Bull. Austral. Math. Soc. 20B05, 20B35
Vol. 62 (2000) [311–317]

ON MINIMAL FAITHFUL PERMUTATION REPRESENTATIONS OF FINITE GROUPS

L. G. Kovács and Cheryl E. Praeger

The minimal faithful permutation degree $\mu(G)$ of a finite group G is the least positive integer n such that G is isomorphic to a subgroup of the symmetric group S_n. Let N be a normal subgroup of a finite group G. We prove that $\mu(G/N) \leqslant \mu(G)$ if G/N has no nontrivial Abelian normal subgroup. There is an as yet unproved conjecture that the same conclusion holds if G/N is Abelian. We investigate the structure of a (hypothetical) minimal counterexample to this conjecture.

1.

According to a classical theorem of Cayley, each group can be faithfully represented as a group of permutations of some set. In both theoretical and computational investigations of finite groups, it is often useful for the permuted set to be chosen as small as possible. Thus the *minimal faithful permutation degree* $\mu(G)$ of a finite group G is defined as the least positive integer n such that G is isomorphic to a subgroup of the symmetric group S_n, and a faithful permutation representation of G on a set of cardinality $\mu(G)$ is called a *minimal faithful permutation representation* of G. In early results that will be relevant here, Johnson [3] determined $\mu(G)$ for Abelian G and studied the number of orbits in minimal faithful permutation representations of nilpotent G, while Wright [7] proved that $\mu(G) = \mu(H) + \mu(K)$ whenever G is nilpotent with a nontrivial direct factorisation $G = H \times K$.

For computations with finite permutation groups, one often wishes to study quotients G/N of a permutation group G on a set Ω, and for this purpose an efficient faithful representation of G/N as a group of permutations on a set of size comparable to the size of Ω would be useful. With this in mind, it seems natural to seek conditions which guarantee that the minimal faithful permutation degree $\mu(G/N)$ is at most $\mu(G)$.

Some condition is certainly necessary, because in certain cases $\mu(G/N)$ is very much greater than $\mu(G)$. For example, it was pointed out by P. M. Neumann in the introduction to [5] that the direct product of m copies of the dihedral group of order 8

Received 21st February, 2000

https://doi.org/10.1017/S0004972700018797 Published online by Cambridge University Press

has a natural faithful permutation representation of degree $4m$ but it has an extraspecial quotient which has no faithful permutation representation of degree less than 2^{m+1}. (As L. Pyber remarked to us, the direct product may be viewed as the base group of the wreath product of the dihedral group with a cyclic group of order m. This wreath product has a faithful *transitive* representation of degree $4m$, but it also has a quotient which contains the extraspecial group which has no faithful representation of degree less than 2^{m+1}. This shows that assuming transitivity would not help.)

This paper addresses the problem of finding useful classes of groups G, or quotients G/N, for which we can guarantee that $\mu(G/N) \leqslant \mu(G)$. First we present a simple result which provides sufficient conditions on G/N for this to be true. It is an extension of [**1**, Proposition 1.3] which shows that, if N is an Abelian normal subgroup of G, then there exists an Abelian normal subgroup M, containing N, such that $\mu(G/M) \leqslant \mu(G)$. One consequence of this result is that, for all finite groups G, $\mu(G/\operatorname{sol} G) \leqslant \mu(G)$, where $\operatorname{sol} G$ is the largest soluble normal subgroup of G. We prove here a second consequence of [**1**, Proposition 1.3].

THEOREM 1. *If G/N has no nontrivial Abelian normal subgroup, then $\mu(G/N) \leqslant \mu(G)$.*

PROOF: Suppose that $\mu(G/N) > \mu(G)$ and that G/N has no nontrivial Abelian normal subgroup. Choose such a pair G, N with least possible $\mu(G)$, and among these choose one with least possible $|G|$. Take G as a subgroup of $\operatorname{Sym}\Omega$ with $|\Omega| = \mu(G)$. Clearly $N \neq 1$. If N is not contained in the Frattini subgroup $\Phi(G)$, then there is a maximal subgroup H of G not containing N, so $G = HN$. But then H, $H \cap N$ is not a counterexample to the theorem, and $H/(H \cap N) \cong HN/N = G/N$, so $\mu(G/N) = \mu(H/(H \cap N)) \leqslant \mu(H) \leqslant \mu(G)$, which is a contradiction. Hence $N \leqslant \Phi(G)$. Thus N is nilpotent and so, since G/N has no nontrivial Abelian normal subgroup, N is the soluble radical $\operatorname{sol} G$ of G. Applying Proposition 1.3 of [**1**] with K the centre $Z(N)$, we see that G has an Abelian normal subgroup L containing K such that $\mu(G/L) < \mu(G)$. Since L is Abelian, $L \leqslant \operatorname{sol} G = N$ and $\operatorname{sol}(G/L) = N/L$, so G/L, N/L is a counterexample with $\mu(G/L) < \mu(G)$, contradicting the minimality of $\mu(G)$. ∎

It follows from this result that, if the group G has no Abelian composition factors, then $\mu(G/N) \leqslant \mu(G)$ for every normal subgroup N. This consequence of Theorem 1 was used by Jackie Walton in [**6**] to prove that, for all finite groups G and all normal subgroups N of G, $\mu(G/N)$ is bounded above by an exponential function of $\mu(G)$. More precisely, she proved that $\mu(G/N) \leqslant \mu(G)c^{\mu(G)-1}$ where the constant c is approximately 5.34.

https://doi.org/10.1017/S0004972700018797 Published online by Cambridge University Press

2.

In the rest of the paper we examine finite groups G with Abelian quotients G/N. It was remarked upon in [1] that, if $\mu(G/N) > \mu(G)$, then G is not Abelian and G/N is not cyclic. For this case, we proved in [4] that G/N is not elementary Abelian, and conjectured that G/N cannot even be Abelian. This conjecture is still open, and our objective here is to draw more attention to it by gathering information about a (hypothetical) minimal counterexample.

Almost all the results which admit concise statements follow readily from the work of Johnson [3] and Wright [7] that we mentioned above.

THEOREM 2. *Suppose that there exists a finite group G with an Abelian quotient G/N such that $\mu(G/N) > \mu(G)$. Among such groups, let G be chosen with $\mu(G)$ as small as possible, and from all examples with this minimal faithful permutation degree, let G have minimal order. Then the following all hold.*

(a) *G is a directly indecomposable p-group, for some prime p; in particular, the socle $\operatorname{soc} G$ lies in the Frattini subgroup $\Phi(G)$.*

(b) *N is the commutator subgroup of G, and $\mu(G/N) = \mu(G) + p$.*

(c) *Consider a minimal faithful permutation representation of G, with the maximum number of orbits among all such representations. Then the number of orbits is the rank of the centre of G, while the group of permutations induced by G on any one orbit is non-Abelian and has cyclic centre.*

PROOF: We use standard notation: if a permutation group G on a certain set leaves invariant a subset Δ, then the group of permutations of Δ induced by G is written as G^{Δ}. The *transitive constituents* of G are the G^{Δ} with Δ an orbit of G.

As remarked at the end of Section 1 of [1], the claim that G is a p-group follows from the proofs of Lemma 1.1(a) and Proposition 1.6 in that paper. Suppose that N is strictly larger than the commutator subgroup G'. Each quotient of a finite Abelian group is isomorphic to a subgroup, so in particular the proper quotient G/N of G/G' is isomorphic to some proper subgroup of G/G'; say, to H/G'. Then H, G' is a counterexample with $\mu(H) \leqslant \mu(G)$ and $|H| < |G|$, contrary to the minimal choice of G, N. This proves that we must have $N = G'$. If G were a direct product, say, $G = H \times K$ with nontrivial H, K, we would also have $G/G' = H/H' \times K/K'$, and (by the minimal choice of G) neither H nor K could be a counterexample. It was proved by Wright [7] that $\mu(G) = \mu(H) + \mu(K)$ whenever G is nilpotent, and this would now show that G is not a counterexample either. This proves that G is directly indecomposable. If some minimal normal subgroup of G were to avoid the Frattini subgroup, it would be a direct factor, so the socle must lie in the Frattini subgroup.

https://doi.org/10.1017/S0004972700018797 Published online by Cambridge University Press

Johnson [3] proved that, in a minimal faithful representation of an arbitrary p-group, the number of orbits is at most the rank of the centre, and that this bound is achieved by at least one minimal faithful representation. The number of orbits in the representation of G considered in part (c) is therefore the rank of the centre. Next, Johnson's result applied to a transitive constituent G^{Δ} yields that, if the centre of G^{Δ} were not cyclic, then G^{Δ} would have an intransitive minimal representation. However, then G would have a minimal faithful representation with even more orbits, so this cannot be the case.

To complete the proof of (c), suppose that a transitive constituent $H = G^{\Delta}$ is Abelian, and set $K = G^{\Omega\setminus\Delta}$. Then $\mu(G) = \mu(H) + \mu(K)$, while $G \leqslant H \times K$ with $G' = 1 \times K'$ so G/G' is isomorphic to a subgroup of $H \times K/K'$. By the minimal choice of G, K is not a counterexample, so

$$\mu(G) < \mu(G/G') \leqslant \mu(H) + \mu(K/K') \leqslant \mu(H) + \mu(K) = \mu(G),$$

a contradiction.

The one remaining claim, namely $\mu(G/G') = \mu(G) + p$, will be part (c) of Lemma 3. Before we can state that, we need some technicalities about Abelian groups.

LEMMA 1. *If A is a finite Abelian p-group and B is an elementary Abelian subgroup of A, then A has a direct decomposition $A = \prod_{i\in I} C_i$ with the C_i cyclic such that $B = \prod_{i\in I}(B \cap C_i)$.*

PROOF: Let C_1 be a cyclic factor of maximal order in A. Then $A = C_1 \times A_1$ for any subgroup A_1 of A which is maximal in A with respect to avoiding C_1 (see [2, pp.74–75, consequence b) of Lemma 22.1]). Choose a complement for $B \cap C_1$ in B and choose A_1 to contain that. The result follows by induction on the number of direct factors in an unrefinable direct decomposition of A. ∎

LEMMA 2. *Let A be a finite Abelian p-group, B an elementary Abelian subgroup of A, and $A = \prod_{i\in I} C_i$ a direct decomposition with (nontrivial) cyclic C_i such that $B = \prod_{i\in I}(B \cap C_i)$. Further, let $I = X \cup Y \cup Z$ where*

$$\begin{aligned} X &:= \{\, i \in I \mid C_i \cap B = 1 \,\}, \\ Y &:= \{\, i \in I \mid C_i > C_i \cap B > 1 \,\}, \text{ and} \\ Z &:= \{\, i \in I \mid C_i \leqslant B \,\}. \end{aligned}$$

If $\mu(A/B) < \mu(A)/p$, then $1 + (p-1)|X| \leqslant |Z|$. In particular, $|Z| \geq 1$ (that is, B contains at least one of the direct factors C_i of order p), and if $|Z| < p$ then $X = \emptyset$ (that is, $B = \operatorname{soc} A$).

https://doi.org/10.1017/S0004972700018797 Published online by Cambridge University Press

PROOF: Now $\mu(A) = \sum_{i\in I} |C_i|$, and $\mu(A/B) = \sum_{i\in X} |C_i| + \sum_{i\in Y} |C_i|/p$. Since $\mu(A)/p$ is an integer, we have $1+\mu(A/B) \leqslant \mu(A)/p$, whence $1+(p-1)\sum_{i\in X} |C_i|/p \leqslant \sum_{i\in Z} |C_i|/p$. As B is elementary Abelian, it follows that $\sum_{i\in Z} |C_i|/p = |Z|$, and we have proved (a little more than) what we claimed. □

Given a permutation representation $G \to \operatorname{Sym}\Omega$, we denote by $\Omega/\operatorname{soc} G$ the set of $(\operatorname{soc} G)$-orbits in Ω, and by $G_{(\Omega/\operatorname{soc} G)}$ the kernel of the action of G on this set: that is, the normal subgroup of G consisting of the elements that leave each $(\operatorname{soc} G)$-orbit setwise invariant.

LEMMA 3. *Let G be as in Theorem* 2, *let $G \to \operatorname{Sym}\Omega$ be a minimal faithful representation chosen as in part* (c) *of that theorem, and set $L = G_{(\Omega/\operatorname{soc} G)}$.*

(a) *The subgroup L is elementary Abelian, it is not contained in $\Phi(G)$, and*

$$\mu(G/LG') < \mu(G/G')/p.$$

(b) *In any decomposition of G/G' as a direct product of cyclic groups which matches the elementary Abelian subgroup LG'/G' in the sense of Lemma* 1, *at least one direct factor of order p must lie in LG'/G'. If K/G' is such a direct factor and H is any maximal subgroup of G not containing K, then $H' = G'$ and $\mu(H) = \mu(G) = \mu(H/G')$.*

(c) $\mu(G/G') = \mu(G) + p$.

PROOF: It follows from Theorem 2(c) that $\operatorname{soc} G$ acts on each G-orbit in Ω as a semiregular group of order p; in particular $\operatorname{soc} G$ is fixed-point-free on Ω, and $|\Omega/\operatorname{soc} G| = |\Omega|/p$. By [**1**, Proposition 1.3] L is elementary Abelian and contains $\operatorname{soc} G$, while as G/L is faithful on $\Omega/\operatorname{soc} G$, we have $\mu(G/L) \leqslant \mu(G)/p$. The minimality of $\mu(G)$ now implies that $\mu(G/LG') \leqslant \mu(G/L) \leqslant \mu(G)/p < \mu(G/G')/p$. The first claim in (b) then follows from Lemma 2 applied with $A = G/G'$, $B = LG'/G'$. As LG'/G' contains a nontrivial direct factor of G/G', we know that $LG'/G' \not\leqslant \Phi(G/G')$, and so $L \not\leqslant \Phi(G)$.

Given a nontrivial cyclic direct factor K/G' of G/G' contained in LG'/G' (and hence having order p), let H be any maximal subgroup of G not containing K. Then $G/G' = H/G' \times K/G'$, and H/G' is isomorphic to a subgroup of H/H', so

$$\begin{aligned} \mu(G/G') &= \mu(H/G') + p \\ &\leqslant \mu(H/H') + p \\ &\leqslant \mu(H) + p \quad \text{(since } H \text{ is not a counterexample)} \\ &\leqslant \mu(G) + p \\ &\leqslant \mu(G/G') \end{aligned}$$

https://doi.org/10.1017/S0004972700018797 Published online by Cambridge University Press

(since $\mu(G) < \mu(G/G')$ and the numbers on the two sides of this inequality are multiples of p). Therefore $\mu(G/G') = \mu(G) + p$, and $\mu(H/G') = \mu(H/H') = \mu(H) = \mu(G)$. It follows also that $H' = G'$. This completes the proof of the lemma, as well as the proof of Theorem 2. $\square$

Remark 1. Given a direct decomposition $G/G' = \prod_{i\in I} C_i$ matching LG'/G' in the sense of Lemma 2, write each C_i as K_i/G' and, for $j \in Z$, set $H_j/G' = \prod_{i\neq j} C_i$: then each H_j is able to play the role of H in Lemma 3(b). Moreover, their intersection, $T = \bigcap_{j\in Z} H_j$, is transitive on each G-orbit Δ in Ω. Indeed, $T/G' = \prod_{i\in I\setminus Z} C_i$ and $G/G' = T/G' \times \prod_{j\in Z} C_j$, so $G = TL$. This implies that T is transitive on Δ/L; but each L-orbit is a $(\operatorname{soc} G)$-orbit by the definition of L, and is contained in a T-orbit since $\operatorname{soc} G \leqslant \Phi(G) \leqslant T$.

One may also wish to note that $L \cap T \leqslant \Phi(G)$, because

$$(L\cap T)G'/G' \leqslant (LG'/G') \cap (T/G') = \prod_{i\in Y} \operatorname{soc} C_i \leqslant \prod_{i\in Y} C_i^p \leqslant \Phi(G/G').$$

Remark 2. A slightly different exploration yields a little more information about the action. Let Δ be a G-orbit in Ω and p^d the cardinality of Δ; we know from Theorem 2(c) that $d \geq 2$. Set

$$D = G_{(\Omega\setminus\Delta)} \cap G_{(\Delta/\operatorname{soc} G)}.$$

Of course, then $(\operatorname{soc} G) \cap D = (\operatorname{soc} G)_{(\Omega\setminus\Delta)}$ has order p, and D is elementary Abelian. Since G/D is faithful on $(\Omega \setminus \Delta) \cup (\Delta/\operatorname{soc} G)$, $\mu(G/D) \leqslant \mu(G) - p^{d-1}(p-1)$. By the minimality of G, G/D is not a counterexample, and so

$$\mu(G/DG') \leqslant \mu(G/D) \leqslant \mu(G) - p^{d-1}(p-1) = \mu(G/G') - p - p^{d-1}(p-1) < \mu(G/G').$$

In particular, $D \nleqslant G'$.

References

[1] D. Easdown and C.E. Praeger, 'On minimal faithful permutation representations of finite groups', *Bull. Austral. Math. Soc.* **38** (1988), 207-220.

[2] L. Fuchs, *Abelian groups* (Akadémiai Kiadó, Budapest, 1958).

[3] D.L. Johnson, 'Minimal permutation representations of finite groups', *Amer. J. Math.* **93** (1971), 857–866.

[4] L.G. Kovács and C.E. Praeger, 'Finite permutation groups with large abelian quotients', *Pacific J. Math.* **136** (1989), 283–292.

[5] P.M. Neumann, 'Some algorithms for computing with finite permutation groups', in *Proceedings of Groups — St Andrews 1985*, (E.F. Robertson and C.M. Campbell, Editors), London Math. Soc. Lecture Notes **121** (Cambridge University Press, 1987), **pp.** 59–92.

[6] J. Walton, *Representing the quotient groups of a finite permutation group*, (PhD thesis) (University of Warwick, 1999).

[7] D. Wright, 'Degrees of minimal embeddings for some direct products', *Amer. J. Math.* **97** (1975), 897–903.

Australian National University
Canberra ACT 0200
Australia
e-mail: kovacs@maths.anu.edu.au

University of Western Australia
Perth WA 6907
Australia
e-mail: praeger@maths.uwa.edu.au

https://doi.org/10.1017/S0004972700018797 Published online by Cambridge University Press