Discrete Mathematics 106/107 (1992) 135–138
North-Holland

On the number of fixed point free elements in a permutation group

Peter J. Cameron
Queen Mary and Westfield College, Mile End Road, London E1 4NS, UK

Arjeh M. Cohen
CWI, Kruislaan 413, 1098 SJ Amsterdam, Netherlands

Received 27 November 1991
Revised 6 March 1992

Abstract

Cameron, P.J. and A.M. Cohen, On the number of fixed point free elements in a permutation group, Discrete Mathematics 106/107 (1992) 135–138.

A lower bound is given for the number of fixed point free elements in a permutation group.

At the end of May, 1991, H.W. Lenstra Jr asked the second author whether the number of fixed point free elements of a finite transitive group on a set of n elements, $n > 1$, is at least $1/n$th of the order of G (with equality only for Frobenius groups of order $n(n-1)$). An affirmative answer would be useful to know in connection with a new number factorization algorithm, so he was told.

Almost convinced that such a result should be in the pre-world-war literature and taking a lazy option, the second author e-mailed a few colleagues for references. In the meantime, he tried some of the combinatorial approaches taught by van Lint. The result was the proposition below, which generalizes an affirmative answer to the above query to arbitrary $n \geq 1$. (If $n = 1$ then, in the setting below, $r = 1$ so both the number and the lower bound are equal to 0.)

Before reading the solution (e-mailed shortly after the reference query), the first author replied with more or less the same result. No surprise, one might argue, for someone who has also been under van Lint's influence.... Anyway, as no reference to the literature has come up so far, the result may be worthy of note here, especially since a recent result on minimal degrees gives rise to improvements of the bound, as stated in the theorem of this note and its corollary.

Correspondence to: A.M. Cohen, CWI, Kruislaan 413, 1098 SJ Amsterdam, Netherlands.

Proposition. *Suppose G is a transitive permutation group of degree n with permutation rank r. Then the number of elements of G without fixed points is at least $((r-1)/n)\,|G|$, with equality if and only if G is a Frobenius group of order $n \cdot (n-1)/(r-1)$.*

Proof. Denote by f_i the number of elements of G fixing exactly i points. Then $f_n = 1$ and

$$\sum_{i=0}^{n} f_i = |G|. \tag{1}$$

Transitivity of G is equivalent to

$$\sum_{i=0}^{n} i f_i = |G|. \tag{2}$$

For the equation expresses the familiar fact that the inner product of the permutation character and the trivial character is 1. The fact that the inner product of the permutation character with itself equals the permutation rank can be similarly expressed:

$$\sum_{i=0}^{n} i^2 f_i = r\,|G|. \tag{3}$$

Comparing (1) and (2) gives

$$f_0 = \sum_{i=1}^{n} (i-1) f_i. \tag{4}$$

Adding (1), (3) and subtracting (2) twice from the result yields

$$\sum_{i=0}^{n} (i-1)^2 f_i = (r-1)\,|G|. \tag{5}$$

Using (4) and (5), we obtain

$$n f_0 = f_0 + (n-1) \sum_{i=1}^{n} (i-1) f_i \geqslant (r-1)\,|G|,$$

whence $f_0 \geqslant ((r-1)/n)\,|G|$, the required inequality. If equality holds, we must have $(n-1)(i-1)f_i = (i-1)^2 f_i$ for all $i = 2, \ldots, n-1$, in which case $f_i \neq 0$ only for $i \in \{0, 1, n\}$. From (1)–(3), it readily follows that then $f_0 = n-1$ and G is a Frobenius group of order $n \cdot (n-1)/(r-1)$ with kernel of order $f_0 + f_n = n$. □

Minimal degrees. In order to derive a sharper bound, we shall introduce one more parameter: the so-called *minimal degree* of a permutation group G. It stands for the minimum number of points moved (i.e., not fixed) by any non-identity element of G. The relevance of the minimal degree d of G is that

$$f_{n-d+1} = f_{n-d+2} = \cdots = f_{n-1} = 0.$$

Now, from (4) and (5) above, we find, for G, n and r as in the proposition,

$$\begin{aligned}(n-d)f_0 &= f_0 + (n-d-1)\left(\sum_{i=1}^{n-d}(i-1)f_i\right) + (n-d-1)(n-1)f_n \\ &\geqslant (r-1)\,|G| - (n-1)^2 + (n-d-1)(n-1) \\ &= (r-1)\,|G| - d(n-1),\end{aligned}$$

whence we have the following.

Theorem. *Suppose G is a transitive permutation group of degree n with permutation rank r and minimal degree d. Then the number f_0 of elements of G without fixed points satisfies*

$$f_0 \geqslant \frac{(r-1)\,|G| - d(n-1)}{n-d}, \tag{6}$$

with equality if and only if each element of G fixes at least $n-d$ (whence n or $n-d$) or at most 1 point. In particular,

$$f_0 \geqslant \frac{(r-1)\,|G| \log |G| - n(n-1)}{n(\log |G| - 1)}.$$

Proof. The first statement follows immediately from the above. As for the second, we use some unpublished observations of Babai, cf. [1], which we repeat here for the reader's convenience. First recall another parameter, the *base size* of a permutation group G, the smallest number of points whose pointwise stabiliser is the identity. Now we have:

(a) If *G is transitive of degree n, with minimal degree d and base size b, then* $bd \geqslant n$. This is clear from the fact that any base meets the support of any non-identity element of G.

(b) $b \leqslant \log_2 |G|$. For, given a minimal base, let $G(i)$ be the pointwise stabiliser of the first i base points. Then $G(i) > G(i+1)$ (else the $(i+1)$st base point is redundant), so $|G(i)| \geqslant 2\,|G(i+1)|$; and $G(0) = G$, $G(b) = 1$.

So $d \geqslant n/\log |G|$ (where logarithms are to base 2). The right-hand side of (6) is monotonically increasing as a function in d. Thus, we may substitute $n/\log |G|$ for d in (6), which yields the second statement. □

For the symmetric and alternating groups of degree at least 3, the minimal degrees are 2 and 3, respectively. But if G is a primitive permutation group of degree $n \geqslant 4$, distinct from the symmetric group and from the alternating on n letters, better lower bounds of d in terms of n are known. We cite Theorem 2 of [2] (where more references to minimal degree literature are to be found), again, for the reader's convenience.

Liebeck and Saxl's minimal degree result ([2]; the proof uses the classification of finite simple groups). *Suppose G is a primitive permutation group of degree $n \geq 4$, minimal degree d and permutation rank r. Then one of*

(i) $G \leq \mathrm{Sym}_m \mathrm{wr} \mathrm{Sym}_r$ *containing* $(\mathrm{Alt}_m)^r$ $(m \geq 5)$ *where the action of* Sym_m *is on k-subsets of an m-set and the wreath product has the product action of degree* $n = \binom{m}{k}^r$;

(ii) $d \geq n/3$.

This result gives the following corollary of (6).

Corollary. *Suppose G is a primitive permutation group of degree $n > 3$, permutation rank r and minimal degree d. If G is distinct from the permutation groups described in* (i) *above, then*

$$f_0 \geq \frac{3(r-1)}{2n}|G| - \frac{n-1}{2}.$$

Remark. If $d = n - 2$, we have equality in (6). For instance, if $G = \mathrm{PSL}(2, q)$ (the fractional linear group over the field of q elements) acting on the projective line of size $n = q + 1$, in which case $d = n - 2$ and $r = 2$, the actual number is

$$f_0 = \frac{1}{2}\left(1 - \frac{(2, q+1)}{q+1}\right)|G|.$$

References

[1] L. Babai, On the order of uniprimitive permutation groups, Ann. Math. 113 (1981) 553–568.

[2] M.W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, Proc. London Math. Soc., II Ser. 63 (1991) 266–314.