J. Austral. Math. Soc. **71** (2001), 243–258

BOUNDS ON FINITE QUASIPRIMITIVE PERMUTATION GROUPS

CHERYL E. PRAEGER and ANER SHALEV

To Laci Kovács on his 65th birthday

(Received 11 July 2001)

Communicated by R. A. Bryce

Abstract

A permutation group is said to be quasiprimitive if every nontrivial normal subgroup is transitive. Every primitive permutation group is quasiprimitive, but the converse is not true. In this paper we start a project whose goal is to check which of the classical results on finite primitive permutation groups also holds for quasiprimitive ones (possibly with some modifications). The main topics addressed here are bounds on order, minimum degree and base size, as well as groups containing special p-elements. We also pose some problems for further research.

2000 *Mathematics subject classification*: primary 20B05, 20B15; secondary 20B35.
Keywords and phrases: primitive permutation group, quasiprimitive permutation group.

1. Introduction

A permutation group G on a finite set Ω of size n is said to be *quasiprimitive* on Ω if every nontrivial normal subgroup of G is transitive on Ω. The name 'quasiprimitive' was suggested by Helmut Wielandt for this concept when it arose in work of Woflgang Knapp in the 1970's on subconstituents of finite primitive permutation groups (see [19, 20]). The concept of quasiprimitivity arose again in the study of certain families of arc-transitive graphs. In particular each finite, non-bipartite, 2-arc transitive graph was shown in [29] to be a cover of a possibly simpler graph admitting an automorphism group which was quasiprimitive on vertices as well as transitive on 2-arcs. It was

This paper forms part of an Australian Research Council large grant project of the first author. The second author acknowledges the support of the Israel Science Foundation, founded by the Israeli Academy of Science and Humanities.

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

this graph theoretic result which prompted a detailed study of finite quasiprimitive permutation groups.

As suggested by the name, quasiprimitivity is a generalisation of the primitivity property for permutation groups. A permutation group G on Ω is said to be *primitive* on Ω if G is transitive, and there are no nontrivial G-invariant partitions of Ω. (A partition of Ω is nontrivial if both the number and size of its blocks are greater than 1, and is G-invariant if the elements of G permute the blocks blockwise.) Every primitive permutation group G on Ω is quasiprimitive, since the set of orbits of a normal subgroup of G is a G-invariant partition. However the converse is not true since, for example, the permutation group induced by right multiplication of a nonabelian simple group on the set of right cosets of a non-maximal subgroup is quasiprimitive but not primitive. Hence, to some extent, a full understanding of quasiprimitive permutation groups requires determination of all subgroups of finite simple groups, which is a formidable (and in many ways hopeless) task. Still, we show below that many of the classical results on primitive permutation groups can be extended to quasiprimitive permutation groups.

More specifically, for finite primitive permutation groups G on Ω there are bounds available in terms of the degree $n = |\Omega|$ for the order $|G|$, the minimum base size of G, the minimum degree of G, and various other parameters. The purpose of this paper is to investigate which of these bounds for finite primitive permutation groups hold also for finite quasiprimitive groups. We show that many of them do carry over to quasiprimitive groups, with some requiring small modifications. We also pose some problems for further research.

The following basic observation seems to be rather useful, and already provides some preliminary consequences. Let G be a finite quasiprimitive permutation group on a set Ω of n points, where $n > 1$. Then there is a G-invariant partition Σ of Ω with blocks of size b, say, less than n, and with the blocks maximal with this property. We call such a partition a *maximal block system* for G. Clearly G induces a primitive permutation group on Σ. The kernel of this action is a normal subgroup of G which is intransitive on Ω (since $|\Sigma| > 1$), and hence is trivial (since G is quasiprimitive). Thus G is isomorphic to a primitive permutation group on Σ of degree $|\Sigma| = n/b \leq n$. This discussion suggests that many properties of primitive permutation groups may carry over easily to quasiprimitive groups. In some cases this is so, while other cases require more thought.

2. Elements of prime order in quasiprimitive permutation groups

Let G be a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on Ω, where $|\Omega| = n$, and suppose that G is quasiprimitive on Ω. In 1873 and 1875, Jordan ([15, 16] or see [13, Theorem 3.3E]) proved that if $n \geq p+3$, where p is a prime, and if G is primitive on Ω and contains a p-cycle, then $G = \mathrm{Alt}(\Omega)$ or $\mathrm{Sym}(\Omega)$. In particular if a primitive group on Ω contains a 3-cycle then Jordan proved that it contains the alternating group $\mathrm{Alt}(\Omega)$. This result carries over easily to quasiprimitive groups.

THEOREM 2.1. *Let G be a quasiprimitive permutation group of degree n such that G contains a p-cycle, for some prime p. Then either $G \geq \mathrm{Alt}(\Omega)$, or $n \leq p+2$ and $p \geq 5$. In particular, if G contains a 3-cycle, then G contains $\mathrm{Alt}(\Omega)$.*

PROOF. As discussed in the introduction, G acts faithfully on a maximal block system Σ. Let $g \in G$ act on Ω as a p-cycle. Since G is faithful on Σ, the element g must act nontrivially on Σ and hence must induce a p-cycle on Σ. However, if the size of the blocks in Σ is b then g acts on Ω as a product of b cycles of length p. We conclude that the blocks of Σ have size 1 and G is primitive on Ω, and hence the result follows from Jordan's Theorem. □

This seminal result of Jordan was extended and applied in a number of ways during the next century in the analysis of primitive permutation groups. Much of this analysis applies equally well to quasiprimitive groups.

One direction in which Theorem 2.1 was extended was in the study of elements of prime order in primitive groups. If a primitive group G of degree n, other than A_n or S_n, contains an element of prime order p with a small number q of cycles of length p, then it was shown that the number $n - qp$ of fixed points is bounded above by a linear function of q. The best result from the early 20th century is due to Manning [24], and dealt with the case $q \leq (p+1)/2$. A summary of these early results may be found in [28] or [35]. The linear bound on $n - qp$ cannot hold for larger values of q because the alternating and symmetric groups A_c and S_c ($c \geq p$) acting primitively on the $n = \binom{c}{2}$ unordered pairs of distinct points from a set of size c contain elements of order p with $q = c - (p+1)/2$ cycles of length p and a large number of fixed points: for example, if $c = (3p-1)/2$ then these elements of order p have $q = p - 1$ cycles of length p and $n - qp = q(q-2)/8$ fixed points in this action. It was shown in [28, Theorem A] that this action of alternating and symmetric groups on pairs was essentially the only obstruction for a linear bound for numbers of cycles less than p. The result in [28] is the best result of this type in the literature which does not depend on the finite simple group classification, and it holds with a small modification for quasiprimitive groups.

THEOREM 2.2. *Let G be a quasiprimitive permutation group on a set Ω of n points, such that, for some prime p, G contains an element of order p with q cycles of length p in Ω, where $2 \leq q < p$. Then one of the following holds.*

(i) $n - qp \leq 5q/2 - 1$;

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

(ii) *$G = A_n$ or S_n;*

(iii) *$G = A_c$ or S_c on unordered pairs ($n = \binom{c}{2}$, $c \geq p$, $q = c - (p+1)/2$).*

PROOF. If G is primitive on Ω then one of parts (i)–(iii) hold by [28, Theorem A]. So we may assume that G is imprimitive on Ω. Let Σ be a maximal block system for G in Ω, with r blocks of length b, where $n = br$. Then G acts faithfully and primitively on Σ. Let $g \in G$ be an element of order p with q cycles of length p in Ω, and let $f := n - qp$, the number of fixed points of g in Ω. Then g acts nontrivially on Σ, and each cycle of g of length p in Σ corresponds to b cycles of length p of g in Ω. Since $q < p$, it follows that $b \leq q < p$, and consequently g has $q' := q/b$ cycles of length p in Σ, and $f' := f/b$ fixed points in Σ. Also $q \geq b \geq 2$ (and in particular p is odd), and since p divides $|G|$ we have $r \geq p$. Let $B \in \Sigma$ and $\alpha \in B$.

If $p = 3$, then $q = b = 2$ and g acts as a 3-cycle on Σ, so by Jordan's Theorem, $G \geq A_r$. Therefore $G_B \geq A_{r-1}$, and G_B has G_α as a subgroup of index $b = 2$. It follows that $G = S_r$, $G_\alpha = A_{r-1}$, $n = br = 2r$. However A_r is intransitive and so G is not quasiprimitive. Thus $p \geq 5$.

Suppose first that $G \geq A_r$. Then $G_B = A_{r-1}$ or S_{r-1}, and G_α is a subgroup of G_B of index $b \leq q \leq p - 1 \leq r - 1$. If G_α contains A_{r-1}, then $G = S_r$, $G_\alpha = A_{r-1}$ and, as above, G is not quasiprimitive. Hence G_α does not contain A_{r-1}. Thus $G_\alpha \cap A_{r-1}$ is a proper subgroup of A_{r-1} of index at most $b \leq r - 1$. Since $r \geq p \geq 5$, it follows that either (a) $G_\alpha = G_{B,B'}$, for some $B' \in \Sigma \setminus \{B\}$, and $b = p - 1 = r - 1 = q$, or (b) $r = p = 7$ and $G_\alpha \cap A_6 = \mathrm{PSL}(2,5)$, or (c) $r = p = 5$. In each of these cases, p does not divide $|G_\alpha|$, so $f = 0$ and (i) holds. Thus we may assume that G does not contain A_r.

Suppose next that $q' = 1$, that is, $b = q$. Then by Jordan's Theorem, $f' \leq 2$, so $f = bf' \leq 2b = 2q \leq 5q/2 - 1$, and (i) holds. Thus we may assume further that $q' \geq 2$. Then one of cases (ii) or (iv) of [28, Theorem A] holds. If $G = A_c$ or S_c acting on Σ as on the unordered pairs from a set of size c, then (see the discussion preceding the statement of the theorem) $c = q' + (p+1)/2 \geq p$ so $q' \geq (p-1)/2$. It follows that $q' = (p-1)/2$, so $c = p$ and g has no fixed points in Σ, so (i) holds. Also if $f' \leq 5q'/2$, then $f \leq 5q/2$ and again (i) holds. □

Using [28, Theorem A] and the finite simple group classification, Liebeck and Saxl [22] obtained a complete classification of the finite primitive permutation groups which contain an element of prime order p with fewer than p cycles of length p. This classification could be extended to give a classification of the quasiprimitive permutation groups having this property. For the extension to quasiprimitive groups, a careful analysis of the result of [22] will be needed to identify any extra quasiprimitive almost simple examples.

PROBLEM 1. *Classify all finite quasiprimitive permutation groups which contain*

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

an element of prime order p with fewer than p cycles of length p.

3. Quasiprimitive Jordan groups

In 1871 Jordan [14] initiated an investigation of a family of primitive permutation groups which are now called Jordan groups. It was perhaps this investigation which led a few years later to his theorem discussed in Section 2. Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group on Ω, and let Γ be a subset of Ω such that $1 < |\Gamma| < |\Omega|$. We shall say that Γ is a *Jordan set* for G in Ω if the pointwise stabiliser $G_{(\Omega\setminus\Gamma)}$ in G of $\Omega \setminus \Gamma$ acts transitively on Γ. In this case we shall call G a *Jordan group* on Ω. One family of examples of Jordan sets arises from k-transitive permutation groups G, namely the sets obtained by removing $k - 1$ points from Ω. Such Jordan sets are called *trivial Jordan sets* and all other examples are said to be *nontrivial*. A Jordan group is called *nontrivial* if it has at least one nontrivial Jordan set.

In [14] Jordan studied primitive permutation groups which we would now call primitive Jordan groups. He proved that, if G is primitive on Ω and $G_{(\Omega\setminus\Gamma)}$ is primitive on Γ, then Γ is a trivial Jordan set for G. He also proved that, if Γ is a Jordan set for a primitive permutation group G on Ω, and $1 < |\Gamma| \leq |\Omega|/2$, then G is 3-transitive on Ω. The latter result was strengthened by Marggraf in 1892; Marggraf deduced that, if $1 < |\Gamma| < |\Omega|/2$ then G is $\mathrm{Alt}(\Omega)$ or $\mathrm{Sym}(\Omega)$ ([26], or see [35, Theorem 13.5]). Both of these theorems hold also for quasiprimitive groups.

THEOREM 3.1. *Let G be a quasiprimitive permutation group on a set Ω of n points, and suppose that a subset Γ of Ω is a Jordan set for G. Then*:

(i) *if $G_{(\Omega\setminus\Gamma)}$ is primitive on Γ, then Γ is a trivial Jordan set*;

(ii) *if $1 < |\Gamma| < n/2$, then $G = A_n$ or S_n.*

PROOF. We may assume that G is imprimitive. Let Σ be a maximal block system for G in Ω. Then G is faithful and primitive on Σ. It follows that Γ is a union of complete blocks of Σ, and that $H := G_{(\Omega\setminus\Gamma)}$ is transitive on the set Γ_Σ of blocks of Σ contained in Γ. If Γ_Σ consisted of a single block of Σ, then H would be contained in the kernel of G on Σ, which is not the case. Hence $1 < |\Gamma_\Sigma| < |\Sigma|$, and so Γ_Σ is a Jordan set for G in Σ.

If H is primitive on Γ then, since a block of Σ contained in Γ is a block of imprimitivity for the action of H on Γ, it follows that the blocks of Σ have size 1. Hence G is primitive, which contradicts our assumption. Thus G must be primitive in part (i), and so (i) is proved.

If $1 < |\Gamma| < n/2$, then $1 < |\Gamma_\Sigma| < |\Sigma|/2$, and so $G = A_r$ or S_r, where $r = |\Sigma|$. For $B \in \Sigma$, $B \not\subseteq \Gamma$, the stabiliser $G_B = A_{r-1}$ or S_{r-1} is transitive on B of degree

$b := |B| > 1$. In particular $r \geq 3$. However, H fixes B pointwise, and so the kernel of G_B on B is nontrivial. It follows that either (i) $G = S_r$, $b = 2$, and the pointwise stabiliser $G_{(B)} = A_{r-1}$, or (ii) $r = 5$, $G_{(B)} = Z_2 \times Z_2$, and $b = 3|G : G'|$. In case (i), the normal subgroup A_r is not transitive on Ω, so G is not quasiprimitive. In case (ii), since $1 < |\Gamma_\Sigma| < 5/2$, we have $|\Gamma_\Sigma| = 2$, and since the pointwise stabiliser of $\Sigma \setminus \Gamma_\Sigma$ contains H (and so is nontrivial), we must have $G = S_5$, and $H = Z_2$. This however contradicts the fact that H is transitive on the set Γ of $2b$ points. □

The finite primitive Jordan groups were studied in depth by Kantor in [17], and when the finite simple group classification was complete, he was able to complete the primitive Jordan group classification, see [18]. It is likely that this classification can be extended to the quasiprimitive case. We propose the following.

PROBLEM 2. *Classify all finite quasiprimitive Jordan groups.*

4. Orders of quasiprimitive groups

Let $G \leq \mathrm{Sym}(\Omega)$ where $|\Omega| = n$, and suppose that G is quasiprimitive on Ω. In this section we analyse various upper bounds available for the orders of primitive permutation groups to see which of them hold for quasiprimitive groups. The problem of finding an upper bound 'much smaller than $n!$' for the order of a primitive group of degree n which does not contain A_n was one of the central problems of 19th century Group Theory. The best result from that period, due to Bochert [6] in 1889 (or see [35, 14.2]), is that such groups have orders at most $n!/[(n+1)/2]!$. Bochert proved that a primitive subgroup of S_n of order greater than $[(n+1)/2]!$ must contain a 3-cycle, and then applied Jordan's Theorem (Theorem 2.1). It is very easy to extend this result to quasiprimitive groups.

THEOREM 4.1. *Let G be a quasiprimitive permutation group of degree n such that $A_n \not\subseteq G$. Then $|G| \leq n!/[(n+1)/2]!$.*

PROOF. By Bochert's result we may assume that G is quasiprimitive and imprimitive on Ω of degree n. Then, as discussed in the introduction, G is isomorphic to a primitive permutation group of degree r where r is a proper divisor of n. Thus $|G| \leq r!$, and it is easy to show that $r! \leq n!/[(n+1)/2]!$. □

The first significant improvement on Bochert's bound was made in 1969 by Wielandt. He proved [36, Theorem 8.7] that a simply primitive group (that is, a primitive ;roup which is not 2-transitive) of degree n has order less than c^n, for some constant $c \leq 24$. Wielandt's bound was extended in 1980 in [30] to all primitive

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

groups not containing A_n, and the value of the constant was reduced to $c = 4$. The bound has a number of advantages in applications, sometimes over asymptotically better bounds, since it is a simple function of n, and it holds for primitive permutation groups of all degrees n. With a little care we prove that the result of [30] holds also for finite quasiprimitive groups.

THEOREM 4.2. *Let G be a quasiprimitive permutation group of degree $n \geq 1$. Then either $|G| < 4^n$ or $G = A_n$ or S_n.*

PROOF. By [30], we may assume that G is quasiprimitive and imprimitive on Ω of degree n. Let Σ be a maximal block system for G in Ω with $r = n/b$ blocks of size b. Then G is isomorphic to a primitive permutation group on Σ and, since G is imprimitive on Ω, $b > 1$. If $G \not\cong A_r$ or S_r, then by [30], $|G| < 4^r < 4^n$. So we may assume that $G \cong A_r$ or S_r. Since G is quasiprimitive $G' = A_r$ is transitive on Ω.

Let $\alpha \in \Omega$, and let $\sigma \in \Sigma$ be the block containing α. Then G'_α is a proper subgroup of $G'_\sigma = A_{r-1}$. There is a maximum positive integer i such that $G'_\alpha \leq A_{r-i}$. If $i \geq 2$ then there is a second maximal block system Φ for G in Ω comprising the unordered pairs from Σ. Since G does not induce the full alternating or symmetric group on Φ, we have from [30] that $|G| < 4^{|\Phi|} < 4^n$. Thus we may assume that $i = 1$. Moreover, since $|G| \leq r!$ and we have $r! < 4^r < 4^n$ for $r \leq 7$, we may assume that $r \geq 8$. Then, in this final case, $G_\sigma = A_{r-1}$ or S_{r-1} induces a faithful quasiprimitive permutation group on the block σ of degree b. Moreover, since $i = 1$, this action is not the natural action of degree $r - 1$, and hence, again by [30], $|G_\sigma| < 4^b$ so $|G| = r|G_\sigma| < r \cdot 4^b < 4^n$. □

Not long after the exponential bound was proved, Babai obtained the first sub-exponential upper bound for the orders of primitive groups. Again the 2-transitive groups were treated separately from the simply primitive groups: for $G \leq S_n$, it was shown that $|G| < \exp(4n^{1/2}(\log n)^2)$ if G is simply primitive (of any degree $n > 1$) in [2, Section 3] and, for n sufficiently large, that $|G| < \exp\exp(1.18(\log n)^{1/2})$ if G is 2-transitive, and $A_n \not\subseteq G$, in [3, Theorem 1.1]. The bound for 2-transitive groups is better than the one for simply primitive groups, and moreover the 2-transitive bound was improved by Pyber in [34] to $|G| < \exp(32\log^3 n)$ if G is 2-transitive of degree $n \geq 400$ and $A_n \not\subseteq G$. Thus the simply primitive bound holds for all primitive groups not containing A_n provided that $n \geq n_{pr}$, for some constant n_{pr}. Babai [3, p. 473] gave a 'rough estimate' of n_{pr} as $5 \cdot 10^5$, and pointed out in [2, Comment in Section 3] that the simply primitive bound is close to best possible, since $G = S_c$ acting on $n = c(c-1)/2$ unordered pairs from a set of size c satisfies $|G| = \exp((1/\sqrt{2} + o(1))n^{1/2}\log n)$. We show that the simply primitive bound holds also for quasiprimitive groups (with a larger constant n_0).

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

THEOREM 4.3. *Let G be a quasiprimitive permutation group of degree n, such that $A_n \not\leq G$. There is a constant n_0 such that, if $n \geq n_0$, then* $|G| < \exp(4n^{1/2}\log^2 n)$.

PROOF. Set $f(n) = \exp(4n^{1/2}\log^2 n)$, and let n_{pr} be a constant such that $n_{pr} \geq 8$ and Babai's Theorem 'holds for n_{pr}', that is, for $n \geq n_{pr}$, a primitive group of degree n which does not contain A_n has order less than $f(n)$. Let $n_0 := n_{pr}!$. Now suppose that G is a quasiprimitive permutation group on Ω of degree $n \geq n_0$. Then by Babai's Theorem we may assume that G is imprimitive on Ω. Let Σ be a maximal block system for G in Ω with $r = n/b$ blocks of size b, so that G is isomorphic to a primitive permutation group on Σ and, since G is imprimitive on Ω, $b > 1$. If r were less than n_{pr}, then we would have $|G| \leq r! < n_{pr}! = n_0 \leq n$ and G could not be quasiprimitive of degree n. Thus $r \geq n_{pr}$.

The result follows from Babai's Theorem unless G contains A_r, so we may assume that $G = A_r$ or S_r. Let $\alpha \in \Omega$ and $\sigma \in \Sigma$ be the block containing α. Then $G'_\sigma = A_{r-1}$, and arguing as in the previous proof, we may assume that σ is the unique element of Σ fixed setwise by G_α. Since G is quasiprimitive, G'_σ is transitive on σ, and since A_{r-1} is a nonabelian simple group, G_σ is quasiprimitive on σ of degree b. Clearly $b \geq r - 1$, and as we have just observed, the action of G_σ on σ is not the natural action of degree $r - 1$, so (since $r - 1 \neq 6$) $b \geq r \geq n_{pr}$. Applying Babai's Theorem again, to the action of G_σ on σ, we find $|G| < rf(b) < f(n)$. □

As we mentioned above, the bound of Babai is almost best possible for primitive groups not containing A_n. Better bounds for primitive group orders are available if we specify a larger class of exceptions than just A_n and S_n, but the proofs usually rely on the classification of the finite simple groups. One of these bounds, namely $n^{c\log n}$, was obtained by Cameron [7, Section 6], or see [9, Theorem 5.8]. We show below that this bound also carries over for quasiprimitive groups with a larger class of exceptions than in the primitive case.

THEOREM 4.4. *Let G be a quasiprimitive permutation group of degree n. Then there exist constants c, c' such that either*

(a) $|G| \leq n^{c\log n}$, *or*

(b) *for positive integers m, k, l such that $k \leq c'$, $l \leq c'$ and $m > 4c'$, we have $G \leq S_m \wr S_l$ with* $\mathrm{soc}(G) = A_m^l$ *and* $(A_{m-k})^l \leq \mathrm{soc}(G)_\alpha \leq (S_{m-k} \times S_k)^l \cap \mathrm{soc}(G)$.

PROOF. By the result [7, Theorem 6.1(S)] of Cameron, either (a) or (b) holds, for some constants c, c', when G is primitive on Ω so we may assume that G is imprimitive. Let Σ be a maximal block system with blocks of size $b > 1$. Then applying Cameron's result again we deduce that either (a) holds or, for some $m > 4c'$ and $l \leq c'$, we have $A_m^l \leq G \leq S_m \wr S_l$ and for every choice of Σ there is an integer $k \leq c'$ such that the action of G on Σ is its product action with A_m acting on k-subsets.

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

Assume that the latter holds, set $N = \mathrm{soc}(G) = A_m^l$, and choose Σ with k ($k \le c'$) as large as possible. Let $\sigma \in \Sigma$. Then $N_\sigma = ((S_{m-k} \times S_k) \cap A_m)^l$. For $i = 1, \dots, l$, let π_i denote the projection of N_σ onto the copy of S_{m-k} in the i^{th} direct factor of N_σ.

Consider the subgroups $\pi_i(N_\alpha)$, where $\alpha \in \sigma$ and $1 \le i \le l$. Since G is quasiprimitive, N is transitive on Ω, so $G = NG_\alpha$. Hence G_α permutes transitively by conjugation the l simple direct factors of N, and also permutes transitively the subgroups $\pi_i(N_\alpha)$ ($1 \le i \le l$). In particular either all or none of the $\pi_i(N_\alpha)$ are transitive subgroups of S_{m-k}. Suppose first that $\pi_1(N_\alpha)$ is intransitive. Then $\pi_1(N_\alpha)$ leaves invariant a subset of size k', where $1 \le k' \le (m-k)/2$ and so $N_\alpha \le (S_{m-k'} \times S_{k'})^l \cap \mathrm{soc}(G)$. By our assumption in the previous paragraph about maximal block systems, $k' \le c'$. Thus $k + k' \le 2c' < m/2$, and since $N_\alpha \le (S_{m-k-k'} \times S_{k+k'})^l \cap \mathrm{soc}(G)$, our assumption about maximal block systems implies that $k + k' \le c'$, but this contradicts the maximality of k.

Thus $\pi_1(N_\alpha)$ is transitive. Suppose next that $\pi_1(N_\alpha)$ does not contain A_{m-k}. Then $|\pi_1(N_\alpha)| \le |S_{\lceil (m-k)/2 \rceil} \wr S_2|$ (for by Theorem 4.2 or 4.3 primitive groups have smaller order than this, and the upper bound given is the largest order of an imprimitive subgroup). Thus

$$b = |N_\sigma : N_\alpha| \ge \left(\frac{1}{2} \binom{m-k}{\lceil (m-k)/2 \rceil} \right)^l \ge 2^{(m-k)l/2}$$

and so $ml \le 2 \log_2 b + (c')^2$. Since $|G| \le m!^l l!$ it follows that (a) holds (with a possibly modified constant c). Thus we may assume that $\pi_1(N_\alpha)$ contains A_{m-k}. The derived group N'_α is therefore isomorphic to A^r_{m-k} for some $r \le l$. If $r = l$ then part (b) holds, while if $r < l$ then $b \ge |A_{m-k}|$ and arguing as before we find that (a) holds. □

In case (b), G has a maximal block system Σ such that the action of G on Σ is faithful and permutationally isomorphic to the product action with A_m or S_m acting on k-subsets. The proof of Cameron's result, and hence also of this result, relies on the finite simple group classification. The original statement of Cameron's theorem [7, Theorem 6.1(S)] gave an even smaller bound $n^{c \log \log n}$ with a longer list of exceptional primitive groups, namely either

(a) G has an elementary abelian regular normal subgroup, or

(b) $T^l \le G \le \mathrm{Aut}(T) \wr S_l$ ($l \ge 1$) in product action where T is either an alternating group acting on k-subsets, or a classical group acting on an orbit of subspaces (or in the case of $\mathrm{PSL}(d, q)$, on pairs of subspaces of complementary dimension).

A similar treatment to that in the proof above should identify the finite quasiprimitive permutation groups of degree n which have order greater than $n^{c \log \log n}$.

PROBLEM 3. *Classify the quasiprimitive permutation groups of degree n and order*

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

greater than $n^{c \log\log n}$.

If a quasiprimitive permutation group has a nontrivial abelian normal subgroup, then it is in fact primitive of affine type, see [29]. This means in particular that a soluble quasiprimitive permutation group is primitive, so for example, a result of Pálfy and Wolf [27, 37] may be restated as: a quasiprimitive soluble permutation group of degree n has order at most $24^{-1/3}n^{1+c_0}$, where $c_0 = 2.243\ldots$. Finally in this section we mention a result of Pyber [32] (or see [33, Theorem 2.10]) on the orders of the cyclic composition factors of a primitive group, which extends immediately to quasiprimitive groups (because a quasiprimitive group is faithful on a maximal block system).

THEOREM 4.5. *Let G be a quasiprimitive permutation group of degree n. Then*

(a) *the product of the orders of the cyclic composition factors of G is at most $24^{-1/3}n^{1+c_0}$, where c_0 is the same constant as in the Pálfy-Wolf result mentioned above, and*

(b) *the number of non-cyclic composition factors of G is at most* $\log n$.

5. Bases of quasiprimitive groups

A *base* of a permutation group G on a set Ω is a sequence $\alpha_1, \alpha_2, \ldots, \alpha_b$ of elements of Ω such that the only element of G which fixes each of the α_i is the identity element. By considering the chain of stabiliser subgroups

$$G \geq G_{\alpha_1} \geq G_{\alpha_1\alpha_2} \geq \cdots \geq G_{\alpha_1\alpha_2\cdots\alpha_b} = \{1_G\} \tag{1}$$

it is clear that $|G| \leq n^b$. Thus a bound on b yields a bound on $|G|$. In fact, the subexponential bound of Babai [2] for simply primitive groups of degree n was proved by showing that such groups have a base of size at most $4\sqrt{n}\log n$. For such estimations it is therefore sensible to require that each of the inclusions in (1) be proper. Such a base is said to be *irredundant*. Moreover we are interested in the *minimum base size* $b(G)$ for a permutation group G. Of course a base of minimum size is irredundant, and we have $2^{b(G)} \leq |G| \leq n^{b(G)}$. It therefore follows from [34] that for n sufficiently large, a 2-transitive group G of degree n, such that G does not contain A_n, also has $b(G)$ less than Babai's simply primitive bound above, so this bound holds for all primitive groups of degree n which do not contain A_n. The crucial but elementary fact which allows results about base sizes for primitive groups to be extended to quasiprimitive groups is the following lemma.

LEMMA 5.1. *Let G be a quasiprimitive permutation group on a set Ω of size n, and let Σ be a maximal block system for G in Ω. Let $b_\Omega(G)$, $b_\Sigma(G)$ denote the minimal*

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

base sizes of the permutation groups induced by G on Ω and Σ respectively. Then $b_\Omega(G) \leq b_\Sigma(G)$.

PROOF. Let $\sigma_1, \sigma_2, \ldots, \sigma_b$ be a base for G in Σ, and let $\alpha_i \in \sigma_i$ for each $i = 1, \ldots, b$. Suppose that $g \in G$ fixes each of the α_i. Then g also fixes each of the σ_i setwise and hence acts trivially on Σ, since $\sigma_1, \sigma_2, \ldots, \sigma_b$ is a base. It follows that $g = 1$ since G is faithful on Σ. Hence $\alpha_1, \alpha_2, \ldots, \alpha_b$ is a base for G in Ω. □

Using Lemma 5.1, it follows immediately that the bound discussed above for base sizes of primitive groups also holds for quasiprimitive groups. Let n_0 be as in the previous section.

THEOREM 5.2. *Let G be a quasiprimitive permutation group of degree $n \geq n_0$ such that $A_n \not\leq G$. Then $b(G) \leq 4\sqrt{n}\log n$.*

A number of additional results on bases for primitive groups have immediate consequences for quasiprimitive groups, in terms of actions on maximal block systems. We provide two examples below.

It follows from Liebeck's base bound [21] for primitive groups that, if G is a quasiprimitive permutation group of degree n, then either

(a) $b(G) \leq 9\log n$, or

(b) $A_m^l \leq G \leq S_m \wr S_l$ ($l \geq 1$) and G induces a product action on a maximal block system, where the action of A_m is on k-subsets ($k \geq 1$).

The second example concerns the proof in [23] of a conjecture of Cameron and Kantor (see [8, Conjecture 3.4], or [10, page 260]) that, for almost simple primitive groups G, in 'most' cases $b(G)$ is bounded above by an absolute constant c. A group G is said to be *almost simple* if $T \leq G \leq \mathrm{Aut}(T)$ for some nonabelian simple group T. If G is an almost simple classical group with socle T and natural module V over a field of characteristic p, then a subgroup H of G is called a *subspace subgroup* if one of the following holds.

(1) H is the stabiliser in G of a proper nonzero subspace U of V, where U is totally singular, non-degenerate, or, if G is orthogonal and $p = 2$, a non-singular 1-space (U is any subspace if $T = \mathrm{PSL}(V)$);
(2) $T = \mathrm{PSL}(V)$, G contains a graph automorphism of T, and H is the stabiliser of a pair U, W of proper nonzero subspaces of V such that $\dim V = \dim U + \dim W$ and either $U \subseteq W$, or $V = U \oplus W$;
(3) $T = \mathrm{Sp}_{2m}(q)$, where $q = 2^a \geq 2$ and $H \cap T = \mathrm{O}_{2m}^{\pm}(q)$.

Note that, in (3), $T \cong \mathrm{O}_{2m+1}(q)$ and under this isomorphism $H \cap T$ is a stabiliser of a $(2m)$-dimensional subspace of the natural $(2m+1)$-dimensional module. A *subspace action* of a classical group G is an action of G by right multiplication on

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

the set of right cosets of a subspace subgroup. It follows immediately from [23, Theorem 1.3] and Lemma 5.1 that there exists an absolute constant c such that, if G is an almost simple quasiprimitive permutation group on a finite set Ω, then one of

(a) $b(G) \leq c$; or

(b) G is A_m or S_m and the action of G on a maximal block system in Ω is its action on k-subsets of $\{1, \dots , m\}$ or on partitions of $\{1, \dots , m\}$ into k parts of size m/k $(k \geq 1)$; or

(c) G is a classical group and G induces a subspace action on a maximal block system in Ω.

Moreover, excluding groups in parts (b) and (c), the probability that a random c-tuple of elements of Ω forms a base for G tends to 1 as $|G| \to \infty$.

PROBLEM 4. *Extract more information about the action of G above, beyond the information given about its action on a maximal block system.*

6. Quasiprimitive groups with restricted sections

Many of the bounds discussed in Sections 4 and 5 can be improved if the quasiprimitive group satisfies certain restrictions on the nature of its composition factors or sections. (A *section* of a group G is a quotient group of a subgroup of G.) The first result of this nature was due to Babai, Cameron and Palfy [4] in 1982. They obtained a polynomial bound on the order of primitive groups which satisfied certain restrictions on their non-cyclic composition factors. Their proof relies on the finite simple group classification. The size of the exponent in this polynomial bound was investigated further in [5], and in that paper a refinement was given for the definition of the restricted family of groups involved. For a positive integer d, let Γ_d denote the class of groups which do not involve the alternating group A_d as a section. Since a quasiprimitive permutation group acts faithfully on a maximal block system, the result of [4] (or see [33, Theorem 2.8]) yields immediately the following information about quasiprimitive groups.

THEOREM 6.1. *Let $G \in \Gamma_d$, and suppose that G is a quasiprimitive permutation group on a set Ω of size n. Then $|G| \leq n^{c(d)}$, for some constant $c(d)$.*

It was shown by Pyber [32] (or see [33, Theorem 2.9]) that $c(d)$ is bounded above by a linear function of d.

These results suggest that the minimum base size $b(G)$ for a quasiprimitive group $G \in \Gamma_d$ may be bounded by a linear function of d. That this is the case for primitive groups was proved recently by Liebeck and the second author in [23, Theorem 1.4], and extends immediately to quasiprimitive groups.

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

THEOREM 6.2. *Let $G \in \Gamma_d$, and suppose that G is a quasiprimitive permutation group of degree n. Then $b(G)$ is bounded above by a linear function of d.*

7. Minimal degree and fixity for quasiprimitive groups

One of the early ways of investigating the orders of primitive groups was to study their minimal degrees. For $G \leq \mathrm{Sym}(\Omega)$, the *minimal degree* $m(G)$ of G is the minimum number of points of Ω moved by a non-identity permutation in G. If we wish to specify the set acted upon, we write $m_\Omega(G)$ for $m(G)$. A lower bound on $m(G)$ in terms of n could be used to obtain an upper bound on $|G|$ since, clearly, $|G| \leq n^{n-m(G)}$. More recently it has become convenient to study the *fixity* $\mathrm{fix}(G)$ of a subgroup $G \leq \mathrm{Sym}(\Omega)$ which is defined as the maximum of the number $\mathrm{fix}(g)$ of points of Ω fixed by non-identity elements $g \in G$: so $m(G) + \mathrm{fix}(G) = |\Omega|$.

There is a simple inequality relating the minimal degree of a quasiprimitive group with the minimal degree of its action on a maximal block system.

LEMMA 7.1. *Let G be a quasiprimitive permutation group on a set Ω of size n, and let Σ be a block system for G in Ω with blocks of size $s < n$. Then $m_\Omega(G) \geq s \cdot m_\Sigma(G)$.*

PROOF. Set $m := m_\Sigma(G)$ and let $g \in G \setminus \{1\}$. Since G is faithful on Σ, g moves at least m blocks of Σ. Then, since g moves all of the points of Ω in the blocks of Σ which it moves, it follows that g moves at least ms points of Ω. Hence $m_\Omega(G) \geq s \cdot m_\Sigma(G)$. □

The best lower bound on $m(G)$, for primitive permutation groups G, obtained before the classification of finite simple groups follows from the work of Babai [2] discussed in Section 4. If G is simply primitive of degree n, then Babai showed that $m(G) \geq (\sqrt{n} - 1)/2$. That this inequality (and indeed better ones!) also hold for 2-transitive groups not containing A_n was known already in the 1930's from work of Manning [25] (or see [35, Theorem 15.1]). We show that Babai's bound holds for quasiprimitive groups.

THEOREM 7.2. *Let G be a quasiprimitive permutation group on a set Ω of size n such that $G \neq A_n$ or S_n. Then $m(G) \geq (\sqrt{n} - 1)/2$.*

PROOF. We may assume that G is imprimitive on Ω. Let Σ be a maximal block system for G in Ω, and let $|\Sigma| = r$ and $s = n/r$. Now G is primitive and faithful on Σ of degree r, and since G is quasiprimitive all nontrivial normal subgroups of G are transitive on Ω. This means in particular that G has no normal subgroups acting regularly on Σ, and hence $r \geq 5$. If $G \not\cong A_r$ or S_r then by Babai's result and

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

Lemma 7.1, $m_\Omega(G) \geq s(\sqrt{r}-1)/2$, and since $r \geq 5$, this latter quantity is at least $(\sqrt{sr}-1)/2 = (\sqrt{n}-1)/2$.

Thus we may assume that $G \cong A_r$ or S_r, and we have that $G' = A_r$ is transitive on Ω. Let $\sigma \in \Sigma$, and $\alpha \in \sigma$. Then $G_\alpha < G_\sigma = A_{r-1}$ or S_{r-1}, and $(G')_\sigma = A_{r-1}$ is transitive on σ (since G' is transitive on Ω). Suppose that G_σ is quasiprimitive and faithful on σ. This is certainly true if $r \geq 6$ since A_{r-1} is transitive on σ. Let Δ be a maximal block system for G_σ in σ with blocks of size $s' \geq 1$, and let $\delta \in \Delta$ be the block containing α. By Lemma 7.1, $m_\sigma(G_\sigma) \geq s' \cdot m_\Delta(G_\sigma)$. Now G_σ is faithful and primitive on Δ since G_σ is faithful and quasiprimitive on σ and since Δ is maximal. It follows from Babai's result that either (i) $G_\sigma \cong A_{s/s'}$ or $S_{s/s'}$, or (ii) $m_\Delta(G_\sigma) \geq (\sqrt{|\Delta|}-1)/2$.

Consider first case (i). Here $s/s' = |\Delta| = r-1$, and provided $r \neq 7$, it follows that G_α is contained in the stabiliser of two elements of Σ, so G has a second maximal block system on which it acts as A_r or S_r on unordered pairs. In this case the theorem follows from Babai's result applied (as above) to this second block system. If $r = 7$ then either this argument is valid or $G_\delta = \mathrm{PSL}(2,5)$ or $\mathrm{PGL}(2,5)$ and is transitive on $\Sigma \setminus \{\sigma\}$. Let $x \in G, x \neq 1$. Since G is faithful on Σ, the number f of blocks of Σ fixed setwise by x is at most 5. Since G_σ is faithful on Δ, it follows that x moves at least $2s'$ points in each of the f blocks of Σ it fixes setwise. Hence x moves at least $2s'f + |\sigma|(7-f) = 2s'f + 6s'(7-f) = s'(42-4f) \geq 22s'$ points of Ω, and this is greater than $(\sqrt{42s'}-1)/2 = (\sqrt{n}-1)/2$.

Now consider case (ii). Here $m_\sigma(G_\sigma) \geq s' \cdot (\sqrt{|\Delta|}-1)/2 \geq (\sqrt{s}-1)/2$. Let $x \in G$, $x \neq 1$, and suppose that x fixes setwise exactly f blocks σ of Σ. We have just shown that the number of points of each such σ moved by x is at least $m_\sigma(G_\sigma) \geq (\sqrt{s}-1)/2$. Thus x moves at least $f(\sqrt{s}-1)/2 + (r-f)s \geq r(\sqrt{s}-1)/2 \geq (\sqrt{n}-1)/2$ points of Ω.

The remaining case to be considered is the case where $r = 5$ and $(G')_\sigma = A_4$ is transitive on σ but its normal subgroup $O_2((G')_\sigma)$ of order 4 is intransitive. Hence $s = 3, 6$ or 12 according as $O_2((G')_\sigma)$-orbits in σ have length 1, 2 or 4. Since G is faithful on Σ each non-identity element of G moves at least two blocks of Σ and hence at least $2s$ points of Ω. Since $2s \geq (\sqrt{5s}-1)/2$ for all possible values of s, the result follows in this final case also. □

8. A density result for quasiprimitive groups

In 1982 Cameron, Neumann and Teague [11] showed that the number of integers $n \leq x$ which occur as degrees of primitive permutation groups, other than A_n and S_n in their natural action, is at most $O(x/\log x)$. By the prime number theorem there are at most $O(x/\log x)$ integers $n \leq x$ which are primes, and indeed the leading term in the

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

estimate given in [11] for the density of primitive group degrees is accounted for by primitive groups of degree p (for example Z_p) or $p+1$ (for example, PSL(2, p)), for primes p. It is somewhat surprising that this result can be extended for quasiprimitive permutation groups. Indeed we have

THEOREM 8.1. *There is a constant c such that, for all $x > 0$, at most $cx/\log x$ integers $n \leq x$ occur as degrees of quasiprimitive permutation groups other than A_n and S_n in their natural actions.*

Thus for most integers n the only quasiprimitive permutation groups of degree n are A_n and S_n acting naturally; in particular, for most integers n every quasiprimitive group of degree n is in fact primitive. Another by-product of Theorem 8.1 is that the set of indices of subgroups of finite simple groups excluding that of A_{n-1} in A_n has density zero. The proof of Theorem 8.1, which relies heavily on the finite simple group classification and subgroup structure, will appear in [31].

References

[1] M. Aschbacher and R. M. Guralnick, 'On abelian quotients of primitive groups', *Proc. Amer. Math. Soc.* **107** (1989), 89–95.

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

[3] ———, 'On the order of doubly transitive permutation groups', *Invent. Math.* **65** (1982), 473–484.

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

[5] L. Babai, W. M. Kantor and E. M. Luks, 'Computational complexity and the classification of finite simple groups', in: *Proc. 24th IEEE FACS* (1983) pp. 162–171.

[6] A. Bochert, 'Uber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann', *Math. Ann.* **33** (1889), 584–590.

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

[8] ———, 'Some open problems on permutation groups', in: *Groups, combinatorics and geometry* (eds. M. W. Liebeck and J. Saxl), London Math. Soc. Lecture Note Series 165 (Cambridge Univ. Press, Cambridge, 1992) pp. 340–350.

[9] ———, 'Permutation groups', in: *Handbook of combinatorics* (eds. R. Graham, M. Grötschel and L. Lovász) (Elsevier Science B. V., 1995) chapter 12, pp. 611–645.

[10] P. J. Cameron and W. M. Kantor, 'Random permutations: some group-theoretic aspects', *Combinatorics, Probability and Computing* **2** (1993), 257–262.

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

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wison, *An atlas of finite groups* (Clarendon Press, Oxford, 1985).

[13] J. D. Dixon and B. Mortimer, *Permutation groups* (Springer, New York, 1996).

[14] C. Jordan, 'Théorèmes sur les groupes primitifs', *J. Math. Pures Appl.* **16** (1871), 383–408.

[15] ———, 'Sur la limite de transitivité des groupes non alternés', *Bull. Soc. Math. France* **1** (1873), 40–71.

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press

[16] ———, 'Sur la limite du degré des groupes primitifs qui contiennent une substitution donnée', *J. Reine Angew. Math.* **79** (1875), 248–258.

[17] W. M. Kantor, 'Jordan groups', *J. Algebra* **12** (1969), 471–493.

[18] ———, 'Homogeneous designs and geometric lattices', *J. Combin. Theory Ser. A* **38** (1985), 66–74.

[19] W. Knapp, *Subkonstituenten und Struktur der Stabilisatoruntergruppe einer einfach transitiven Permutationsgruppe* (Ph.D. Thesis, Eberhard-Karls-Universtät Tübingen, Tübingen, 1971).

[20] ———, 'On the point stabilizer in a primitive permutation group', *Math. Z.* **133** (1973), 137–168.

[21] M. W. Liebeck, 'On the minimal degrees and base sizes of primitive groups', *Arch. Math.* **43** (1984), 11–15.

[22] M. W. Liebeck and J. Saxl, 'The primitive permutation groups containing an element of large prime order', *J. London Math. Soc. (2)* **31** (1985), 237–249.

[23] M. W. Liebeck and A. Shalev, 'Simple groups, permutation groups, and probability', *J. Amer. Math. Soc.* **12** (1999), 497–520.

[24] W. A. Manning, 'On the order of primitive groups, I-III', *Trans. Amer. Math. Soc.* **10** (1909), 247–258; **16** (1915), 139–147; **19** (1918), 127–142.

[25] ———, 'The degree and class of multiply transitive groups', *Trans. Amer. Math. Soc.* **35** (1933), 585–599.

[26] B. Marggraf, *Uber primitive Gruppen mit transitiven Untergruppen geringeren Grades* (Dissertation, Giessen, 1892).

[27] P. P. Pálfy, 'A polynomial bound for the orders of primitive soluble groups', *J. Algebra* **77** (1982), 127–137.

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

[29] ———, 'An O'Nan-Scott Theorem for finite quasiprimitive permutation groups, and an application to 2-arc transitive graphs', *J. London Math. Soc. (2)* **47** (1993), 227–239.

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

[31] C. E. Praeger and A. Shalev, 'Indices of subgroups of finite simple groups and quasiprimitive permutation groups', preprint, 2001.

[32] L. Pyber, 'Pálfy-Wolf type theorems for completely reducible subgroups of GL(n, p^{α})', in preparation.

[33] ———, 'Asymptotic results for permutation groups', *DIMACS Series in Discrete Math. and Computer Science* **11** (1993), 197–219.

[34] ———, 'On the orders of doubly transitive permutation groups, elementary estimates', *J. Combin. Theory (A)* **62** (1993), 361–366.

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

[36] ———, 'Permutation groups through invariant relations and invariant functions', Department of Mathematics, Ohio State University, Columbus, Ohio, 1969. (Reprinted in *Mathematische Werke*, Volume 1, de Gruyter, Berlin, 1994, pp. 237–296).

[37] T. R. Wolf, 'Soluble and nilpotent subgroups of GL(n, q^m)', *Canad. J. Math.* **34** (1982), 1097–1111.

Department of Mathematics and Statistics
University of Western Australia
35 Stirling Highway
Crawley WA 6009
Australia
e-mail: praeger@maths.uwa.edu.au

Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel
e-mail: shalev@math.huji.ac.il

https://doi.org/10.1017/S1446788700002895 Published online by Cambridge University Press