p$. This completes the proofs.

LEMMA. *Let V be a non-trivial elementary abelian p-group (written additively) acted on by a group $\langle x\rangle$ of order p, and let W be a maximal subgroup of V containing no non-zero element fixed by x. Then*

$$(p+1)\,|\bigcup\{Wx^i \mid 0 \leqslant i \leqslant p-1\}| \leqslant p\,|V| + 1$$

with equality if and only if $|W| = p$.

Proof. The result is easily checked for $|V| \leqslant p^2$. We shall assume, henceforth, that $|V| = p^s$ with $s \geqslant 3$. Regard V as a vector space over the field $\mathbb{F}_p$ of order p. Identify x with the linear transformation representing it on V. Set $y = x - 1$; note $y^p = x^p - 1^p = 0$. By assumption, $\ker y$ avoids the maximal subspace W, so the dimension of $\ker y$ must be 1. Therefore the Jordan normal form of the nilpotent linear transformation y consists of a single (indecomposable) block; that is, V has a basis of the form $v, vy, \ldots, vy^{s-1}$ (with of course $y^s = 0$ and $s \leqslant p$). Consider the equation defining W as a hyperplane with reference to such a basis: for suitable $\nu_0, \ldots, \nu_{s-1}$ in $\mathbb{F}_p$,

$$\sum \lambda_i v y^i \in W \quad \text{if and only if} \quad \sum \nu_i \lambda_i = 0$$

(with summation always over i from 0 to $s-1$). For $u = \sum \lambda_i v y^i$ in V we have that $uy^j \in W$ if and only if $\sum \nu_{i+j}\lambda_i = 0$ (where $\nu_{i+j} = 0$ for $i + j \geqslant s$). The $s-1$ equations obtained with $j = 0, \ldots, s-2$ form a homogeneous linear system in the s unknowns $\lambda_0, \ldots, \lambda_{s-1}$ and so have a non-zero solution $(\mu_0, \ldots, \mu_{s-1})$. Put $w = \sum \mu_i v y^i$, then $w, wy, \ldots, wy^{s-2} \in W$. As $W \cap \ker y = 0$, even $wy^{s-1} \neq 0$. It is easy to show $\{w, wy, \ldots, wy^{s-1}\}$ is

also a basis of V. The equation of W with respect to this basis has only one non-zero coefficient. Let $0 \leq k \leq p-1$. As $yx^k = y(y+1)^k$, the binomial theorem yields that the coefficient of wy^{s-1} in $(\sum \lambda_i w y^i)x^k$ is $\sum \binom{k}{s-1-i}\lambda_i$ $\left(\text{with the usual convention that } \binom{k}{j}=0 \text{ for } j>k\right)$. So $\sum \lambda_i w y^i \in Wx^{-k}$ if and only if

$$\sum \binom{k}{s-1-i}\lambda_i = 0. \qquad (x)$$

It is easy to see that for $1 \leq t \leq 3$ the solutions of each t of the p equations (x) in the unknowns $\lambda_0, \ldots, \lambda_{s-1}$ form a space of dimension $s-t$ (see also the remark below); in other words the intersection of each t of the Wx^{-k} has order p^{s-t}. Thus by the inclusion-exclusion principle

$$|\bigcup \{Wx^k \mid 0 \leq k \leq p-1\}| \leq \sum \left\{(-1)^{t-1}\binom{p}{t}p^{s-t} \mid 1 \leq t \leq 3\right\}.$$

It is easily checked that the right-hand side is strictly smaller than $(p^{s+1}+1)/(p+1)$ for all odd primes p. Since $p \geq s \geq 3$ this completes the proof.

Remark on the proof of the Lemma. Let $a_1, \ldots, a_t$ be integers pairwise non-congruent modulo p. It is well-known that the determinant of the matrix with (i, j)-entry a_i^{j-1} is (up to sign) the product of the differences of the a_i (with the convention that $a_i^0 = 1$ even when $a_i = 0$) and hence is not divisible by p; this is the so-called Vandermonde determinant. A less known variant, easily derived from this, is that the determinant of the matrix with (i, j)-entry $\binom{a_i}{j-1}$ is also prime to p. It follows that the set of solutions of each t of the equations (x) above is a subspace of V of codimension $\min(s, t)$. Thus the principle of inclusion-exclusion would enable us to calculate $|\bigcup \{Wx^k \mid 0 \leq k \leq p-1\}|$ precisely.

Remark on equality in Theorem 2. Let T_i be a transversal of G_i in G_{i-1}. It is straightforward to check the following additional claims.

THEOREM 2E (continued).

(c) $|G/H_0| = p^{2n-1}$,

(d) *the union of* $1 + p + \cdots + p^{n-1}$ *subsets*

$$H_0 \cup \bigcup \{\bigcup \{(H_{i+1} \setminus H_i)^g \mid g \in T_{i+1}\} \mid 0 \leq i \leq n-2\} \text{ is disjoint,}$$

(e) G_i *is the normaliser of* G_{i+1} *in* G *for* $0 \leq i \leq n-1$, *and so* $G, G_1, \ldots, G_{n-1}, H$ *are the only subgroups of* G *containing* H,

(f) $H \cap H^g = H_i$ *for all* g *in* $G_i \setminus G_{i+1}$ *and* $0 \leq i \leq n-1$.

REFERENCE

1. L. G. Kovács and M. F. Newman, 'Some groups of maximal class'. In preparation.

Merton College,
Oxford, OX1 4JD,
England.

Department of Mathematics, IAS
Australian National University,
G.P.O. Box 4,
Canberra, ACT 2601, Australia.

Department of Mathematics, IAS,
Australian National University,
G.P.O. Box 4,
Canberra, ACT 2601, Australia.

Department of Mathematics,
University of Western Australia,
Nedlands, WA 6009, Australia.