BULL. AUSTRAL. MATH. SOC.
VOL. 28 (1983), 355-365.

20B05, 20B10

FINITE SIMPLE GROUPS AND FINITE PRIMITIVE PERMUTATION GROUPS

CHERYL E. PRAEGER

The classification of the finite simple groups has had far-reaching consequences for many branches of algebra. This paper is a discussion of several problems about primitive permutation groups which have been solved using the simple group classification.

1. Introduction

The central problem of the theory of finite groups is to find for each positive integer n all groups (up to isomorphism) of order n. This is of course equivalent to the two problems of

(i) finding all finite simple groups and

(ii) finding all extensions of one group by another group.

The solution to the more basic problem of classifying all finite simple groups was completed in 1980 and it is now the job of mathematicians in related fields to determine the consequences of this classification on their field of research. The purpose of this paper is to survey several fairly basic problems in the theory of finite permutation groups where the simple group classification has led to a satisfactory solution.

Received 19 July 1983. This paper is based on an invited lecture given at the 1983 Australian Mathematical Society Annual Meeting held at the University of Queensland in May 1983.

As an analogue of the preceding discussion of finite groups one might say that the central problem of the theory of finite permutation groups is to find for each positive integer n all permutation groups (up to equivalence) of degree n. (A *permutation group of degree* n is a subgroup of the symmetric group S_n of all permutations of the set $\mathbf{n} = \{1, 2, \ldots, n\}$. Two permutation groups G, H of degree n are said to be *equivalent* if there is a group isomorphism $f : G \to H$ and a bijection $\phi : \mathbf{n} \to \mathbf{n}$ such that for all g in G and i in $\mathbf{n}$, $(i^g)\phi = (i\phi)^{gf}$; that is G and H are equivalent if and only if they are isomorphic and act in the same way on $\mathbf{n}$ up to a relabelling of $\mathbf{n}$.)

Now let $G \leq S_n$: then G determines an equivalence relation on $\mathbf{n}$ by

$$i \sim j \iff i^g = j \quad \text{for some} \quad g \quad \text{in} \quad G .$$

The equivalence classes are called *orbits* and G is called *transitive* if it has exactly one orbit. The central problem is then equivalent to finding

(i) all transitive permutation groups and

(ii) all ways of putting together transitive groups to find all permutation groups.

So let us now suppose that $G \leq S_n$ is transitive. Sometimes it is possible for $\mathbf{n}$ to be partitioned into blocks of equal size which are permuted (blockwise) by G (that is for such a block B and g in G, B^g either equals B or is disjoint from B). G is said to be *primitive* if the only possible sets of blocks are $\{\mathbf{n}\}$ and $\{\{i\} \mid 1 \leq i \leq n\}$. The problem of finding all transitive permutation groups is then equivalent to finding

(i) all primitive permutation groups and

(ii) all ways of putting together primitive groups to find all transitive groups.

While problem (ii) is by no means trivial, the problem of finding all primitive groups is more basic to the subject, and indeed the primitive permutation groups play a role in the theory of finite permutation groups

analogous to the role of finite simple groups in the theory of finite groups. Certainly the consequences of the simple group classification have been most spectacular for problems about primitive permutation groups.

2. Simple groups and primitive groups

The finite simple groups G may be conveniently listed as follows:

(a) $G = Z_p$, the cyclic group of order p, p a prime;

(b) $G = A_n$, the alternating group of degree n, that is the group of all even permutations of a set of size n, $n \geq 5$;

(c) G a group of Lie type: these may be divided into

(i) $G = G(n, q)$, a classical group of dimension n "over" a field of q elements (these comprise linear, orthogonal, unitary and symplectic groups, six families in all),

(ii) $G = G(q)$, an exceptional group over a field of q elements (10 families);

(d) G is one of the 26 sporadic simple groups.

Further information about groups of Lie type may be found in [9] for example, and about the sporadic simple groups in [10].

So far, the most useful result which has allowed the classification of the finite simple groups to be used to make headway with problems involving primitive permutation groups is a theorem of M. O'Nan and L.L. Scott. It allows some questions about primitive permutation groups G to be reduced to the cases where G is a group of affine transformations of a vector space or $T \leq G \leq \mathrm{Aut}\, T$ for some non-abelian simple group T. In essence their result is as follows (see [6], Theorem 4.1, for details and [1], [12] for details of the correction at part (ii)).

THEOREM 2.1. *Let G be a primitive permutation group on a set X of n points, and let N be the socle of G (that is the group generated by all minimal normal subgroups of G). Then one of the following occurs.*

(i) N is elementary abelian of order p^d and regular, $n = p^d$ where p is prime and $d \geq 1$, and $G \leq \mathrm{AGL}(d, p)$ the group of affine

https://doi.org/10.1017/S0004972700021080 Published online by Cambridge University Press

transformations of N .

(ii) $N = T_1 \times \ldots \times T_m$ *where* T_i *are isomorphic to a fixed non-abelian simple group* T *and* $m \geq 1$. *Moreover if* $m \geq 2$ *then*

(a) $n = |T|^{m-1}$ *and the action of* N *on* X *is equivalent to its "diagonal action" on the cosets of a diagonal subgroup* $D = T$ *of* N , *or*

(b) $n = n_0^k$, $m = kr$, $G \leq G_0$ wr S_k , *where* G_0 *is primitive on* Y *of degree* n_0 *with a minimal normal subgroup isomorphic to* T^r , *and the action of* G *on* X *is equivalent to its "product action" on* Y^k . *Further either* T^r *is the socle of* G_0 *(and* G_0 *satisfies (a) or* $r = 1$ *),* *or* $r = 1$ *and* T *is regular on* Y .

Of course other links exist between certain questions about primitive groups and related questions about simple groups, but this theorem has proved the most useful. We shall now consider several longstanding problems about primitive permutation groups for which the classification of simple groups has provided major "break throughs".

3. How big are primitive permutation groups?

The symmetric group S_n and the alternating group A_n $(n \neq 2)$, are both primitive of degree n and $|S_n| = 2|A_n| = n!$. The problem of finding an upper bound $f(n)$, "much smaller" than $n!$, for the orders of primitive groups G of degree n other than S_n and A_n was one of the central problems of 19th century group theory. The best result obtained last century is the theorem of Bochert ([5], or see [21], 14.2) that $f(n) = n!/[(n+1)/2]!$ is an upper bound. No significant progress was made until 1969 when Wielandt [22] showed that for primitive but not doubly transitive groups, $f(n)$ could be taken as 24^n . This result was generalised in 1981 to all primitive groups with $f(n) = 4^n$, by Saxl and the author [18]. Soon after this and using completely different methods

Babai [2, 3] showed that $f(n) = \exp\left(4\sqrt{n}\log^2 n\right)$ was a bound. These various bounds can be compared easily using the following table, where $(\log f(n))^*$ denotes the order of the dominant term in the asymptotic expansion of $\log f(n)$. However using the classification of simple groups Cameron ([6], Theorem 6.1 (S)) showed that $f(n)$ could be taken as $n^{c\log n}$ for some constant c, if one excludes $G \leq S_m$ wr S_k in the product action, where S_m is acting on j-element subsets, $j \geq 1$, $k \geq 1$.

TABLE 1. Orders of primitive groups

		$f(n)$	$(\log f(n))^*$
Bochert	1889	$n!/[(n+1)/2]!$	$n \log n$
Wielandt Praeger, Saxl	1969 1981	4^n	n
Babai	1982	$\exp\left(4\sqrt{n}\log^2 n\right)$	$\sqrt{n}\log^2 n$
Cameron[(1)]	1981	$n^{c\log n}$	$\log^2 n$
Babai, Cameron Palfy[(1)]	1982	n^c	$\log n$

(1) Bound for a subclass of primitive groups, see text.

He showed that even better results were possible if one was "careful". Finally (also using the simple group classification) Babai, Cameron and Palfy [4] showed that if the set of composition factors of the primitive group G of degree n contains no alternating group of degree greater than d and no classical group of dimension greater than d for some fixed positive integer d then $|G|$ is polynomially bounded, that is $|G| \leq n^c$ for some constant $c = c(d)$.

4. How many primitive permutation groups are there?

For each positive integer n the symmetric group S_n is primitive of degree n, as is the alternating group A_n for $n \neq 2$, while, for $n \leq 4$, there are no other primitive groups of degree n. By 1861 Mathieu

https://doi.org/10.1017/S0004972700021080 Published online by Cambridge University Press

[14] had shown that for each $n = 5, \ldots, 33$ there was a primitive (indeed a multiply transitive) group of degree n other than A_n and S_n.

Let E be the set of positive integers n for which there exists a primitive group of degree n other than A_n and S_n. Thus E contains $\{n \mid 5 \leq n \leq 33\}$. It is non-trivial to show that E does not contain 34. In 1970 Sims [19] published a complete list of primitive groups of degrees $n \leq 20$, and he has determined (but not published) the primitive groups of degrees $n \leq 50$: the only integers n, $5 \leq n \leq 50$, which are not in E are 34, 39 and 46. Further, certain other integers were proved to lie outside of E by Miyamoto [15] in 1975 and Neumann and Saxl [16] in 1979: this was a consequence of their investigations of primitive groups of certain special degrees, for example

(i) if $n = 2p = 4q + 2 = f(r) > 22$, p, q, r prime, $f(r) = r + 3$, $r + 5$ or $5r + 3$ then $n \notin E$ (for example, $n = 46, 94, 118, 166, 214, \ldots$),

(ii) if $n = 4p$ where p and $(p-1)/2$ are prime and $4p - 1$ is composite then $n \notin E$ (for example $n = 92, 188, 236, \ldots$).

These "pre-classification" results strongly suggest that $\mathbb{N} - E$ is infinite. However using the simple group classification Cameron, Neumann and Teague [7] have shown not only that $\mathbb{N} - E$ is infinite but also that E has density zero in the natural numbers $\mathbb{N}$, that is that non-trivial primitive groups G of degree n (that is $G \neq S_n, A_n$) are rare. This is a very surprising result which had not even been guessed at before the classification. If $e(x) = |\{n \in E \mid n \leq x\}|$, then it is shown that

$$e(x) = 2\pi(x) + (1+\sqrt{2})x^{\frac{1}{2}} + O\left(x^{\frac{1}{2}}/\log x\right) \sim 2x/\log x .$$

That $e(x) \geq 2\pi(x) + (1+\sqrt{2})x^{\frac{1}{2}} - O(\log x)$ follows easily from the facts that $n = p \in E$, p a prime (taking $G = Z_p$), $n = p + 1 \in E$, ($G = \mathrm{PSL}(2, p)$ in its natural action on the projective line), $n = m^2 \in E$ ($G = S_m$ wr Z_2 in its product action), $n = m(m-1)/2 \in E$ ($G = S_m$ on unordered pairs) and there are at most $O(\log x)$ cases where these

https://doi.org/10.1017/S0004972700021080 Published online by Cambridge University Press

integers coincide. The classification of simple groups is used to show that $e(x)$ is at most the expression above. This involves an examination of permutation representations of alternating groups and groups of Lie type.

5. Which permutations are excluded from primitive groups?

Let G be a primitive permutation group of degree n, $G \neq S_n, A_n$. We have seen that $|G|$ is much smaller than $n!$. Are there many permutations $g \in S_n$ which are excluded from membership of any such G? In 1873 Jordan [11] showed that any permutation of prime order p with exactly one cycle of length p and at least 3 fixed points is excluded from membership of any primitive $G \ (\neq S_n, A_n)$.

A permutation of $g \in S_n$ is said to have *type*

$$\mathbf{t} = 1^{a_1} 2^{a_2} \ldots n^{a_n}, \quad \sum i a_i = n,$$

if g has a_i cycles of length i for $i = 1, \ldots, n$. Let T_n be the set of types $\mathbf{t}$ of permutations in S_n such that no permutation of type $\mathbf{t}$ may belong to any primitive permutation group G of degree n, $G \neq S_n, A_n$. Then Jordan's result is that $\mathbf{t} = 1^a p^1 \in T_n$ where p is prime and $a = n - p \geq 3$. Of course the previous section shows that T_n contains all types for "almost all" n since for almost all n no non-trivial primitive groups exist. Nevertheless the sets T_n are very much of interest as long as the classification of primitive permutation groups is incomplete. Jordan announced similar results, namely that $1^a p^q \in T_n$ where p is prime $p > q$, $1 \leq q \leq 5$ and $a > q+1$. Proofs of these results did not appear until W.A. Manning published them in 1909 and 1915. The best result of this period was obtained by Manning in 1918 (see [17] for a summary of results of the time), namely

$$\mathbf{t} = 1^a p^q \in T_n, \quad p \text{ prime}, \quad 5 < q \leq (p+1)/2, \quad a > 4q - 4.$$

There were efforts to extend the range of q, but the lower bound on a

https://doi.org/10.1017/S0004972700021080 Published online by Cambridge University Press

had to increase markedly since the groups S_m and A_m, $m = q + (p+1)/2$, acting on unordered pairs contain an element of type $1^a p^q$ with $a = \left((2q-p)^2-1\right)/8$. In 1979, [17], it was shown that these were the only groups containing such elements; namely if $2 < q < p$ and $a > (5q-4)/2$ then either $\mathbf{t} = 1^a p^q \in T_n$, or $n = m(m-1)/2$, where $m = q + (p+1)/2$, $a = \left((2q-p)^2-1\right)/8$, and in this case A_m and S_m on unordered pairs are the only non-trivial primitive groups containing elements of type $1^a p^q$.

Very recently using the simple group classification Liebeck and Saxl [13] have been able to classify all primitive permutation groups which contain elements of type $1^a p^q$ for $q < p$ and any $a \geq 0$.

6. Primitive groups with given rank

Let $G \leq S_n$ be primitive and let $X_1 = \{1\}, X_2, \ldots, X_r$ be the orbits of the stabilizer G_1 of 1 in $\mathbf{n}$. Then G is said to have *rank* r. Clearly $r \geq 2$ and if $r = 2$, G is called *2-transitive*. One of the first major consequences of the classification of the simple groups was the classification of all finite 2-transitive groups. A proof of this important result is given in Cameron's paper [6], Theorem 5.3 (S). In his paper various other results about groups with given rank are discussed.

7. Primitive groups with given subdegree

With the notation of the previous section, the integers $d_i = |X_i|$, $1 \leq i \leq r$, are called the *subdegrees* of G. Let d be one of the subdegrees. It was conjectured by Sims that the order of G_1 is bounded by a function of d. That G is primitive is crucial for the conjecture to be true since the usual imprimitive action of $G = S_{(d+1)}$ wr S_k of degree $n = (d+1)k$ has a subdegree d and the stabilizer of a point has order $d!(d+1)!^{(k-1)}(k-1)!$. This conjecture has been much studied in the past 15

https://doi.org/10.1017/S0004972700021080 Published online by Cambridge University Press

years and many partial results have been obtained. In particular Thompson [20] showed that G_1 has a normal subgroup of prime power order whose index in G_1 is bounded by a function of d. It has been possible to use the classification together with Thompson's result to prove the conjecture true. Although no attempt was made to get the best possible function it was shown that $|G_1| \leq \exp(d^2 o(d))$, [8].

8. Closely related topics

Permutation groups often arise as automorphism groups of geometrical structures, and in these related areas one would expect to find new theorems which rely on the simple group classification. Algebraic graph theory is one field where several results have been proved and many more can be expected - for example one consequence of Sims' conjecture is that there are only a finite number of distance transitive graphs with a given valency, see [8]. In the theory of designs, already the 2-transitive designs have been classified (by W.M. Kantor (private communication)), and I would expect more results in this area also in the near future.

References

[1] M. Aschbacher and J.L. Scott, "Maximal subgroups of finite groups", *J. Algebra* (to appear).

[2] L. Babai, "On the order of uniprimitive permutation groups", *Ann. of Math.* (2) 113 (1981), 553-568.

[3] L. Babai, "On the order of doubly transitive permutation groups", *Invent. Math.* 65 (1982), 473-484.

[4] L. Babai, P.J. Cameron and P.P. Palfy, "On the orders of primitive groups with restricted nonabelian composition factors", *J. Algebra* 79 (1982), 161-168.

[5] A. Bochert, "Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann", *Math. Ann.* 33 (1889), 584-590.

[6] P.J. Cameron, "Finite permutation groups and finite simple groups", *Bull. London Math. Soc.* 13 (1981), 1-22.

[7] P.J. Cameron, P.M. Neumann and D.N. Teague, "On the degrees of primitive permutation groups", *Math. Z.* 180 (1982), 141-149.

[8] P.J. Cameron, C.E. Praeger, J. Saxl and G.M. Seitz, "On the Sims conjecture and distance transitive graphs", *Bull. London Math. Soc.* 15 (1983), 499-506.

[9] R.W. Carter, *Simple groups of Lie type* (John Wiley & Sons, London, New York, Sydney, 1972).

[10] J.F. Hurley and A. Rudvalis, "Finite simple groups", *Amer. Math. Monthly* 84 (1978), 693-714.

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

[12] L.G. Kovács, "Maximal subgroups in composite finite groups", in preparation.

[13] M. Liebeck and J. Saxl, "Primitive permutation groups containing an element of large prime order", unpublished.

[14] E. Mathieu, "Mémoire sur l'étude des fonctions de plusieurs quantités, sur le manière de les former et sur les substitutions qui les laissent invariables", *J. Math. Pure Appl. (Liouville)* (2) 6 (1861), 241-323.

[15] I. Miyamoto, "On primitive permutation groups of degree $2p = 4q + 2$, p and q being prime numbers", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 22 (1975), 17-23.

[16] P.M. Neumann and J. Saxl, "The primitive permutation groups of some special degrees, II: small multiples of certain large primes", *Math. Z.* 169 (1979), 205-222.

[17] C.E. Praeger, "On elements of prime order in primitive permutation groups", *J. Algebra* 60 (1979), 126-157.

[18] C.E. Praeger and J. Saxl, "On the orders of primitive permutation groups", *Bull. London Math. Soc.* 12 (1980), 303-307.

[19] C.C. Sims, "Computational methods in the study of permutation groups", *Computational problems in abstract algebra*, 169-183 (Proc. Conf. Oxford, 1967. Pergamon, London, 1970).

[20] J.G. Thompson, "Bounds for orders of maximal subgroups", *J. Algebra* 14 (1970), 135-138.

[21] H. Wielandt, *Finite permutation groups* (Academic Press, New York, London, 1964).

[22] H. Wielandt, *Permutation groups through invariant relations and invariant functions* (Ohio State University Lecture Notes. Ohio State University, Columbus, Ohio, 1969).

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