The Australian National University

Mathematics Research Report 022–93 SMS–117–93

Notes on minimal faithful permutation representations of finite groups

L. G. Kovács and Cheryl E. Praeger

School of Mathematical Sciences

MRR–022–93 SMS–117–93

Notes on minimal faithful permutation representations of finite groups

L. G. Kovács and Cheryl E. Praeger

School of Mathematical Sciences, Australian National University
and
Department of Mathematics, University of Western Australia

Abstract. For a finite group G, the *minimal faithful permutation degree* $\mu(G)$ of G is the least positive integer n such that G is isomorphic to a subgroup of the symmetric group S_n. Examples show that $\mu(G/N) \leq \mu(G)$ does not always hold. It is proved here that if G/N has no nontrivial abelian normal subgroup then $\mu(G/N) \leq \mu(G)$.

Easdown and the second author have conjectured that $\mu(G/N) \leq \mu(G)$ must always hold if G/N is abelian. It certainly holds when G/N is cyclic, and was previously shown by the authors to hold whenever G/N is elementary abelian. Most of this report is devoted to an exploration of the properties of a (hypothetical) minimal counterexample to the conjecture. With reference to a suitable interpretation of 'minimal', it is shown that each such counterexample G is of prime-power order and has no direct factor of prime order, while N is precisely the commutator subgroup of G. In any faithful permutation representation of G which has degree $\mu(G)$ and as many orbits as possible, the number of orbits is the same as the rank of the centre of G. In such a representation, the transitive groups induced by G on the various orbits are all nonabelian with cyclic centre. Several other properties of minimal counterexamples are also established, but the question of their existence remains beyond reach.

1991 *Mathematics Subject Classification*: primary 20B05; secondary 20D15.

Postal addresses:
Mathematics IAS, Australian National University, Canberra ACT 0200
(*E-mail*: kovacs@maths.anu.edu.au)
Department of Mathematics, University of Western Australia, Nedlands WA 6009
(*E-mail*: praeger@maths.uwa.edu.au)

Notes on minimal faithful permutation representations of finite groups

L. G. Kovács and Cheryl E. Praeger

1. For a finite group G, let $\mu(G)$ denote the least positive integer n such that G has a faithful permutation representation of degree n. The paper [EP] investigated finite groups G for which $\mu(G/N) > \mu(G)$ for some normal subgroup N.

We begin these notes by proving the following.

Theorem 1. *If G/N has no nontrivial abelian normal subgroup, then $\mu(G/N) \leq \mu(G)$.*

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 $\mathrm{Sym}(\Omega)$ 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 $\mu(G/N) = \mu(H/(H \cap N)) \leq \mu(H) \leq \mu(G)$, which is a contradiction. Hence $N \leq \Phi(G)$. Thus N is nilpotent and so, since G/N has no nontrivial abelian normal subgroup, N is the soluble radical $\mathrm{solrad}(G)$ of G. Applying Proposition 1.3 of [EP] to $K = Z(N)$, we see that G has an abelian normal subgroup L containing K such that $\mu(G/L) < \mu(G)$. Since L is abelian, $L \leq \mathrm{solrad}(G) = N$ and $\mathrm{solrad}(G/L) = N/L$, so G/L, N/L is a counterexample with $\mu(G/L) < \mu(G)$, contradicting the minimality of $\mu(G)$. □

2. Easdown and the second author conjectured in [EP] that $\mu(G/N) \leq \mu(G)$ must always hold if G/N is abelian. As was noted at the top of p. 208 in [EP], it certainly holds when G/N is cyclic (for if $G/N = \langle Ng \rangle$ then $\mu(G/N) \leq \mu(\langle Ng \rangle) \leq \mu(\langle g \rangle) \leq \mu(G)$). We showed in [KP] that it holds whenever G/N is elementary abelian.

The last section of this report will be devoted to investigating in detail the structure of a hypothetical minimal counterexample to this conjecture. To prepare for that, in the present section we gather some general facts.

Lemma 1. *If A and B are finite abelian groups, then A has a subgroup isomorphic to B if and only if A has a quotient isomorphic to B.*

Proof. We sketch the proof for p-groups. Let $A = \prod_{i=1}^{n} C(p^{a(i)})$ and $B = \prod_{i=1}^{n} C(p^{b(i)})$ be such that $a(1) \geq a(2) \geq \cdots \geq a(n) \geq 0$ and $b(1) \geq b(2) \geq \cdots \geq b(n) \geq 0$. Then A

These incomplete notes date from 1989. They are issued here because, although we have made no progress along these lines since then, others seem to continue to find them useful.

has a subgroup isomorphic to B if and only if $a(i) \geq b(i)$ for all i if and only if A has a quotient isomorphic to B. □

LEMMA 2. *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 [F], 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 3. *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*

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

If $\mu(A/B) < \mu(A)/p$, then

$$p^2 + (p-1)\sum_{i \in X} |C_i| \leq p|Z|.$$

In particular, $|Z| \geq p$ (that is, B contains at least p of the direct factors C_i of order p), and if $|Z| = p$ then $X = \varnothing$.

PROOF. Now $\mu(A) = \sum_{i \in I} |C_i|$, and $\mu(A/B) = \sum_{i \in X} |C_i| + \left(\sum_{i \in Y} |C_i|\right)/p$. Also, since $\mu(A/B)$ and $\mu(A)$ are both multiples of p, we have $\mu(A/B) + p \leq \mu(A)/p$, and it follows that $\sum_{i \in X} |C_i| + p \leq \left(\sum_{i \in X \cup Z} |C_i|\right)/p$, whence $p^2 + (p-1)\sum_{i \in X} |C_i| \leq \sum_{i \in Z} |C_i|$. In particular, since B is elementary abelian, $|Z|p = \sum_{i \in Z} |C_i| \geq p^2$, B contains $|Z| \geq p$ direct factors C_i of order p, and if $|Z| = p$ then $|X| = 0$. □

Given $G \to \mathrm{Sym}(\Omega)$, we denote by Ω/G the set of G-orbits in Ω.

LEMMA 4. *If G is a subgroup of $\mathrm{Sym}(\Omega)$ such that the socle $\operatorname{soc} G$ of G is the direct product of s minimal normal subgroups of G, then from the G-orbits in Ω one can select at most s so that G is faithful on the union of these orbits. In particular, if $|\Omega| = \mu(G)$ then $|\Omega/G| \leq s$.*

PROOF. Let $\Delta_1, \dots, \Delta_n$ be the G-orbits in Ω, and consider the chain of pointwise stabilizers

$$\operatorname{soc} G \geq (\operatorname{soc} G)_{(\Delta_1)} \geq (\operatorname{soc} G)_{(\Delta_1 \cup \Delta_2)} \geq (\operatorname{soc} G)_{(\Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_n)} = \{1\}.$$

This cannot be strictly descending at more than s steps, so the orbits may be re-numbered so as to ensure that $(\operatorname{soc} G)_{(\Delta_1 \cup \cdots \cup \Delta_r)} = \{1\}$ with some $r \leq s$. Then G is faithful on $\bigcup_{i=1}^{r} \Delta_i$. □

LEMMA 5. *Let P be a finite p-subgroup of* $\operatorname{Sym}(\Omega)$ *with $|\Omega| = \mu(P)$. If $p = 2$, suppose also that no other embedding of P in* $\operatorname{Sym}(\Omega)$ *results in a larger number of P-orbits.*

(a) *Each transitive constituent of P has cyclic centre.*

(b) $|\Omega/P| = \operatorname{rk}(Z(P))$.

(c) $\mu(P \times C(p)) = \mu(P) + p$.

PROOF. (a) If possible, let Δ be a P-orbit and $Z(P^\Delta) \geq A \times B$ with $|A| = |B| = p$. Since the central subgroup $A \times B$ must act semiregularly on Δ, it follows that P^Δ acts faithfully on $(\Delta/A) \cup (\Delta/B)$. Replacing the action of P^Δ on Δ by its action on $(\Delta/A) \cup (\Delta/B)$ yields a faithful representation of P^Δ of degree $|(\Delta/A) \cup (\Delta/B)| = 2|\Delta|/p$. In view of $|\Omega| = \mu(P)$ this cannot happen unless $p = 2$, and then it violates our additional assumption on the maximality of $|\Omega/P|$. This contradiction proves (a).

(b) Since $|\Omega| = \mu(P)$, for each P-orbit Δ, the pointwise stabilizer $P_{(\Omega \setminus \Delta)}$ of $\Omega \setminus \Delta$ is nontrivial, and hence also $Z(P)_{(\Omega \setminus \Delta)} \neq \{1\}$. The subgroup of $Z(P)$ generated by the $Z(P)_{(\Omega \setminus \Delta)}$ is the direct product of these nontrivial groups, so $\operatorname{rk} Z(P) \geq |\Omega/P|$. The converse inequality is a direct consequence of Lemma 4.

(c) Since $\mu(P \times C(p)) \leq \mu(P) + \mu(C(p)) = \mu(P) + p$, and since the minimal degree of each p-group is a multiple of p, the result is true unless $\mu(P \times C(p)) = \mu(P)$. In that case there is, by part (b), a subgroup $Q \times R$ of $\operatorname{Sym}(\Omega)$ with $Q \cong P$, $|R| = p$, and $|\Omega/(Q \times R)| = \operatorname{rk} Z(Q \times R) = 1 + \operatorname{rk} Z(Q)$, but then

should be rk Z(Q)

$$1 + \boxed{\cancel{\operatorname{rk}(Q)}} = |\Omega/(Q \times R)| \leq |\Omega/Q| \leq \operatorname{rk} Z(Q),$$

which is a contradiction. □

3. We are now ready to begin our (inconclusive) examination of a minimal counterexample to the conjecture stated at the beginning of the previous section. Suppose that there exist counterexamples: finite groups G with abelian quotients G/N such that $\mu(G/N) > \mu(G)$.

Among such counterexamples, consider those *with* $\mu(G)$ *minimal*, and among these, choose one *with* $|G|$ *minimal*. Then take this G in a representation of degree $\mu(G)$ *with as many orbits as possible*: say, this representation is $G \to \mathrm{Sym}(\Omega)$. *Keep this choice fixed throughout this section.*

LEMMA 6. *The group G is a p-group for some prime p, and N is the commutator subgroup G' of G. The number of orbits of G in Ω is the rank of the centre of G, and the permutation group induced by G on any one orbit has cyclic centre.*

PROOF. As remarked at the end of Section 1 of [EP], the first statement follows from the proofs of Lemma 1.1(a) and Proposition 1.6 in that paper. Suppose that $N > G'$. By Lemma 1, 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 $\mu(H) \leq \mu(G)$ and $|H| < |G|$, contrary to the minimal choice of G, N. This proves that we must have $N = G'$. The third and fourth statement come directly from Lemma 5. □

LEMMA 7. (a) *There is an elementary abelian normal subgroup L of G which contains* $\mathrm{soc}\, G = \Omega_1(Z(G))$ *and satisfies*

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

(b) *In a decomposition of G/G' as direct product of cyclic groups which matches the elementary abelian subgroup LG'/G' in the sense of Lemma 2, let t denote the number of direct factors K_i/G' (of order p) which lie in LG'/G'. Then $t \geq p$, $LG'/G' \geq (K_1/G') \times \cdots \times (K_t/G')$, and $K_i \not\leq \Phi(G)$ for $i = 1, \ldots, t$ (so $L \not\leq \Phi(G)$).*

(c) $\mu(G/G') = \mu(G) + p$ *and, for $i = 1, \ldots, t$, there is a maximal subgroup H_i of G such that $G = H_i K_i$, $\mu(H_i) = \mu(G) = \mu(H_i/G')$, and $H_i' = G'$.*

should be | \Omega | = \mu(G)

PROOF. It follows from $\boxed{\Omega = \mu(G)}$ and Lemma 5(a) that $\mathrm{soc}\, G = \Omega_1(Z(G))$ acts on each G-orbit in Ω as a semiregular group of order p; in particular $\mathrm{soc}\, G$ is fixed-point-free on Ω, and $|\Omega/\mathrm{soc}\, G| = |\Omega|/p$. By Proposition 1.3 of [EP], the normal subgroup $L := G_{(\Omega/\mathrm{soc}\, G)}$ is elementary abelian and contains $\mathrm{soc}\, G$, while as G/L is faithful on $\Omega/\mathrm{soc}\, G$, we have $\mu(G/L) \leq \mu(G)/p$. The minimality of $\mu(G)$ implies that $\mu(G/LG') \leq \mu(G/L) \leq \mu(G)/p < \mu(G/G')/p$. The claim $t \geq p$ now follows from Lemma 3. As K_i/G' is a direct factor of G/G', we know that $K_i \not\leq \Phi(G)$, and so even $t \geq 1$ would imply that $L \not\leq \Phi(G)$.

For $i = 1, \ldots, t$, let H_i be a maximal subgroup of G not containing K_i. Then

$G/G' = (H_i/G') \times (K_i/G')$, so

$$\begin{aligned}\mu(G/G') &= \mu(H_i/G') + p \\ &\leq \mu(H_i/H_i') + p \quad \text{(by Lemma 1)} \\ &\leq \mu(H_i) + p \quad \text{(since } H_i \text{ is not a counterexample)} \\ &\leq \mu(G) + p \\ &\leq \mu(G/G')\end{aligned}$$

(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 $\mu(H_i/G') = \mu(H_i/H_i') = \mu(H_i) = \mu(G)$. It follows that $H_i' = G'$. □

LEMMA 8. (a) *G has no direct factor of order p; that is, $\operatorname{soc} G \leq \Phi(G)$.*

(b) *Let $H = H_1 \cap \ldots \cap H_t$, where the H_i are as in Lemma 7(c). Then H is transitive on each G-orbit in Ω.*

(c) *The H_i can be chosen so that $H \cap L \leq \Phi(G)$.*

PROOF. If $G = P \times C(p)$ then, by Lemma 5(c), $\mu(G) = \mu(P) + p$. However, then we have also that $G/G' \cong (P/P') \times C(p)$, so that

$$\begin{aligned}\mu(G/G') &= \mu(P/P') + p \\ &\leq \mu(P) + p \quad \text{(since } P \text{ is not a counterexample to the conjecture)} \\ &= \mu(G),\end{aligned}$$

which is a contradiction. Hence G has no direct factor of order p, and this is equivalent to $\operatorname{soc} G \leq \Phi(G)$.

Since each H_i and K_i contain G', we clearly have $G = HK_1 \ldots K_t$, and since each K_i lies in L, also $G = HL$. Hence H is transitive on Ω/L. However, each L-orbit is a $(\operatorname{soc} G)$-orbit by the definition of L, and is contained in an H-orbit since $\operatorname{soc} G \leq \Phi(G) \leq H$. Hence H is transitive on each G-orbit in Ω.

If we choose a direct decomposition $G/G' = \prod_{i \in I} C_i$ matching LG'/G', then each K_j/G' is one of the direct factors C_i of order p: say, $K_j/G' = C_{k_j}$. We can then choose each H_j so that $H_j/G' = \prod_{i \neq k_j} C_i$, and then $H/G' = \prod_{i \notin \{k_1, \ldots, k_t\}} C_i$. Since $\Phi(G)$ is the subgroup containing G' such that $\Phi(G)/G' = \prod_{i \in I} C_i^p$, clearly $\Phi(G)/G' \leq \prod_{|C_i| > p} C_i$, and so it follows that $H \cap L \leq \Phi(G)$. □

We can make a slightly different exploration of the representation and obtain more information about the action. Let $\Delta_1, \ldots, \Delta_r$ be the G-orbits in Ω, where $|\Delta_i| = p^{a_i}$

with $1 \le a_1 \le \ldots \le a_r$. For $i = 1, \ldots, r$, set $L_i = G_{(\Omega\setminus\Delta_i)} \cap G_{(\Delta_i/\mathrm{soc}\,G)}$. Then we may assume that $(\mathrm{soc}\,G) \cap L_i = (\mathrm{soc}\,G)_{(\Omega\setminus\Delta_i)} \cong C(p)$, and L_i is elementary abelian.

LEMMA 9. (a) $L_i \not\le G'$.

(b) G^{Δ_i} *is not abelian and in particular* $a_i \ge a_1 \ge 2$.

(c) $(G')^{\Delta_i} \ne \{1\}$.

(d) $\mu(G/L_iG') \le \mu(G/L_i) \le \mu(G) - p^{a_i-1}(p-1) = \mu(G/G') - p - p^{a_i-1}(p-1)$.

PROOF. Since G/L_i is faithful on $(\Omega\setminus\Delta_i) \cup (\Delta_i/\mathrm{soc}\,G)$, $\mu(G/L_i) \le \mu(G) - p^{a_i-1}(p-1)$. By the minimality of G, G/L_i is not a counterexample, and so

$$\mu(G/L_iG') \le \mu(G/L_i) \le \mu(G) - p^{a_i-1}(p-1) = \mu(G/G') - p - p^{a_i-1}(p-1) < \mu(G/G').$$

Hence $L_i \not\le G'$, proving (a) and (d).

Since L_iG'/G' is elementary abelian, by Lemma 2.there is a direct decomposition $G/G' = \prod_{i\in I} C_i$ with each C_i cyclic, such that $L_iG'/G' = \prod_{j\in J} \mathrm{soc}\,C_j$ for some $J \subseteq I$.

Suppose that G^{Δ_i} is abelian. Then, since $Z(G^{\Delta_i})$ is cyclic, G^{Δ_i} is cyclic. Then G^{Δ_i} is regular and hence $|L_i| = p$, that is, $L_i \le \mathrm{soc}\,G \le \Phi(G)$. So we have $L_iG'/G' = \mathrm{soc}\,C_{k_i}$ for some $k_i \in I$, and as $L_iG' \subseteq \Phi(G)$, $|C_{k_i}| \ge p^2$. Now

$$\mu(G/L_iG') = \sum_{j\ne k_i} |C_j| + |C_{k_i}|/p = \mu(G/G') - |C_{k_i}|(p-1)/p.$$

From part (d) we find that $|C_{k_i}| \ge p^{a_i} + p^2/(p-1) > p^{a_i}$, that is, $|C_{k_i}| \ge p^{a_i+1}$. Let $C_{k_i} = \langle gG' \rangle$. Then as $|\Delta_i| = p^{a_i}$, $g^{p^{a_i}} \in G_{(\Delta_i)}$. Further, since $G/G_{(\Delta_i)} = G^{\Delta_i}$ is cyclic, $G_{(\Delta_i)} \le G'$, and hence $\langle g^{p^{a_i}}, G' \rangle \le G_{(\Delta_i)}$. However, $L_iG'/G' = \mathrm{soc}\,C_{k_i} = \langle g^{p^{a_i}}G' \rangle$, so $L_i \le \langle g^{p^{a_i}}, G' \rangle \le G_{(\Delta_i)}$, which is a contradiction. Hence G^{Δ_i} is nonabelian. In particular, $a_i \ge a_1 \ge 2$, and $(G')^{\Delta_i} \ne \{1\}$. □

These lemmas only begin to build a picture: we cannot say whether they have got us any closer to settling the conjecture.

REFERENCES

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

[KP] L. G. Kovács and Cheryl E. Praeger, Finite permutation groups with large abelian quotients, *Pacific J. Math.* **136** (1989), 283-292.

[F] L. Fuchs, Abelian Groups, Akadémiai Kiadó, Budapest, 1958.