PACIFIC JOURNAL OF MATHEMATICS
Vol. 136, No. 2, 1989

FINITE PERMUTATION GROUPS WITH LARGE ABELIAN QUOTIENTS

L. G. KOVÁCS AND CHERYL E. PRAEGER

We show that if G is a group of permutations on a set of n points and if $|G/G'|$ denotes the order of its largest abelian quotient, then either $|G/G'| = 1$ or there is a prime p dividing $|G/G'|$ such that $|G/G'| \leq p^{n/p}$. Equality holds if and only if G is a p-group which is the direct product of its transitive constituents, with each of those having order p, except when $p = 2$ in which case one must also allow as transitive constituents the groups of order 4, the dihedral group of order 8 and degree 4, and the extraspecial group of order 32 and degree 8.

1. Introduction. In this paper we obtain upper bounds on the orders of abelian quotients of permutation groups in terms of the degrees of the groups, and identify the groups which attain these bounds. First we consider abelian p-quotients for a given prime p.

Recall that a constituent of a permutation group is the restriction of the group to some union of orbits, the restrictions to single orbits being the transitive constituents. By a *transitive non-p'-constituent* we mean a transitive constituent whose order is divisible by p. The *largest p'-constituent* is the restriction to the union of those orbits (if any) on which the group acts as a p'-group.

THEOREM. *If G is a group of permutations on a finite set and if kp denotes the number of points moved by a Sylow p-subgroup of G, then the largest abelian p-quotient of G has order at most p^k. This maximum is achieved by G if and only if G is the direct product of its largest p'-constituent (if any) and of its transitive non-p'-constituents, each of the latter being from the following list of groups*:

(i) *C_p, of order and degree p*;

(ii) *C_4, $C_2 \times C_2$, and D_8, of degree* 4, *and the central product $D_8 \curlyvee D_8$ of order* 32 *and degree* 8, *when $p = 2$*;

(iii) *the affine groups* AGL(1,3) *and* AGL(1,5), *when $p = 2$*;

(iv) *the affine group* AGL$(1, p + 1)$, *when $p + 1$ is a power of* 2.

COROLLARY. *If G is a permutation group of degree n and if $|G/G'|$ denotes the order of its largest abelian quotient, then either $|G/G'| = 1$ or $|G/G'|$ has a prime divisor p such that $|G/G'| \leq p^{n/p}$. Consequently, $|G/G'| \leq 3^{n/3}$. Given a prime p, one has $|G/G'| = p^{n/p}$ if and only if G is the direct product of its transitive constituents and each constituent is as in* (i) *or* (ii) *above* (*so in particular G is a p-group*).

The original motivation for this investigation came from a problem in [2] about the *minimal* (*faithful*) *degree* of an abstract group. Let $\mu(G)$ be the least integer for which G has a faithful permutation representation of degree $\mu(G)$.

Conjecture. If G/N is abelian, then $\mu(G/N) \leq \mu(G)$.

Our theorem implies that this holds whenever G/N is an elementary abelian p-group. Indeed, in that case, if $|G/N| = p^r$ then $\mu(G/N) = rp$. Consider G a permutation group of degree $\mu(G)$ and denote by kp the number of points moved by a Sylow p-subgroup: then obviously $kp \leq \mu(G)$. By the theorem we have $p^r = |G/N| \leq p^k$ so $r \leq k$, and hence $\mu(G/N) = rp \leq kp \leq \mu(G)$. Further, the theorem enables one to identify the groups G and the elementary abelian p-quotients G/N for which $\mu(G/N) = \mu(G)$. In general, the conjecture remains open.

A second motivation came from a question of L. Babai, who asked (in a private communication) for an upper bound on $|G/G'|$ for transitive G of degree n. The bound provided by the corollary is exponential in n; is there a better one for transitive groups? We expect there is one which is exponential in $n(\log n)^{-1/2}$. For examples showing that one cannot hope for improvements beyond that, see Audu [1], Kovács and Newman [5].

Finally, we note that $|G/G'| \leq p^{n/p}$ may hold for more than one, yet need not hold for all, prime divisors p of $|G/G'|$. For example, when G is $C_2 \times C_3 \times C_5$ of degree 2+3+5, one has

$$3^{10/3} = 9^{5/3} > 8^{5/3} = 2^{10/2} > |G/G'| > 5^{10/5}.$$

2. Preliminaries. We shall need some elementary facts concerning (sub)direct products of (abstract) finite groups. For a fixed prime p and each finite group G, write $G^* = G'\mathbf{O}^p(G)$, so the largest abelian p-quotient of G is G/G^*. Let $p^{\psi(G)}$ denote the maximum of the orders of the abelian p-sections of G (that is, of the abelian p-quotients K/L where $L \trianglelefteq K \leq G$). Let G be a subdirect product of A and B: that is,

$$G \leq A \times B = AG = BG. \tag{1}$$

It is clear that for the mutual commutator subgroup $[A \cap G, A]$ we have

$$(2) \qquad [A \cap G, A] \leq A \cap G',$$

and that

$$(3) \qquad \text{if } A \leq G \quad \text{then } G = A \times B.$$

Obviously, $\psi(A) + \psi(B) \leq \psi(A \times B)$, and it is easy to see that in fact

$$(4) \qquad \psi(A) + \psi(B) = \psi(A \times B).$$

Indeed, let G be a subgroup of $A \times B$ such that

$$(5) \qquad p^{\psi(A \times B)} = |G/G^*|:$$

towards showing that $|G/G^*| \leq p^{\psi(A)+\psi(B)}$, we first replace A and B by $A \cap BG$ and by $AG \cap B$, respectively, so (1) holds, and then argue as follows. Note that

$$\begin{gathered}
(A \cap G)G^*/G^* \cong (A \cap G)/(A \cap G^*), \\
G/(A \cap G)G^* = G/(G \cap AG^*) \cong AG/AG^* = AB/AG^* \cong B/(AG^* \cap B), \\
(A \cap G)^* \leq A \cap G^*, \\
(B \cap G)^* \leq B \cap G^*;
\end{gathered}$$

so (see Figure 1)

$$\begin{aligned}
p^{\psi(A)+\psi(B)} \leq p^{\psi(A \times B)} &= |G/G^*| \\
&= |(A \cap G)G^*/G^*|\,|G/(A \cap G)G^*| \\
&= |(A \cap G)/(A \cap G^*)|\,|B/(AG^* \cap B)| \\
&\leq |(A \cap G)/(A \cap G)^*|\,|B/B^*| \\
&\leq p^{\psi(A)}p^{\psi(B)}.
\end{aligned}$$

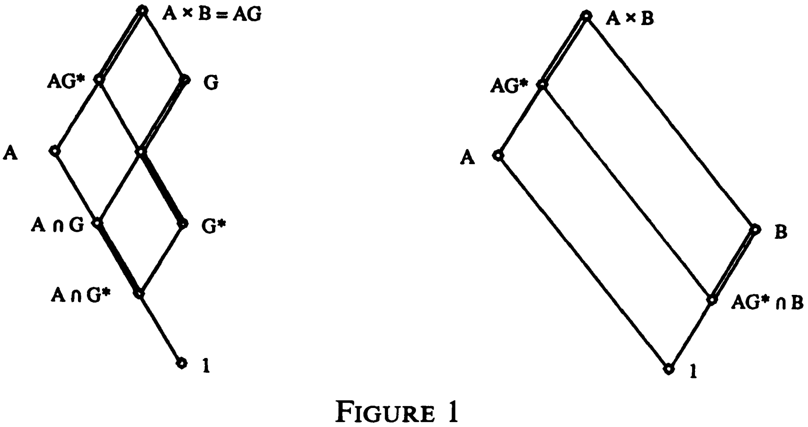

FIGURE 1

It follows that all these inequalities are in fact equalities: so (4) is proved, and as a bonus we get that (1) and (5) together imply that

(6) $(A \cap G)^* = A \cap G^*,$

(7) $|(A \cap G)/(A \cap G^*)| = p^{\psi(A)},$

(8) $B^* = AG^* \cap B,$

(9) $|B/B^*| = p^{\psi(B)}.$

By symmetry, they also imply that

(6′) $(B \cap G)^* = B \cap G^*,$

(7′) $|(B \cap G)/(B \cap G^*)| = p^{\psi(B)},$

(8′) $A^* = A \cap BG^*,$

(9′) $|A/A^*| = p^{\psi(A)}.$

We shall also need some facts concerning permutation groups. The Sylow p-subgroup of the symmetric group of degree p^2 is sufficiently well known (the wreath product of two groups of order p):

(10) in this, no transitive subgroup has an abelian quotient of order p^p except when $p = 2$, in which case C_4, $C_2 \times C_2$, and D_8 are the relevant examples.

In the holomorph of D_8, the left and the right translations form two copies of D_8 which centralize each other and meet precisely in their common centre; their product is the extraspecial group $D_8 \curlyvee D_8$. In any holomorph the two translation groups have a common complement, namely the automorphism group: here that is abstractly isomorphic to D_8. The involution (in the symmetric group on the set of the elements of the original group) which inverts each group element always normalizes the automorphism group and interchanges the two translation groups; an order count shows that here the holomorph and that involution generate a Sylow 2-subgroup P of the symmetric group of degree 8 (on the set of elements of the original D_8). We leave it to the reader to establish the following.

(11) The only transitive subgroup of P which has an abelian quotient of order at least 16 is the product $D_8 \curlyvee D_8$ of the two translation groups.

(12) Let A and A_1 be groups of permutations on the same set, with $A_1 \leq A$. Suppose that either A is one of the transitive groups listed in the theorem or A_1 is one of the nilpotent groups listed there. If $[A_1, A] \leq A_1'$ and, for the relevant prime, $\psi(A_1) \geq \psi(A)$, then $A_1 = A$.

(13) If G is a transitive group of permutations on a set Ω and if the stabilizer G_α of a point α, as group of permutations on $\Omega \setminus \{\alpha\}$, is one of the transitive groups listed in the theorem, then either G is one of the affine groups listed there or $|G/G'| \leq 2$ and a Sylow 2-subgroup of G moves more than 2 points.

In verifying (13), it is convenient to distinguish two cases: under the hypotheses *either* G_α is nilpotent of class at most 2 so G is soluble (Deskins, Janko, Thompson; see Huppert [**3**], IV.7.4), Ω is a vector space, and G_α acts on Ω faithfully as an irreducible linear group, *or* G_α is sharply 2-transitive, so G is sharply 3-transitive, in which case $|G/G'| \leq 2$ (Zassenhaus; see Huppert and Blackburn [**4**], XI.2.1 and XI.2.6).

3. Proofs. First we prove the theorem for p-groups. In this case, it has the following simpler form.

(14) If a p-group G is a permutation group of degree kp, then $|G/G'| \leq p^k$. Equality holds if and only if G is the direct product of its transitive constituents and each of these is one of the groups listed in (i) and (ii) of the theorem.

In fact we shall show by induction on k that if $|G/G'| \geq p^k$ then G is the product of its transitive constituents and each of these is one of the groups listed: $|G/G'| = p^k$ is then automatic. The claim is obvious when $k = 1$. For the inductive step, suppose $k > 1$.

Consider first the case of intransitive G. Let A be a nontrivial transitive constituent of G, and B the restriction of G to the union of the other orbits: then (1) holds. Say, the degree of A is lp; then the degree of B is $(k-l)p$, and the inductive hypothesis gives that $\psi(A) \leq l$, $\psi(B) \leq k - l$. By (4) we can now conclude that

$$p^{\psi(A\times B)} \leq p^k \leq |G/G'| \leq p^{\psi(A\times B)},$$

so in fact $\psi(A) = l$, $\psi(B) = k - l$, (5) holds and hence (6)–(9′) are also available. In particular, $|A/A'| = p^l$ by (9′) and then the inductive hypothesis gives that A is one of the listed groups. By (2), (7), and (12) with $A_1 = A \cap G$, we have $A \cap G = A$: so $G = A \times B$ by (3). As (9) gives $|B/B'| = p^{k-l}$, the inductive hypothesis applied to B completes this case of the inductive step.

Suppose next that G is transitive. For this case (10) and (11) provide a more generous initial step: so we now assume not just $k > 1$ but

$k > p$ and $kp > 8$. Let H be a maximal subgroup of G containing a point stabilizer: then H is a normal subgroup of index p; it has p orbits, which are permuted transitively by G, each having length k; of course now k is a power of p: set $k = mp$. Let A be a transitive constituent of H (the other transitive constituents being G-conjugates of A), and B the restriction of H to the union of the other orbits: then H is a subdirect product of A and B.

Consider the case $|(A \cap H)/(A \cap H')| \geq p^m$. From the inductive hypothesis we get that $\psi(A) = \psi(A \cap H) = m$; in particular $(A \cap H)' = A \cap H'$ so by (2) we have

$$(2') \qquad [A \cap H, A] \leq (A \cap H)' ;$$

moreover $A \cap H$ is the direct product of its transitive constituents. As $A \cap H$ is normal in the transitive A, these constituents are all conjugate in A: this contradicts (2′) unless $A \cap H$ is transitive. In that case $A \cap H$ is one of the listed groups, so (2′) and (12) with $A_1 = A \cap H$ yields $A \cap H = A$, whence $H = A \times B$ by (3). Now H is the product of the G-conjugates of A which in the abelian G/G' have common image AG'/G', hence $H/G' = AG'/G'$ and so

$$p^{mp} \leq |G/G'| = p|H/G'| = p|A/(A \cap G')| \leq p|A/A'| \leq p^{m+1}$$

which is impossible under our assumption that $mp = k > p$ and $kp > 8$.

In the remaining case, that is, when $|(A \cap H)/(A \cap H')| < p^m$, we have that

$$|H/H'| \geq |H/G'| \geq p^{mp-1}$$

while Figure 1 (read with H in place of G and taking advantage of $\mathbf{O}^p(H) = 1$) yields that

$$\begin{aligned}|H/H'| &= |(A \cap H)H'/H'|\,|H/(A \cap H)H'|\\ &= |(A \cap H)/(A \cap H')|\,|B/(AH' \cap B)|.\end{aligned}$$

It follows that

$$|B/B'| \geq |B/(AH' \cap B)| > p^{mp-1}/p^m, \quad \text{so } |B/B'| \geq p^{mp-m}.$$

As the degree of B is $(mp - m)p$, the inductive hypothesis gives that B is the direct product of its transitive constituents (which we know are G-conjugates of A) and each constituent is one of the groups listed under (i) and (ii). The only option consistent with $mp = k > p$ and $kp > 8$ is $p = 2$, $k = 8$, $A \cong B \cong D_8 \curlyvee D_8$. As $A \cap H$ and $B \cap H$

are disjoint conjugate subgroups of G, we must have $|G'| \geq |B \cap H| = |H|/|A|$; hence

$$2^8 \leq |G/G'| \leq |G|\,|A|/|H| = 2|A| = 2^6.$$

This contradiction completes the inductive step, so (14) is proved.

Proof of the Theorem. We shall use induction, firstly on the degree of G and secondly on the order of G. Accordingly, the inductive hypothesis will consist of two parts: the theorem is true for all groups whose degree is smaller than that of G, and also for all proper subgroups of G. As the theorem is a tautology when G is a p'-group and is valid by (14) whenever G is a p-group, the initial step presents no problem. Indeed we can assume that G is neither a p-group nor a p'-group.

The first sentence of the theorem is an immediate consequence of applying the inductive hypothesis to a Sylow p-subgroup of G. The "if" part of the second sentence is obvious. To deal with the "only if" part, suppose that $|G/G'\mathbf{O}^p(G)| = p^k$: the task is to prove that G has the required structure. Note that, since a Sylow p-subgroup of a subgroup of G cannot move more than kp points, by the inductive hypothesis we have that

(15) a proper subgroup which supplements $G'\mathbf{O}^p(G)$ in G must have the required structure and its Sylow p-subgroup must move precisely kp points.

The case of intransitive G can be handled by adapting the corresponding step from the proof of (14): the relevant preliminaries in §2 had been prepared with this in mind. The only extra point is that now a transitive non-p'-constituent should be chosen as A.

The next case we consider is that of a transitive G whose degree is divisible by p. Then a point stabilizer cannot contain any Sylow p-subgroup of G; equivalently, a Sylow p-subgroup P of G can fix no point: so the degree of G is kp. It follows that all proper supplements of $G'\mathbf{O}^p(G)$ in G are p-groups: for, by (15), they must have the required structure but now can have no affine constituents. Let q be another prime divisor of $|G|$; by the Frattini argument, the normalizer $\mathbf{N}_G(Q)$ of a Sylow q-subgroup Q supplements $G'\mathbf{O}^p(G)$; by the previous sentence, $\mathbf{N}_G(Q)$ cannot be a proper subgroup: so Q is normal in G. By a similar argument, $PQ = G$. As Q is normal, its orbits form a system of imprimitivity; in particular, they have a common length, say q^b. The degree kp being divisible both by q^b and by p, neither P

nor Q is transitive. Let Γ and Γ' be distinct P-orbits and Δ a Q-orbit. Since $PQ = G$, each coset of P meets each coset of Q and so each P-orbit meets each Q-orbit: consequently $\Delta \not\supseteq \Gamma$ and we can choose a δ in $\Gamma' \cap \Delta$. Since P is the direct product of its transitive constituents (by (15)), the point stabilizer P_δ is transitive on Γ. Now we use that Δ is a block of imprimitivity for G: it must be fixed (setwise) by P_δ because $\delta \in \Delta$, and cannot be fixed by P_δ because it meets but does not contain the P_δ-orbit Γ. This contradiction shows that the case under consideration cannot arise.

It remains to consider transitive G of degree prime to p. Our first aim is to show that in this case G is primitive. Take any point stabilizer G_α, any Sylow p-subgroup P of G contained in G_α, and any maximal subgroup M containing G_α. Assume that $G_\alpha < M$: we shall show that this leads to a contradiction. Consider the corresponding system of imprimitivity, and let m denote the common length $|G_\alpha : M|$ of its blocks: note that p does not divide m, so no P-orbit Γ can be a union of blocks. If a block Δ meets two P-orbits Γ, Γ' without containing both of them, we get a contradiction as at the end of the previous paragraph. If a block Δ' meets only one P-orbit Γ, then of course $\Delta' \subset \Gamma$ so Γ must also meet some block Δ which it does not contain; in turn, that Δ must meet another P-orbit Γ' as well, and the previous sentence applies. In the remaining case each block is a union of P-orbits, that is, P fixes each block setwise: P lies in the intersection, say N, of the conjugates of M. Note that $N\mathbf{O}^p(G) = G$. Since N is normal in the transitive G, the transitive constituents of N are all G-conjugate: in particular they are all isomorphic so none of them can be a p'-group, and hence N is their direct product by (15). As $G_\alpha N \leq M < G$, there is more than one transitive constituent; thus if A is any one of them, a Sylow p-subgroup of A cannot move as many as kp elements, and the inductive hypothesis gives that $|A/A'\mathbf{O}^p(A)| < p^k$. On the other hand, N being the product of the conjugates of A implies that $AG'/G' = NG'/G'$ whence $AG'\mathbf{O}^p(G) = NG'\mathbf{O}^p(G) = G$, and then

$$\begin{aligned} p^k &> |A/A'\mathbf{O}^p(A)| \geq |A/(A \cap G'\mathbf{O}^p(G))| \\ &= |G/G'\mathbf{O}^p(G)| = p^k \end{aligned}$$

is the desired contradiction.

This has proved that G is primitive. The next aim is to show that G is 2-transitive. By 18.4 in Wielandt's **[6]**, no transitive constituent of G_α except that on $\{\alpha\}$ can be a p'-group, so by (15) we know that G_α is the direct product of its transitive constituents. Let Γ be a G_α-orbit, other than $\{\alpha\}$, of shortest possible length, say, d. Choose a point γ in Γ and an element h in G such that $\alpha h = \gamma$; let Δ be the G_γ-orbit Γh, and Δ' the G_γ-orbit paired with Δ: that is, Δ' consists of all the γg with $g \in \{g \in G | \gamma \in \Delta g\}$. By 16.3 in [6], the length of Δ' is also d, while $\alpha \in \Delta'$ because $\alpha = \gamma h^{-1}$ and $\gamma \in \Gamma = (\Gamma h)h^{-1} = \Delta h^{-1}$. Since G_α is the direct product of its transitive constituents, $G_{\alpha\gamma}$ acts transitively on each G_α-orbit other than Γ: hence all the $G_{\alpha\gamma}$-orbits of length less than d lie in $\{\alpha\} \cup \Gamma$. On the other hand, $\{\gamma\} \cup \Delta'$ is a union of G_γ-orbits; as this set has $d+1$ elements of which two, α and γ, are fixed by $G_{\alpha\gamma}$, it is a union of $G_{\alpha\gamma}$-orbits each of length less than d. Consequently $\{\gamma\} \cup \Delta' \subseteq \{\alpha\} \cup \Gamma$; as both sets have cardinality $d+1$, they are in fact equal. It follows that this set is fixed (setwise) by G_α and by G_γ, so it is fixed by G and is therefore the whole set, say Ω, on which G acts. In particular, G_α is transitive on $\Omega \setminus \{\alpha\}$.

By (15) it follows that G_α is one of the transitive groups listed, so (13) is applicable, and the proof of the theorem is complete.

Proof of the Corollary. Since the function $x^{1/x}$ is decreasing when $x \geq e$,

$$3^{1/3} > 4^{1/4} = 2^{1/2} > 5^{1/5} > \cdots$$

and so only the first sentence of the corollary needs additional justification. Suppose that is false. Let n be the least integer for which counterexamples of degree n exist, and let G be a degree n counterexample of minimal order. For a prime p dividing $|G|$, let P be a Sylow p-subgroup of G. By the Frattini argument applied with the normal subgroup PG', we have that $\mathrm{N}_G(P)G' = G$ so G/G' is a homomorphic image of $\mathrm{N}_G(P)/\mathrm{N}_G(P)'$: as $|G|$ is minimal, this can only happen if $\mathrm{N}_G(P) = G$. Thus all Sylow subgroups of G are normal: G is nilpotent. By the theorem $G \neq P$, so $G = P \times Q$ with a nontrivial subgroup Q. Of course, $G/G' \cong (P/P') \times (Q/Q')$. Any orbit of a direct product of a p-group P and a p'-group Q may be viewed as the cartesian product $\Gamma \times \Delta$ of a P-orbit Γ and a Q-orbit Δ. If there were a G-orbit $\Gamma \times \Delta$ on which both P and Q acted nontrivially, one could replace it by the disjoint union $\Gamma \cup \Delta$, obtaining a smaller set on which G still acted faithfully, and this would contradict the minimality of n. Thus if a denotes the number of points moved by P and b the number moved by Q, we have

$$a + b = n.$$

By the minimality of n we have $|P/P'| \leq p^{a/p}$ and $|Q/Q'| \leq q^{b/q}$ for some prime divisor q of $|Q/Q'|$: then $|G/G'| \leq p^{a/p}q^{b/q}$. Finally, by the last two displayed lines, $p^{a/p}q^{b/q}$ cannot be larger than both of $p^{n/p}$ and $q^{n/q}$, so G is not a counterexample after all.

References

[1] Muhammed Salihu Audu, *Transitive permutation groups of prime-power order*, D. Phil. thesis, Oxford, 1983.

[2] D. Easdown and C. E. Praeger, *On the minimal faithful degree of a finite group*, University of Western Australia Research Report, 1987.

[3] B. Huppert, *Endliche Gruppen* I, Springer-Verlag, Berlin Heidelberg New York, 1967.

[4] B. Huppert and N. Blackburn, *Finite Groups* III, Springer-Verlag, Berlin Heidelberg New York, 1982.

[5] L. G. Kovács and M. F. Newman, *Generating transitive permutation groups*, Quarterly J. Math. Oxford, (2) **39** (1988), to appear.

[6] Helmut Wielandt, *Finite Permutation Groups*, Academic Press, New York and London, 1964.

Received November 13, 1987.

Australian National University
Canberra, ACT 2601

and

University of Western Australia
Nedlands, WA 6009