Arch. Math. 77 (2001) 138–142
0003-889X/01/020138-05 $ 2.50/0
© Birkhäuser Verlag, Basel, 2001

Archiv der Mathematik

Regular orbits in powers of permutation representations

By

JONATHAN D. H. SMITH

Abstract. Let (Q, G) be a faithful permutation representation of a finite group G. Suppose that the G-set Q has t distinct non-zero marks. In a permutation representation analogue of a theorem of Brauer on linear representations, it is shown that the direct power $(Q, G)^t$ of (Q, G) contains a regular orbit. As a corollary, the probability that a random element of Q^r lies in a regular orbit of $(Q, G)^r$ is shown to tend to 1 exponentially fast as r tends to ∞. Further, knowledge of the rate of convergence is equivalent to knowledge of the second largest value of the character of the linear permutation representation.

1. Introduction. Let G be a finite group. A *G-set* (Q, G) or *permutation representation* of the group G consists of a set Q, together with a (right) action of G on Q via a homomorphism

$$G \to Q!\,;\ g \mapsto (q \mapsto qg) \tag{1.1}$$

from G into the group $Q!$ of all permutations of the set Q. The G-set (Q, G) may be construed as an algebra of unary operations on the set Q. For a positive integer r, the direct power $(Q, G)^r$ of this algebra is the G-set Q^r with *diagonal action*

$$g : (q_1, \ldots, q_r) \mapsto (q_1 g, \ldots, q_r g) \tag{1.2}$$

of the elements g of G. Suppose that the G-set (Q, G) is faithful [i.e. (1.1) injects]. This paper is concerned with the appearance of regular orbits of G [i.e. G-sets $G \to G!\,;\ g \mapsto (h \mapsto h \cdot g)$ using the multiplication $\cdot$ of G] as subalgebras of powers $(Q, G)^r$ of (Q, G). Theorem B below shows that as r increases, the probability of a random element of Q^r lying in a regular orbit tends to 1 exponentially fast. Furthermore, knowledge of the rate of convergence is equivalent to knowledge of the second largest value of the character of the linear permutation representation.

As proved here, Theorem B is a corollary of Theorem A, a permutation representation analogue of a theorem of Brauer about complex linear representations. Burnside [4, Ch. XV, Th. IV] showed that, given a faithful complex linear representation ρ of G, every irreducible representation of G appears as a constituent of a tensor power $\rho \otimes \ldots \otimes \rho$ of ρ. Brauer [3] (cf. [1, Theorem I.6.3], [5, Satz V 10.8]) refined Burnside's result to show that, if the character of ρ takes on at most t distinct values, then each irreducible representation of G already appears as a constituent of one of the first t tensor powers of ρ. Now the complex linearization of the regular permutation representation of G includes all the irreducible complex linear representations of G as constituents. Thus for a permutation representation, the appearance

Mathematics Subject Classification (1991): 19A22, 60B10.

of a regular orbit is the analogue of the appearance of all the irreducible linear representations as constituents of a linear representation. In place of the t distinct values of the character of a linear representation ρ, Theorem A requires t distinct non-zero values for the mark of a subgroup K of G in the faithful permutation representation (Q, G) of G. Under this condition, Theorem A guarantees that the direct power $(Q, G)^t$ contains a regular orbit. The proof of Theorem A uses the same Vandermonde determinant technique that Brauer used. Since permutation representations are sometimes viewed as "linear representations over GF(1)", Section 3 summarizes Theorem A as "Brauer's Theorem in characteristic 1".

The constant c appearing in the estimate of Theorem B is given in terms of the mark table of the group G. Section 2 recalls the Burnside algebra techniques required for the formulation of the probability of lying in a regular orbit in a power of a permutation representation.

2. Permutation representations and Burnside algebras. For a finite group G, let $\underline{\underline{G}}$ denote the variety of right G-sets, considered as a category with homomorphisms (G-equivariant maps) as morphisms. Given G-sets A and B, their disjoint union $A + B$ provides a coproduct in $\underline{\underline{G}}$ and their direct product $A \times B$ provides a product in $\underline{\underline{G}}$. The empty G-set is the initial object of $\underline{\underline{G}}$, while the singleton G-set $\{1\}$ or 1 is a terminal object of $\underline{\underline{G}}$. For a G-set A, let $[A]$ denote the isomorphism class of A in $\underline{\underline{G}}$. Let $\mathrm{A}^+(G)$ be the set of $\underline{\underline{G}}$-isomorphism classes of finite G-sets. It becomes a commutative, unital semiring $(\mathrm{A}^+(G), +, \cdot, 0, 1)$ under $[A] + [B] = [A + B]$, $[A][B] = [A \times B]$, $0 = [\varnothing]$ and $1 = [1]$ (cf. [8, §1.1]).

For a subgroup H of G, there is a *restriction* functor $\downarrow^G_H\colon \underline{\underline{G}} \to \underline{\underline{H}}$; $(A, G) \mapsto (A, H)$. The restriction functor is right adjoint to an *induction* functor $\uparrow^G_H\colon \underline{\underline{H}} \to \underline{\underline{G}}$ [7, I §2.8 and III §3]. The induced action $1 \uparrow^G_H$ may be realized as the set $H \setminus G = \{Hx | x \in G\}$ with action $g : Hx \mapsto Hxg$ of elements g of G. An arbitrary G-set (A, G) breaks up as the disjoint union $A = \sum_{X \in A/G} (X, G)$ of irreducible G-subsets (X, G), the orbits of G on A. The set of G-orbits on A is written here as A/G. Each orbit (X, G) is isomorphic to $1 \uparrow^G_H$ for the stabilizer $H = \{g \in G | xg = x\}$ of an element x of X. Let $\mathrm{Sb}\, G$ denote the lattice of subgroups of G. The inner automorphism group $\mathrm{Inn}\, G$ of G acts on $\mathrm{Sb}\, G$ by conjugation. For subgroups H and K of G, one has $1 \uparrow^G_H = 1 \uparrow^G_K$ iff the orbits $H\, \mathrm{Inn}\, G$ and $K\, \mathrm{Inn}\, G$ coincide [5, Aufg. I 23)c)]. Let

$$\{H_i \mid 1 \leqq i \leqq s\} \tag{2.1}$$

be a set of representatives for the orbits of $\mathrm{Inn}\, G$ on $\mathrm{Sb}\, G$, ordered so that $|H_i| \leqq |H_j|$ for $i \leqq j$.

Define the *mark function*

$$\mathrm{A}^+(G) \to \mathbb{Q}^{\mathrm{Sb}G}; [A] \mapsto \left(H \mapsto \left|\underline{\underline{H}}\left(1, A \downarrow^G_H\right)\right|\right) \tag{2.2}$$

(cf. [4, §180]). Since the right adjoint $\downarrow^G_H$ preserves coproducts, (2.1) is an additive homomorphism. Now

$$\left|\underline{\underline{G}}\left(1 \uparrow^G_H, A\right)\right| = \left|\underline{\underline{H}}\left(1, A \downarrow^G_H\right)\right| \tag{2.3}$$

by the adjointness between restriction and induction. Since $|\underline{\underline{G}}(1 \uparrow^G_H, A \times B)| = |\underline{\underline{G}}(1 \uparrow^G_H, A)| \cdot |\underline{\underline{G}}(1 \uparrow^G_H, B)|$, the mark function (2.2) is also a multiplicative homomorphism. Indeed, it is also injective [2, pp. 70–1] [8, Prop. I.2.2], so $\mathrm{A}^+(G)$ is identified with its image under (2.2). The $\mathbb{Q}$-subalgebra of $\mathbb{Q}^G$ generated by $\mathrm{A}^+(G)$ is called the (*rational*) *Burnside algebra* $\mathrm{B}(G)$ of G.

For a G-set Q, the mark function of $[Q]$ is specified by the row vector

$$\left[\,\left|\underline{\underline{G}}\big(H_j\backslash G,\,Q\big)\right|\,\big|\,1 \leqq j \leqq s\right] \tag{2.4}$$

of *marks* of Q. The *mark table* of G is the $s \times s$ matrix B whose i-th row is the vector of marks of the G-set $H_i \setminus G$ [4, §180] [6, p. 8]. The matrix B is lower triangular with non-zero diagonal entries (whence the injectivity of the mark function). Let

$$B^{-1} = [a_{ij} | 1 \leqq i,\, j \leqq s] \tag{2.5}$$

be the inverse of the mark table.

3. Brauer's Theorem in characteristic 1. Let G be a non-trivial finite group. Let (Q, G) be a faithful permutation representation of G of degree $|Q| = n$.

Theorem A. *Suppose that (Q, G) is a faithful permutation representation of G having exactly t distinct non-zero marks. Then the t-th power $(Q, G)^t$ of the permutation representation (Q, G) contains a regular orbit.*

Proof. Let the vector of marks of Q be

$$f = [f_1, \ldots, f_s]. \tag{3.1}$$

Then the vector of marks of Q^j is $[f_1^j, \ldots, f_s^j]$, so the vector of multiplicities of isomorphism classes of orbits of Q^j is $[f_1^j, \ldots, f_s^j]B^{-1}$. In particular, the number of regular orbits in Q^j is the first component of this vector, namely

$$\sum_{i=1}^{s} f_i^j a_{j1}. \tag{3.2}$$

Suppose that

$$\{f_1, \ldots, f_s\} = \{n = n_0 > \ldots > n_t = 0\}. \tag{3.3}$$

For $0 \leqq i < t$, define

$$x_i = \sum\{a_{j1} \mid f_j = n_i\}. \tag{3.4}$$

In particular, note

$$x_0 = a_{11} = 1/|G| : \tag{3.5}$$

since Q is faithful, $f_j = n$ implies $j = 1$. Suppose that $(Q, G)^t$ were to contain no regular orbit. Since $(Q, G)^t$ contains (diagonal) copies of $(Q, G)^j$ for $1 \leqq j < t$, it would follow that none of the $(Q, G)^j$ for $1 \leqq j \leqq t$ would contain any regular orbit. Now by (3.2) and (3.4), the number of regular orbits in $(Q, G)^j$ is

$$x_0 n_0^j + x_1 n_1^j + \cdots + x_{t-1} n_{t-1}^j. \tag{3.6}$$

One would thus obtain the homogeneous system

$$\begin{aligned} x_0 n_0^1 + x_1 n_1^1 + \cdots + x_{t-1} n_{t-1}^1 &= 0 \\ x_0 n_0^2 + x_1 n_1^2 + \cdots + x_{t-1} n_{t-1}^2 &= 0 \\ &\cdots \\ x_0 n_0^t + x_1 n_1^t + \cdots + x_{t-1} n_{t-1}^t &= 0 \end{aligned} \tag{3.7}$$

of linear equations in $x_0, x_1, \ldots, x_{t-1}$. Since the Vandermonde determinant

$$\det\left[n_i^{j+1} \middle| 0 \leqq i,\, j < t\right] = n_0 n_1 \ldots n_{t-1} \prod_{0 \leqq k < l < t} (n_l - n_k) \tag{3.8}$$

is non-zero, one would then have the contradiction $x_0 = 0$ to (3.5). □

R e m a r k. There are other approaches to the proof of Theorem A, e.g. using the ideas underlying the greedy algorithm of Blaha [2]. The approach adopted here, using the argument of Brauer [3], is designed to facilitate the estimates in the following section.

4. Probability of a regular orbit. Throughout this section, the hypotheses and notation of Section 3 are maintained. Consider the sequence $(Q, G)^r$, for $r = 1, 2, \ldots,$ of powers of the faithful permutation representation (Q, G) of G. For each r, consider the uniform distribution on Q^r. Theorem B below shows that as r increases, the probability of a random element of Q^r lying in a regular orbit tends to 1 exponentially fast. The first part of the theorem gives an estimate of the probability for each r, while the second part shows that knowledge of the rate of convergence is equivalent to knowledge of the second largest permutation character value.

Theorem B. *Let Q be a faithful permutation representation of G of degree n. Suppose that the second largest value of the permutation character π of Q is m.*

(a) *There is a positive constant c such that, for each positive integer r, the probability P_r of a random element of Q^r lying in a regular orbit of $(Q, G)^r$ differs from one by at most $c\left(\frac{m}{n}\right)^r$.*
(b) *The probability P_r satisfies*

$$\lim_{r\to\infty} (1 - P_r)^{\frac{1}{r}} = \frac{m}{n}.$$

P r o o f. Suppose that $\pi(g) = m$ for some element g of G. Then $m = n_1$, the mark of $\langle g \rangle$, since the mark of any given subgroup H of G is not greater than the marks of the subgroups K of H. By (3.5) and (3.6), the number of regular orbits of Q^r is

$$|G|^{-1} n^r + x_1 n_1^r + \cdots + x_{t-1} n_{t-1}^r. \tag{4.1}$$

For $0 \leqq i \leqq t$, define $p_i = n_i/n$. In particular, $p_1 = m/n$. By (3.3), one has

$$1 = p_0 > p_1 > \ldots > p_t = 0. \tag{4.2}$$

The probability P_r that a random element of Q^r lies in a regular orbit is given by

$$P_r = 1 + |G|.\left[x_1 p_1^r + x_2 p_2^r + \cdots + x_{t-1} p_{t-1}^r\right],$$

with coefficients x_i as in (3.4). Then

$$1 - P_r = \left(\frac{m}{n}\right)^r |G|.\left| x_1 + x_2 \left(\frac{p_2}{p_1}\right)^r + \cdots + x_{t-1} \left(\frac{p_{t-1}}{p_1}\right)^r \right|. \tag{4.3}$$

Define

$$c = |G| \sum_{i=1}^{t-1} |x_i|. \tag{4.4}$$

Use of (4.2) and the triangle inequality on (4.3) yields (a). Taking the limit of the r-th root of each side of (4.3) yields (b). □

A c k n o w l e d g e m e n t. The author is grateful to anonymous referees for many helpful suggestions concerning this paper.

References

[1] E. BANNAI and T. ITO, Algebraic Combinatorics I. Menlo Park, California 1984.
[2] K. D. BLAHA, Minimal bases for permutation groups: the greedy approximation. J. Algorithms **13**, 297–306 (1992).
[3] R. BRAUER, A note on theorems of Burnside and Blichfeldt. Proc. Amer. Math. Soc. **15**, 31–34 (1964).
[4] W. BURNSIDE, Theory of Groups of Finite Order. Cambridge 1911.
[5] B. HUPPERT, Endliche Gruppen I. Berlin-Heidelberg-New York 1967.
[6] H. PAHLINGS, On the Möbius function of a finite group. Arch. Math. **60**, 7–14 (1993).
[7] J. D. H. SMITH and A.B. ROMANOWSKA, Post-Modern Algebra. New York 1999.
[8] T. TOM DIECK, Transformation Groups and Representation Theory. LNM **766** Berlin-Heidelberg-New York 1979.

Eingegangen am 13. 9. 1999

Anschrift des Autors:

Jonathan D. H. Smith
Department of Mathematics
Iowa State University
Ames, IA 50011, USA