J. Austral. Math. Soc. (*Series A*) 36 (1984), 69–86

ON TRANSITIVE PERMUTATION GROUPS WITH A SUBGROUP SATISFYING A CERTAIN CONJUGACY CONDITION

CHERYL E. PRAEGER

(Received 6 July 1982)

Communicated by D. E. Taylor

Abstract

Let G be a transitive permutation group of degree n and let K be a nontrivial pronormal subgroup of G (that is, for all g in G, K and K^g are conjugate in $\langle K, K^g \rangle$). It is shown that K can fix at most $\frac{1}{2}(n-1)$ points. Moreover if K fixes exactly $\frac{1}{2}(n-1)$ points then G is either A_n or S_n, or $\mathrm{GL}(d,2)$ in its natural representation where $n = 2^d - 1 \geqslant 7$. Connections with a result of Michael O'Nan are discussed, and an application to the Sylow subgroups of a one point stabilizer is given.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 20 B 05, 20 B 10.

This paper is concerned with finding an upper bound for the number of fixed points of certain subgroups of a transitive permutation group G. In [16] it was shown that the number of fixed points of a Sylow subgroup was strictly less than half the total number of points. Here we generalise that result to the class of nontrivial pronormal subgroups of G, that is, nontrivial subgroups K such that for all g in G, K^g is conjugate to K by an element of $\langle K^g, K \rangle$. If p is a prime dividing the order of G a p-subgroup K of G is pronormal if and only if each Sylow p-subgroup of G contains exactly one conjugate of K, that is K weakly closed in any Sylow p-subgroup of G containing it. In particular Sylow subgroups are pronormal, and if G is soluble, then its Hall subgroups are pronormal. The main result of the paper is the following theorem. The proof is by induction and exploits results of Cameron [4, 5]. (Note that if K is a permutation group on a set Ω then $\mathrm{fix}_\Omega K$ and $\mathrm{supp}_\Omega K$ denote its set of fixed points in Ω and its support Ω-$\mathrm{fix}_\Omega K$ in Ω respectively.)

THEOREM 1. *Let G be a transitive permutation group on a set Ω of n points, and let K be a nontrivial pronormal subgroup of G. Suppose that K fixes f points of Ω. Then*

(a) $f \leqslant \frac{1}{2}(n-1)$, *and*

(b) *if* $f = \frac{1}{2}(n-1)$ *then K is transitive on its support in Ω, and either* $G \geqslant A_n$, *or* $G = \mathrm{GL}(d,2)$ *acting on the* $n = 2^d - 1$ *nonzero vectors, and K is the pointwise stabilizer of a hyperplane.*

This result may be compared, with a result of Michael O'Nan ([13], Theorem A) on subgroups of prime order of primitive permutation groups. We note that O'Nan's result is true without the restriction that the subgroups have prime power order. As a simple consequence of Theorem 1 and O'Nan's results we have Theorem 2.

THEOREM 2. *Let G be a primitive permutation group on a set Ω of n points and let K be a nontrivial subgroup of G satisfying: if* $g \in G$ *is such that* $\mathrm{supp}_\Omega K \cap \mathrm{supp}_\Omega K^g \neq \varnothing$, *then K is conjugate to K^g in* $\langle K, K^g \rangle$.

Then one of the following is true.

(i) $|\mathrm{fix}_\Omega K| < \frac{1}{2}(n-1)$,

(ii) $G \supseteq A_n$,

(iii) $G = \mathrm{GL}(d,2)$ *on the* $n = 2^d - 1 \geqslant 7$ *nonzero vectors,*

(iv) $G = \mathrm{AGL}(d,2)$ *on the* $n = 2^d \geqslant 8$ *vectors.*

(For if K is conjugate to K^g in $\langle K, K^g \rangle$ for all g in G then K is pronormal and the result follows from Theorem 1; if not then the result follows from [16] Theorem A.) A less trivial consequence is the following; we note that O'Nan's result is not strictly necessary for the proof.

THEOREM 3. *Let G be a primitive permutation group on a set Ω of n points and let K be a nontrivial subgroup of G such that* $\mathrm{fix}_\Omega K$ *is nonempty. Assume that K satisfies*

(*) *If* $g \in G$ *is such that* $\mathrm{fix}_\Omega K \cap \mathrm{fix}_\Omega K^g \neq \varnothing$ *then K is conjugate to K^g in* $\langle K, K^g \rangle$.

Then $f = |\mathrm{fix}_\Omega K| \leqslant \frac{1}{2}n$, *and if* $f = \frac{1}{2}n$ *either* $G \supseteq A_n$ *or* $G = \mathrm{AGL}(m,2)$ *with* $n = 2^m \geqslant 8$.

This has the following corollary.

COROLLARY TO THEOREM 3. *Let G be a primitive permutation group on a set Ω of n points, let p be a prime dividing* $|G|/n$, *and let K be a Sylow p-subgroup of the stabilizer G_α of the point α of Ω. Then* $f = |\mathrm{fix}_\Omega K| \leqslant \frac{1}{2}n$ *and if* $f = \frac{1}{2}n$ *then* $n = 2p$ *and* $G \supseteq A_n$.

Theorem 1 is proved in Section 2, and Section 1 consists of preliminary results among which is the following application of a result of Wielandt.

PROPOSITION 4. *Let G be a primitive permutation group on Ω. For $\alpha \in \Omega$ suppose that K is a subgroup of G_α satisfying:*
(**) If $K^g \leqslant G_\alpha$ for $g \in G$, then $K^{gh} = K$ for some h in G_α.
Then K acts nontrivially on each orbit of G_α in $\Omega - \{\alpha\}$.

In Section 3 we prove a generalization of Theorem 3 and its corollary for transitive groups. Our notation is fairly standard and follows the conventions of [20]. However when it is convenient we shall use the notation of D. G. Higman [7] for suborbits of a permutation group. If G acts as a permutation group on a set Ω, we shall call on orbit of G in $\mathrm{supp}_\Omega G$ a nontrivial orbit.

The author has appreciated the help of Drs. Marcel Herzog, Chris Godsil and Brendan McKay in discussions relating to this work.

1. Preliminary results

In this section we first prove Proposition 4. Then we examine some properties of the groups of Theorem 1(b) and some properties of pronormal subgroups which will be useful in the inductive proof of Theorem 1. Finally we state for convenience some known results about primitive groups with a small subdegree.

PROOF OF PROPOSITION 4. Let G, K satisfy the hypotheses of Proposition 4, and let Γ be an orbit of G_α in $\Omega - \{\alpha\}$. By [20] 18.1, for some g in G, $K^g \leqslant G_\alpha$ and acts nontrivially on Γ. Thus for some x in K^g, β in Γ, we have $\beta^x \neq \beta$. By condition (**), $K^{gh} = K$ for some h in G_α. Then $x^h \in K$, $\beta^h \in \Gamma^h = \Gamma$, and $(\beta^h)^{h^{-1}xh} = \beta^{xh} \neq \beta^h$. Thus K acts nontrivially on Γ.

Note we consider the groups A_n and $\mathrm{GL}(d, 2)$.

LEMMA 1.1. *Suppose that G, K satisfy the hypotheses of Theorem 1 and $G \geqslant A_n$. Then K has only one nontrivial orbit. If this orbit has length a then $f = a - i_a(n)$, where $i_a(n)$ is the integer satisfying $1 \leqslant i_a(n) \leqslant a$, $n + i_a(n) \equiv 0 (\mathrm{mod}\ a)$. Thus if $f = \frac{1}{2}(n-1)$ then $n = 2a - 1$.*

PROOF. Let a be the length of the shortest nontrivial orbit of K. Suppose that $f \geqslant a$ and let Γ be a K-orbit of length a. Then there is an element g in A_n such that $\Gamma^g \subseteq \mathrm{fix}_\Omega K$. Then Γ^g is an orbit both of K^g and of $\langle K, K^g \rangle$. Since K is pronormal $K^{gh} = K$ for some h in $\langle K, K^g \rangle$, but then $\Gamma^{gh} = \Gamma^g$ is an orbit for K, contradiction. Hence $f < a$ and so $f = a - i_a(n)$ and the rest follows immediately.

Clearly $G \geqslant A_n$ has nontrivial pronormal subgroups. As a corollary to the proof we have

COROLLARY 1.2. *If G, K satisfy the hypotheses of Theorem 1 and G is a-transitive then $f = a - i_a(n)$ (where a is the length of the shortest nontrivial orbit of K).*

LEMMA 1.3. *Suppose that $G = \mathrm{GL}(d,2)$, $d \geqslant 3$, acting on the set Ω of $n = 2^d - 1$ nonzero vectors. Let K be the pointwise stabilizer of a hyperplane Δ. Then K is elementary abelian of order 2^{d-1}, is regular on $\Omega - \Delta$, and is pronormal. Moreover no subgroup of K of index 2 is pronormal in G.*

PROOF. It is well known that K is elementary abelian of order 2^{d-1} and acts regularly on $\Omega - \Delta$. Moreover K is pronormal since each Sylow 2-subgroup of $\mathrm{GL}(d,2)$ contains exactly one conjugate of K. Now K has 2^{d-1} subgroups of index 2 and each of these groups has two orbits of equal length in $\Omega - \Delta$. Thus there are $2^d - 2$ orbits in $\Omega - \Delta$ of these subgroups, and each of these orbits is the intersection of $\Omega - \Delta$ with one of the $2^d - 2$ hyperplane distinct from Δ. Since G is 2-transitive on the set of hyperplanes it follows that all subgroups of index 2 in K are conjugate in G. If L, L' are distinct subgroups of K of index 2, then both L and L' are normal in $\langle L, L' \rangle = K$ and so neither is pronormal in G.

In the proof of Theorem 1 we shall use the following results repeatedly.

LEMMA 1.4. *Suppose that K is a nontrivial pronormal subgroup of the group G.*

(a) *If $K \leqslant H \leqslant G$ then K is a pronormal subgroup of H.*

(b) *If X is a normal subgroup of G not containing K, then KX/X is a nontrivial pronormal subgroup of G/X.*

LEMMA 1.5. *Suppose that K is a nontrivial pronormal subgroup of a primitive permutation group G on Ω. If $\alpha \in \mathrm{fix}_\Omega K$ then K acts nontrivially on each orbit of G_α in $\Omega - \{\alpha\}$.*

The proof of Lemma 1.4 is straightforward and that of Lemma 1.5 is simply an application of Proposition 4. Finally we quote some results about primitive permutation groups with small subdegrees.

LEMMA 1.6. *Let G be a simply transitive primitive permutation group on Ω of degree n. Let $\alpha \in \Omega$ and suppose that G_α has an orbit of length k in $\Omega - \{\alpha\}$.*

(a) ([20] 18.7, 18.8) *If* $k = 2$ *then* n *is prime and* G *is a Frobenius group of order* $2n$.

(b) ([21]) *If* $k = 3$ *then* G_α *is soluble with order dividing* 48.

(c) ([18] *Theorem* 2.1 (10)) *If* k *is* 3 *or* 4 *then either* n *is divisible by a prime greater than* 3 *or* $n = 2^c$ *or* $n = 3^c$ *for some* $c < k$.

2. Proof of Theorem 1

Suppose that Theorem 1 is false, let n be the least integer for which a counterexample of degree n exists, and let G be a counterexample of degree n. Thus G has a nontrivial pronormal subgroup K with $f \geqslant \frac{1}{2}(n-1)$ fixed points in Ω, $G \not\geqslant A_n$, and G is not $\mathrm{GL}(d,2)$ in its natural representation for any d.

Lemma 2.1. *G is primitive on Ω.*

Proof. Suppose that G has a set $\Sigma = \{B_1, \ldots, B_t\}$ of blocks of imprimitivity in Ω with $|\Sigma| = t > 1$, $|B_i| = b > 1$, and $n = tb$. Since any block containing a point of $\mathrm{fix}_\Omega K$ is fixed setwise by K and since $f > 0$ it follows that $\mathrm{fix}_\Sigma K$ is nonempty. By [20] 3.5 applied to K^Σ as a subgroup of G^Σ, $N_G(K)$ is transitive on $\mathrm{fix}_\Sigma K$. It follows that $f_B = |\mathrm{fix}_B K|$ is independent of the choice of B in $\mathrm{fix}_\Sigma K$. Thus if we set $f_\Sigma = |\mathrm{fix}_\Sigma K|$ then $f = f_\Sigma f_B$. If for B in $\mathrm{fix}_\Sigma K$, $K^B \neq 1$ then the hypotheses of Theorem 1 hold for the setwise stabilizer of B acting on B. Hence by minimality, $f_B \leqslant \frac{1}{2}(b-1)$, and so $f \leqslant tf_B < \frac{1}{2}(n-1)$. If on the other hand $K^B = 1$ for B in $\mathrm{fix}_\Sigma K$, then $f = bf_\Sigma$ and so $K^\Sigma \neq 1$. The hypotheses of Theorem 1 then hold for G^Σ and again by minimality, $f_\Sigma \leqslant \frac{1}{2}(t-1)$, and $f < \frac{1}{2}(n-1)$. Thus G is primitive on Ω, since $f \geqslant \frac{1}{2}(n-1)$.

Lemma 2.2. *G is 2-transitive on Ω and $f = \frac{1}{2}(n-1)$.*

Proof. Let $\alpha \in \mathrm{fix}_\Omega K$. Then by Lemma 1.5, K acts nontrivially on each orbit Γ of G_α in $\Omega - \{\alpha\}$. By Lemma 1.4, the hypotheses of the theorem hold for G_α^Γ with nontrivial pronormal subgroup K^Γ. Let $\{\Gamma_j;\ 1 \leqslant j \leqslant s\}$ be the G_α-orbits in $\Omega - \{\alpha\}$, $s \geqslant 1$, and let $|\Gamma_j| = n_j$ and $|\mathrm{fix}\, K \cap \Gamma_j| = f_j$, $1 \leqslant j \leqslant s$. Then by minimality $f = 1 + \Sigma f_j \leqslant 1 + \frac{1}{2}\Sigma(n_j - 1) = \frac{1}{2}(n + 1 - s)$. Thus either $f = \frac{1}{2}(n - 1)$ and $s \leqslant 2$ or $s = 1$ and $f = \frac{1}{2}n$. Assume that G_α is transitive on $\Omega - \{\alpha\}$ and $|\mathrm{fix}\, K - \{\alpha\}| = \frac{1}{2}((n-1)-1)$. Then by minimality, either $G_\alpha \geqslant A_{n-1}$, or $G_\alpha = \mathrm{GL}(d,2)$ with $n - 1 = 2^d - 1$ and K the pointwise stabilizer of a hyperplane. Since $G \not\geqslant A_n$, $G_\alpha = \mathrm{GL}(d,2)$ is the collineation group of $(d-1)$-dimensional projective geometry over a field of order 2 and $d \geqslant 3$. It follows from [6] 2.4.34 that G is a collineation group of a d-dimensional affine geometry over a field of order 2. Since fix $K - \{\alpha\}$ is a hyperplane of the projective geometry, then both fix K and supp K are hyperplanes of the affine geometry. Now G is transitive on hyperplanes (since G_α is transitive on the hyperplanes containing α), and so $(\operatorname{supp} K)^g = \operatorname{fix} K$ for some g in G. Then K and K^g centralise each other, a contradiction since K is pronormal.

Thus $f = \frac{1}{2}(n-1)$ and $s \leq 2$. Assume that $s = 2$. Then $f_j = \frac{1}{2}(n_j - 1)$ for $j = 1, 2$, and by minimality G_α is doubly transitive on both Γ_1 and Γ_2, contradicting [20] 17.7. Thus G is 2-transitive on Ω.

Let G be d-transitive but not $(d+1)$-transitive. Then since $G \not\supseteq A_n$ it follows from [20] 15.1 that $2 \leq d \leq 5$. It is easy to check that $n > 11$ and hence $f > d$. Let Δ be a subset of Ω of size $m = n - d + 1$ such that $\Omega - \Delta \subseteq \operatorname{fix}_\Omega K$, and let H be the pointwise stabilizer in G of $\Omega - \Delta$. Then H is transitive but not 2-transitive on Δ, $K \subseteq H$, and $|\operatorname{fix}_\Delta H| = f - d + 1 = \frac{1}{2}(m - d) = e > 0$, say. Information about an imprimitive H is given by the next lemma.

Lemma 2.3. *Let X be a transitive imprimitive permutation group on a set Δ of $m < n$ points having a nontrivial pronormal subgroup K with $e = \frac{1}{2}(m - z) > 0$ fixed points where $2 \leq z \leq 5$. Then one of the following is true.*

(i) *$m = yz$, X has a set of z or y blocks of imprimitivity in Δ of length y or z respectively, and in either case the action of degree y is A_y or S_y (with $y \geq 3$ and y odd), or* $\mathrm{GL}(r, 2)$ *(with $y = 2^r - 1 \geq 7$).*

(ii) *$m = 4y$, $z = 4$, X has $2y$ blocks of imprimitivity of length 2 and X acts on the set of $2y$ blocks as an imprimitive group with 2 blocks of imprimitivity of length y. The representation of degree y is as in* (1).

(iii) *$m = 2x$, $z = 4$, X has 2 or x blocks of imprimitivity of length x or 2, the representation of degree x is primitive and the fixed point set of K in this representation has size $\frac{1}{2}(x - 2)$.*

Proof. Assume that X is imprimitive on Δ with a set $\Sigma = \{B_1, \ldots, B_t\}$ of $t > 1$ blocks of imprimitivity of length $b > 1$, where $m = tb$. Assume that the blocks are maximal proper blocks so that X acts primitively on Σ. As in Lemma 2.1 $\operatorname{fix}_\Sigma K$ is nonempty and $N_X(K)$ is transitive on $\operatorname{fix}_\Sigma K$. Thus if $e_\Sigma = |\operatorname{fix}_\Sigma K|$ and $e_B = |\operatorname{fix}_B K|$ for B in $\operatorname{fix}_\Sigma K$, then $e = e_\Sigma e_B$. Suppose first that for B in $\operatorname{fix}_\Sigma K$, $K^B \neq 1$. Then by minimality $e_B = \frac{1}{2}(b - u)$ for some positive integer u. Also either $e_\Sigma = t$ or $K^\Sigma \neq 1$ so that (again by minimality) $e_\Sigma < \frac{1}{2}t$. In the latter case $\frac{1}{2}(m - z) = e < \frac{1}{2}te_B = \frac{1}{4}(m - tu)$, that is $m < 2z - tu$ so that $e = \frac{1}{2}(m - z) < \frac{1}{2}(z - tu) \leq \frac{3}{2}$. Hence $e = 1$, $z = 5$, and $m = 7$ which is a contradiction. Thus $\frac{1}{2}(m - z) = e = te_B = \frac{1}{2}(m - tu)$, so that either $t = z$, $u = 1$ and (i) follows by minimality, or $z = 4$ and $t = u = 2$; here consideration of the action on B_1 and B_2 of the subgroup of X fixing B_1 and B_2 setwise shows that one of (i), (ii), (iii), is true. Thus assume that K fixes pointwise each block in $\mathrm{fix}_\Sigma K$. Then $K^\Sigma \neq 1$ and by minimality $e_\Sigma = \frac{1}{2}(t - u)$ for some positive integer u, so that $\frac{1}{2}(m - z) = e = be_\Sigma = \frac{1}{2}(m - bu)$. As above either $b = z$, $u = 1$ and (i) is true, or $z = 4$, $b = u = 2$, and as X is primitive on Σ, (iii) is true.

The next lemma gives information about a primitive group H, and we make this explicit in the corollary.

LEMMA 2.4. *Let X be a primitive permutation group on a set Δ of $m \leqslant n$ points having a nontrivial pronormal subgroup K with $e = \frac{1}{2}(m - z) \geqslant 0$ fixed points where $1 \leqslant z \leqslant 5$. Then*

(i) *if $z = 1$, X is 4-primitive or $X = \mathrm{GL}(d, 2)$, or $X \supseteq A_m$,*

(ii) *if $z = 2$, X is 3-primitive, or $m = 6$, $X = \mathrm{PGL}(2,5)$, or $m = 4$, $X = A_4$, or $m = 2$,*

(iii) *if $z = 3$, X is 2-primitive, or $m = 9$ and X is $\mathrm{ASL}(2,3)$ or $\mathrm{AGL}(2,3)$, or $m = 5$ and $|X|$ is 10 or 20, or $m = 3$,*

(iv) *if $4 \leqslant z \leqslant 5$, X has rank at most z; and if $z = 4$ and X is 2-transitive then X is 2-primitive.*

COROLLARY TO LEMMA 2.4. *H is primitive and d is 4 or 5.*

This corollary follows immediately from Lemma 2.2 and Lemma 2.4 parts (i), (ii), and (iv).

PROOF OF LEMMA 2.4. Suppose that X satisfies the hypotheses of the lemma with degree $m \leqslant n$, and $e = |\mathrm{fix}_\Delta K| = \frac{1}{2}(m - z) \geqslant 0$, $1 \leqslant z \leqslant 5$. Suppose also that the lemma is true for groups of smaller degree. Clearly we may assume that $m \geqslant 7$, and $e > 0$. The proof is given in two steps.

Step 1. First assume that X is not 2-transitive; then $z \geqslant 2$ by minimality and Lemma 2.2. Let $\delta \in \mathrm{fix}_\Delta K$ and let $\Gamma_1, \ldots, \Gamma_s$ be the orbits of X_δ in $\Delta - \{\delta\}$, where $|\Gamma_i| = m_i$ for each $i \leqslant s$, and $s \geqslant 2$. By Lemma 1.5, K acts nontrivially on each Γ_i, and so by minimality $e_i = |\mathrm{fix}\, K \cap \Gamma_i| = \frac{1}{2}(m_i - z_i)$ for some positive integer z_i, and $\Sigma z_i = z + 1$. If $z_j = 1$ for some $j \leqslant s$ then by minimality X_δ acts on Γ_j as A_{m_j}, S_{m_j}, or $\mathrm{GL}(r, 2)$ with $m_j = 2^r - 1$. By [20] 17.7, X_δ cannot act 2-transitively on all of the Γ_j so we conclude that at least one of the z_j is greater than 1. It is convenient to order the Γ_j so that $z_1 \leqslant z_2 \leqslant \cdots \leqslant z_s$; then $z_s \geqslant 2$. Suppose next that $z_j = 1$ for all $j \leqslant s - 1$. Then by [5], $s \leqslant 3$ and if $s = 3$ then $m = 4t^2(t + 2)^2$, and $m_1 = m_2 = t(2t^2 + 4t + 1)$ for some odd positive integer t. Moreover by [4, 17], $m_3 = m_1(m_1 - 1)/k$ where k is 1, 2, or 3. It follows that $t = 1$, $m_1 = 7$, $k = 2$, and (by [5]), $X_\delta^{\Gamma_1} \supseteq A_7$. Here X_δ acts on Γ_3 as on unordered pairs of points of Γ_1, and as K fixes 3 points of Γ_1 and has one orbit of length 4 (in order to be

https://doi.org/10.1017/S1446788700027348 Published online by Cambridge University Press

pronormal) it follows that K fixes exactly 3 points of Γ_3. Thus $z_3 = 15 > z$ which is a contradiction. Thus $s = 2$, $z_1 = 1$, and $2 \leqslant z_2 = z \leqslant 5$. Assume here that z is 2 or 3. Since X_δ on Γ_1 is alternating or symmetric or $\mathrm{GL}(r,2)$, by [4, 17], $m_2 = m_1(m_1 - 1)/k$ where k is 1, 2, or 3, and if $k = 3$ then $r \geqslant 4$. Also, as X_δ cannot be 2-transitive on Γ_2 it follows that X_δ is imprimitive on Γ_2 or $z_2 = 3$ and m_2 is 3 or 5. In the latter case, $m_2 \neq 5$ as $m_2 = m_1(m_1 - 1)/k$, and $m_2 \neq 3$ follows from [20] 18.4. In the imprimitive case it follows from [20] 18.2 and Lemma 2.3(i) that $m_2 = z_2 m_1$ so that (m_1, m_2) is $(3,6)$, $(5,10)$, or $(7,21)$. If $m_1 = 3$ then (see [18]), X is A_5 or S_5 on unordered pairs; here $e = 4$ and so K is generated by a transposition. However such a group is not pronormal. If $m_1 = 5$ then $e = 7$ divides $|X|$ which is impossible by [18]. If $m_1 = 7$ then $m = 39$, and $e = 13$ divides $|X|$ which is impossible by [20] 13.10. Thus if X is not 2-transitive then $z \geqslant 3$; if $3 \leqslant z \leqslant 6$ then X has rank at most z; and if $z = 3$ and X has rank 3 then $z_1 = z_2 = 2$.

Assume then that $z = 3$, $z_1 = z_2 = 2$. Then as X_δ cannot be 2-transitive on both Γ_1 and Γ_2 we may assume that it is imprimitive on Γ_1 and its action satisfies Lemma 2.3(i); in particular $m_1 \equiv 2 (\mathrm{mod}\, 4)$ and $m_1 \geqslant 6$. Suppose that X_δ is primitive on Γ_2. Then either X_δ is 3-transitive on Γ_2, or $m_2 = 4$ and $X_\delta^{\Gamma_2} = A_4$, or $m_2 = 2$. By Lemma 1.6, $m_2 \neq 2$ (since $m_1 \geqslant 6$). By [4], $m_1 = m_2(m_2 - 1)/k$ where k is 1 or 2, or $m = (x+1)^2(x+4)^2$, $m_2 = (x+1)(x^2+5x+5)$, $k = (x+1)(x+2)$ for some integer $x \geqslant 1$. In the latter case x is odd since m_2 is even, and hence m_1 is odd, contradiction. Hence k is 1 or 2. By [20] 17.6, the only nonabelian composition factor of X_δ is A_x, $x = \frac{1}{2}m_1$, or $\mathrm{GL}(r,2)$, $\frac{1}{2}m_1 = 2^r - 1$, $r \geqslant 3$. Also if m_2 is a power of 2 then, since $m_1 = 2(\mathrm{mod}\, 4)$ and $m_1 \geqslant 6$, we have $m_1 = 6$, $m_2 = 4$, $m = 11$, a contradiction to [20] 11.6 and 11.7. Thus we may assume (by [20] 11.3 and 12.1 and [3] page 202), that $X_\delta^{\Gamma_2}$ has a simple normal subgroup S which is 2-transitive of even degree m_2, where S is A_x, or $\mathrm{GL}(r,2)$, and $\frac{1}{2}m_1$ is x, or $2^r - 1$ respectively. By [2, 10], $\left(\frac{1}{2}m_1, m_2\right)$ is $(5,6)$, $(7,8)$, or $(15,8)$ all of which contradict $m_1 = m_2(m_2 - 1)/k$, $k \leqslant 2$.

Thus X_δ is imprimitive on both Γ_1 and Γ_2, with the actions given by Lemma 2.3. By [20] 18.2 it follows that $m_1 = m_2 \equiv 2(\mathrm{mod}\, 4)$ and $m_1 \geqslant 6$. If $m_1 = 6$ then $m = 13$ contradicting [20] 11.6 and 11.7. If $m_1 = 10$ then $m = 21$, $e = 9$, and $|K|$ is divisible by 3. Hence $|N(K)|$ is divisible by 27. However by [20] 13.10, $|X|$ is not divisible by 25 and so X_δ has only one composition factor A_5. It follows that $|X_\delta|$ is not divisible by 9, a contradiction. Thus $m_1 \geqslant 14$. Suppose that A_x, $x = \frac{1}{2}m_1$ is a composition factor of X_δ. Then X_δ contains a 5-element of degree at most 20, a contradiction to [20] 13.10. Thus $x = \frac{1}{2}m_1 = 2^r - 1$, and X_δ has a composition factor $\mathrm{GL}(r,2)$, $r \geqslant 3$. Let Y be the smallest normal subgroup of X_δ such that X_δ/Y is a (possibly trivial) 2-group. Then KY is represented as $\mathrm{GL}(r,2)$ (acting on points or hyperplanes), on either a set of x blocks of imprimitivity in Γ_j or on each of two blocks of length x in Γ_j, for $j = 1$ and $j = 2$. Also the kernel of all these representations of KY is a possibly trivial 2-group. Let θ be one of the sets of size x on which KY is represented. Then K^θ is the pointwise stabilizer of a hyperplane and its normalizer in $(KY)^\theta$ is the setwise stabilizer of the hyperplane and has index x in $(KY)^\theta$; that is to say, if Y_1 is the kernel of KY on θ then $N_{KY}(KY_1)$ has index x in KY. If $g \in N_{KY}(KY_1)$ then $K^g \leqslant KY_1$ and so K is conjugate to K^g in $\langle K, K^g \rangle \leqslant KY_1$. Thus since $N_{KY}(KY_1)$ contains $N_{KY}(K)$, then $|KY\colon\ N_{KY}(K)| = x\,|N_{KY}(KY_1)\colon\ N_{KY}(K)| = x\,|KY_1\colon\ N(K) \cap KY_1|$. Now $(KY)/Y_1 \simeq \mathrm{GL}(r,2)$ and KY has j composition factors isomorphic to $\mathrm{GL}(r,2)$ for some $1 \leqslant j \leqslant 4$. If $j > 1$ then KY_1 is represented as $\mathrm{GL}(r,2)$ on one of the sets of length x described above. We define Y_k inductively as the kernel of a representation of KY_{k-1} as $\mathrm{GL}(r,2)$ as above, for $1 < k \leqslant j$. Then as above, $|KY_{k-1}\colon N(KY_k) \cap KY_{k-1}| = x$ and the number of conjugates of K in $N(KY_k) \cap KY_{k-1}$ is equal to the number of conjugates of K in KY_k. Thus $|KY_{k-1}\colon N(K) \cap KY_{k-1}| = x\,|(N(KY_k) \cap KY_{k-1})\colon\ (N(K) \cap KY_{k-1})| = x\,|KY_k\colon\ N(K) \cap KY_k|$ for $1 < k \leqslant j$. Hence $|KY\colon N_{KY}(K)| = x^j\,|KY_j\colon N(K) \cap KY_j|$, whether or not $j = 1$. As we remarked above Y_j is a possibly trivial 2-group, and $|X_\delta\colon KY|$ is a power of 2. Thus $|X_\delta\colon N(K) \cap X_\delta| = x^j 2^c$ for some $c \geqslant 0$, $1 \leqslant j \leqslant 4$. Now $e = 4(2^{r-1} - 1) + 1 = 2x - 1$ divides $|X\colon N(K) \cap X_\delta|$ which divides $mx^4 2^c$, and this is clearly impossible. Thus if X is not 2-transitive then $z \geqslant 4$.

Step 2. In this second part of the proof we assume that X is 2-transitive but not 2-primitive on Δ of degree $m \leqslant n$, and $e = |\mathrm{fix}\, K| = \frac{1}{2}(m - z)$ where $1 \leqslant z \leqslant 4$. Then if $\delta \in \mathrm{fix}_\Delta K$, X_δ satisfies one of (i), (ii), (iii) of Lemma 2.3 where $e - 1 = |\mathrm{fix}_\Delta K - \{\delta\}| = \frac{1}{2}((m-1) - (z+1))$, $2 \leqslant z + 1 \leqslant 5$. As $m \geqslant 7$, $e - 1 > 0$. Set $u = z + 1$. If in (i) or (iii), X_δ has a set of u or 2 blocks respectively then the kernel of the action on blocks is 2-transitive on each of the blocks. By [12] Theorem D it follows that $X \geqslant \mathrm{PSL}(3,3)$, and $e = 5$ divides $|X|$ which is impossible. If in (i) X_δ acts as A_y or S_y on a set of y blocks of length u then as K fixes a block pointwise and y is odd, it follows from [14] that X contains $\mathrm{PSL}(3, u)$, $u \equiv 2$ or 4, or X is an extension of an elementary abelian group of order 16 by A_5 or S_5, $u = 3$. If $u = 2$ then (i) is true. If $u = 4$ then $|X|$ is divisible by $e\,|K|$ which is divisible by 27, a contradiction. If $u = 3$ then $e = 7$ divides $|X|$, also a contradiction. Thus in case (i) X_δ acts as $\mathrm{GL}(r,2)$ on a set of $2^r - 1$ blocks of length u. If $r = 3$ then $m = 1 + 7u$ and $e = 1 + 3u$; e does not divide $|X|$ if u is 3 or 4 so u is 2 or 5. If $u = 2$ then the 7-element in $N_X(K)$ must be a 7-cycle on Δ, contradiction. If $u = 5$ then by [15] Corollary B1, the translates of $B \cup \{\delta\}$ form the blocks of a design on Δ with $\lambda = 1$, where B is one of the blocks of X_δ of length u; further $\mathrm{fix}_\Delta K$ is the union of three blocks of this design containing δ which forces $N_X(K)$ to fix δ whereas $N_X(K)$ is transitive on $\mathrm{fix}_\Delta K$. Thus $r \geqslant 4$. Let Y be the setwise stabilizer of one of the blocks B of the set Σ of blocks of X_δ in $\Delta - \{\delta\}$. Then Y^Σ is an elementary abelian group N of order 2^{r-1} extended by $\mathrm{GL}(r-1, 2)$ acting irreducibly on N; thus Y^Σ has no transitive representations of

https://doi.org/10.1017/S1446788700027348 Published online by Cambridge University Press

degree u, $2 \leqslant u \leqslant 5$, and so the kernel Z of X_δ on Σ is nontrivial. It follows from [14] Lemma 1.1 that either $u = 2$, $X = \mathrm{GL}(r+1, 2)$ (and so (i) is true), or Z is semiregular on $\Delta - \{\delta\}$. Assume the latter. Since K is the kernel of KZ acting on B, where $B \in \mathrm{fix}_\Sigma K$, it follows that K and Z centralise each other. Now $|X_\delta: N(NZ) \cap X_\delta| = 2^r - 1$; any conjugate K^g of K by an element g in $N(KZ) \cap X_\delta$ is conjugate to K in $\langle K, K^g \rangle \subseteq KZ$ and hence is equal to K. Thus $N(KZ) \cap X_\delta \subseteq N(K) \cap X_\delta$ and it follows that $|X_\delta: N(K) \cap X_\delta| = 2^r - 1$. Thus $e = 1 + u(2^{r-1} - 1) = |N(K): N(K) \cap X_\delta|$ divides $|X: N(K) \cap X_\delta| = (1 + u(2^r - 1))(2^r - 1)$. It follows that $u = 2$, and by [9] 6C(2), X has a regular normal subgroup of order $m = 3^c = 2^{r+1} - 1$; but there is no solution c for any $r \geqslant 4$. Thus we may assume that case (i) of Lemma 2.3 does not hold, and so $u = 4$.

If in case (iii) of Lemma 2.3 X_δ has a set Σ of blocks of length 2, by minimality X_δ is 3-primitive on Σ or x is 6 and $X_\delta^\Sigma = \mathrm{PGL}(2,5)$ or x is 4 and $X_\delta^\Sigma = A_4$ (since $m \geqslant 7$). In the first and third cases X is $\mathrm{AGL}(2,3)$ or $\mathrm{ASL}(2,3)$ by [15] Theorem C and Theorem B respectively, while the case $x = 6$ cannot arise (since $e = 11$ cannot divide $|X|$). Suppose that case (ii) of Lemma 2.3 holds, with $m - 1 = 4y$. If A_y is involved then consideration of a 5-element in A_y and [20] 13.10 shows that y is 3 or 5. If $y = 3$ then $X \geqslant \mathrm{PSL}(3,3)$ (see [18]) and X_δ does not have blocks of size 2. If $y = 5$ then 25 does not divide $|X|$, by [20] 13.10, while 27 divides $e|K|$ which divides $|X|$; these two assertions are incompatible with the structure of X_δ as its only composition factors are Z_2 and A_5. Thus $\mathrm{GL}(r,2)$ is involved in X_δ where $y = 2^r - 1 \geqslant 7$. By [11] the kernel Z of X_δ on its set of $2y$ blocks in $\Delta - \{\delta\}$ has order at most 2 and so K and Z centralise each other. It follows as above that $e = 1 + 4(2^{r-1} - 1)$ divides $|X: N(K) \cap X_\delta| = (1 + 4(2^r - 1))(2^r - 1)$, which gives a contradiction.

Steps (1) and (2) complete the proof of Lemma 2.4 after noting that none of $\mathrm{ASL}(2,3)$, $\mathrm{AGL}(2,3)$ and $\mathrm{PGL}(2,5)$ have transitive extensions.

Lemma 2.5. *Let X be a primitive permutation group on a set Δ of $m < n$ points having a nontrivial pronormal subgroup K with $e = \frac{1}{2}(m-4) \geqslant 0$ fixed points. Then X is 2-transitive.*

Proof. Suppose that X is not 2-transitive, and that m is the least degree for which such a group X exists. Then (see [18]) $m \geqslant 16$. Let $\delta \in \mathrm{fix}_\Delta K$ and let $\Gamma_1, \ldots, \Gamma_s$, $s \geqslant 2$, be the orbits of X_δ in $\Delta - \{\delta\}$, where $|\Gamma_i| = m_i$, $|\mathrm{fix}\, K \cap \Gamma_i| = e_i = \frac{1}{2}(m_i - z_i)$, and $1 \leqslant z_1 \leqslant z_2 \leqslant \cdots \leqslant z_s$. By Lemma 2.4, $2 \leqslant s \leqslant 3$ and in the proof of that result we showed that if $s = 3$ then $z_2 > 1$, that is $z_1 = 1$, $z_2 = z_3 = 2$. In this case by [4, 17] and minimality, m_2, say, is $m_1(m_1 - 1)/k$ where $k \leqslant 3$ and $m_1 \geqslant 15$ if $k = 3$. Further by Lemma 2.4, [20] 17.7, and [5], X_δ is imprimitive on both Γ_2 and Γ_3, and by Lemma 2.3, and [20] 18.2–18.4, $m_2 = m_3 = 2m_1$. Thus $m_1 = 2k + 1$ is 3 or 5. If $m_1 = 3$ then $m = 16$, and we have a contradiction to

https://doi.org/10.1017/S1446788700027348 Published online by Cambridge University Press

Lemma 1.6. If $m_1 = 5$ then $m = 26$, and $e = 11$ divides $|X|$ contradicting [20] 13.10.

Thus $s = 2$ and (z_1, z_2) is $(1, 4)$ or $(2, 3)$. Consider the case $(1, 4)$ first. By minimality and [4, 17] $m_2 = m_1(m_1 - 1)/k$ where $k \leqslant 3$ and m_1 is odd. By the minimality of m and [20] 17.7, X_δ is imprimitive on Γ_2 and so by Lemma 2.3, $m_2 \equiv 0 (\mathrm{mod}\, 4)$ so that $m_1 \equiv 1 (\mathrm{mod}\, 4)$. The case $k = 1$ is impossible by [1, 7]. Thus if $X_\delta^{\Gamma_1}$ is alternating or symmetric then by [4], $k = 2$ and $m_2 = 10 \not\equiv 0 (\mathrm{mod}\, 4)$, contradiction. Hence $m_1 = 2^d - 1$, $d \geqslant 3$; but again $m_1 \not\equiv 1 (\mathrm{mod}\, 4)$.

Thus $z_1 = 2$, $z_2 = 3$. By [20] 17.7, X_δ is not primitive on both Γ_1 and Γ_2. Suppose that X_δ is primitive on Γ_1, so that X_δ is imprimitive on Γ_2. By the minimality of m either X_δ is 4-transitive on Γ_1 or m_1 is 2, 4 or 6 and X_δ is 2-transitive on Γ_1. The case $m_1 = 2$ is impossible by Lemma 1.6 since $e > 1$. Also by [4], $m_2 = m_1(m_1 - 1)/k$ where k is 1 or 2 (for even if m_1 is 4 or 6 then $k \leqslant \frac{1}{2}(m_1 - 1)$ so $k \leqslant 2$). Since m_1 is even and m_2 is odd, $k = 2$ and $m \equiv 2 (\mathrm{mod}\, 4)$. By [20] 17.6, X_δ is faithful on Γ_2 and so the only nonabelian composition factors of X_δ are A_x, where $x = m_2/3$ is odd, or $\mathrm{GL}(r, 2)$ where $m_2/3 = 2^r - 1 \geqslant 7$. Since $m_1 \equiv 2 (\mathrm{mod}\, 4)$, and by [3] page 202 and [20] 11.3 and 12.1, either $X_\delta^{\Gamma_1}$ has a simple normal subgroup S which is 3-transitive on Γ_1, or $m_1 = 6$. Thus if $m_1 > 6$, S is A_x, x odd, or $\mathrm{GL}(r, 2)$. By [2, 10] and since $m_1 \equiv 2 (\mathrm{mod}\, 4)$, it follows that $m_1 = 6$, and $X_\delta^{\Gamma_1} \simeq \mathrm{PGL}(2, 5)$. Thus $m_2 = 15$, $m = 22$, and $e|K^{\Gamma_2}|$ which is 27 or 81 divides $|X|$; further K contains a 3-element of degree at most 9 and this contradicts [13] Theorem E.

Thus X_δ is imprimitive on Γ_1 and its action is given by Lemma 2.3, in particular $m_1 \equiv 2 (\mathrm{mod}\, 4)$. Suppose that X_δ is primitive on Γ_2. Then by the minimality of m, either X_δ is 3-transitive on Γ_2 with $m_2 \geqslant 5$, or m_2 is 3, 5, or 9 and $X_\delta^{\Gamma_2}$ is soluble. In the latter case X_δ is soluble and $m_1 = 6$, $m_2 = 3$ or 9, by [20] 18.3, 18.4. If $m_2 = 3$ then $m = 10$ and this is impossible by [18], as S_5 on pairs has no subgroup fixing $e = 3$ pairs. If $m_2 = 9$ then K contains a 3-element of degree 6, a contradiction to [13] Corollary 4. Thus X_δ is 3-transitive on Γ_2 of odd degree $m_2 \geqslant 5$. Then by [3] page 202, and [20] 11.3, 12.1, $X_\delta^{\Gamma_2}$ has a simple normal subgroup S which is 2-transitive on Γ_2. By [20] 17.6, X_δ is faithful on Γ_1 and it follows that S is either A_x where $x = \frac{1}{2}m_1$ is odd or $\mathrm{GL}(r, 2)$ where $r \geqslant 3$, $m_1 = 2(2^r - 1)$. Hence by [2, 10] either $m_1 = 2m_2$ or (m_1, m_2) is $(14, 15)$. It follows from [4] that $m_1 = 2m_2 = 10$, $e|K^{\Gamma_1}| = 18$ divides $|X|$, and K contains a 3-element of degree 6, contradicting [13] Corollary 4.

Thus X_δ is imprimitive on both Γ_1 and Γ_2. It follows from Lemma 2.3 and [20] 18.2 that $m_1/2 = m_2/3 = x$ for some odd $x \geqslant 3$. If X_δ involves A_x with $x \geqslant 9$ then X_δ contains a 7-element of degree at most 35, contradicting [20] 13.10. Thus if X_δ involves A_x then x is 3, 5 or 7. If $x = 7$, a Sylow 5-subgroup of X fixes 11 points and so $|X|$ is divisible by 11, contradiction. If $x = 5$ then $e = 11$ divides $|X|$, contradiction. If $x = 3$ then $m = 16$, $m_2 = 9$ divides $|X|$, and $N(K)$

contains a 3-element g which fixes Γ_1 pointwise and so has degree at most 9. It follows from [13] Theorem E that a Sylow 3-subgroup of X has order 9, and it clearly fixes only one point and has an orbit length 9. Since $|\mathrm{fix}_\Delta\, g| = 7$ does not divide $|X|$ it follows by [20] 3.5 that $\langle g \rangle$ is not weakly closed in a Sylow 3-subgroup of X, and this clearly has the wrong orbit lengths. Thus $x = 2^r - 1$, $r \geq 3$, and the only insoluble composition factor of X_δ is $\mathrm{GL}(r, 2)$. By a similar argument to that in the proof of Lemma 2.4 we can show that $e = 5.2^{r-1} - 4$ divides $mx^5 6^c = (5x + 1)x^5 6^c$ for some $c \geq 0$. It follows that r is 3 or 4. If $r = 4$ then $m_1 = 30$, and $m_2 = 45$. If $\gamma \in \Gamma_1$ then $X_{\delta\gamma}$ has orbits in $\Gamma_1 - \{\gamma\}$ of lengths 1, 14, 14 or 14, 15. If $\Gamma(\gamma)$ is the orbit of X_γ of length 30 then $\lambda = |\Gamma_1 \cap \Gamma(\gamma)|$ is 0, 1, 14, 15, 28 or 29; since X is primitive $\lambda \neq 29$ by [7] Corollary 3, and by [7] Lemma 5, $2(19 - \lambda)/3$ is an integer. Hence $\lambda = 14$, which contradicts [7] Lemma 7. If $r = 3$ a similar argument shows that $\lambda = 7$, $\mu = 4$. However if $\eta \in \Gamma_2$ then the $X_{\delta\eta}$ orbit lengths in Γ_1 are sums of 1, 1, 6, 6, and no sum of these is equal to $\mu = 4$. This completes the proof of Lemma 2.5.

It follows from Lemmas 2.4 and 2.5 that $d = 5$ and H is primitive but not 2-transitive of rank at most 5. To complete the proof of Theorem 1 we show that this situation is impossible. This follows from the next lemma since we are assuming that H has degree $m = n - 4 > 7$.

LEMMA 2.6. *Let X be a primitive permutation group on a set Δ of $m < n$ points having a nontrivial pronormal subgroup K with $e = \frac{1}{2}(m - 5) \geq 0$ fixed points. Then either m is 5 or 7, or X is 2-transitive.*

PROOF. By [18] the result is true for $m \leq 13$, so assume that $m \geq 15$ is minimal such that X is not 2-transitive. Let $\delta \in \mathrm{fix}_\Delta\, K$ and let $\Gamma_1, \ldots, \Gamma_s$, $s \geq 2$ be the orbits of X_δ in $\Delta - \{\delta\}$, where $|\Gamma_i| = m_i$, $|\mathrm{fix}\, K \cap \Gamma_i| = e_i = \frac{1}{2}(m_i - z_i)$ and $1 \leq z_1 \leq \cdots \leq z_s$. By Lemma 2.4, $\Sigma\, z_i = 6$ and $2 \leq s \leq 4$, and from the proof of that result, if $s \geq 3$ then $z_{s-1} \geq 2$. First let $s = 4$; then $z_1 = z_2 = 1$, $z_3 = z_4 = 2$. By Lemma 2.4 and [5] X_δ is imprimitive on Γ_3 and Γ_4 and these actions are given by Lemma 2.3. By [20] 18.2, and Lemma 2.3, $2m_1 = 2m_2 = m_3 = m_4$. Now by [4] one of the subdegrees is equal to $m_1(m_1 - 1)/k \geq 2m_1$. Thus $k = \frac{1}{2}(m_1 - 1)$ and by [4], m_1 is 3 or 5. Thus $m = 1 + 6m_1$ is 19 or 31, a contradiction to [20] 11.6 and 11.7. Thus s is 2 or 3.

Suppose that s is 3. Then (z_1, z_2, z_3) is $(1, 2, 3)$ or $(2, 2, 2)$. Consider the case $(1, 2, 3)$; X_δ is 2-transitive on Γ_1 and (by Lemma 2.4, [5], Lemma 1.6, and [20] 17.7 and 18.3), imprimitive on Γ_2 and either imprimitive on Γ_3 or m_3 is 3 or 5 and X_δ is soluble. From Lemma 2.3, and [20] 18.2, 18.3, (m_1, m_2, m_3) is $(x, 2x, 3x)$ for some odd $x \geq 3$ or is $(3, 6, 3)$. The latter is impossible by [20] 11.6 and 11.7, so $m_1 = \frac{1}{2}m_2 = m_3/3 = x \geq 3$. Now by [4, 17] one of m_2, m_3 is $x(x - 1)/k$ where

$k \leqslant 3$. If $m_2 = x(x-1)/k$ then $k = (x-1)/2$ is 1 or 2 by [4] and m is 19 or 31, a contradiction as before. Similarly if $m_3 = x(x-1)/k$ then $x = 3k+1 = 7$ as m_1 is odd. Then $m = 43$, again a contradiction.

Thus if $s = 3$ then $z_1 = z_2 = z_3 = 2$. If X_δ is imprimitive on all three suborbits then by Lemma 2.3 and [20] 18.2, $m_1 = m_2 = m_3 = 2x \equiv 2(\text{mod } 4)$. If X_δ has A_x as a composition factor with $x \geqslant 9$ then X contains a 7-element of degree at most 42, a contradiction to [19]. Thus if X_δ has A_x as a factor then x is 3, 5, or 7 and m is 19, 31, or 43 respectively, a contradiction to [20] 11.6 and 11.7. So $x = 2^r - 1 \geqslant 7$. By a similar argument to that in the proof of Lemma 2.4, we can show that $e = 3x - 2$ divides $mx^6 2^c = (6x+1)x^6 2^c$ for some $c \geqslant 0$, a contradiction. Thus we may assume that X_δ is primitive on at least one suborbit and we may suppose that m_1 is maximal among the m_i such that X_δ is primitive on Γ_i. By the minimality of m, X_δ is 5-transitive on Γ_1, or $m_1 \leqslant 6$ and X_δ is 2-transitive on Γ_1. Then by [4], m_2 say is $m_1(m_1 - 1)/k$ where k is 1 or 2 (even if $m_1 \leqslant 6$). By the maximality of m_1, X_δ is imprimitive on Γ_2, and by Lemma 2.3, $m_2 \geqslant 6$ so $m_1 \geqslant 4$; also $m_2 \equiv 2(\text{mod } 4)$. By [20] 17.5, X_δ acts faithfully on the union of suborbits on which it is imprimitive. Hence by Lemma 2.3 and [20] 18.2 the only insoluble composition factor of X_δ is A_x, where $x = m_2/2 \geqslant 3$ is odd, or $GL(r,2)$ where $m_2 = 2(2^r - 1)$, $r \geqslant 3$. By [20] 11.3, 12.1 and [3] page 202, if $m_1 > 6$ then X_δ has a simple normal subgroup S which is 4-transitive on Γ_1 of even degree m_1. Since S must be A_x or $GL(r,2)$ this is impossible. Hence m_1 is 4 or 6. If m_1 is 4 then by [20] 18.3, X_δ is soluble so that $m_2 = 6$, and m_3 is 4 (if X_δ is primitive on Γ_3) or 6 (if X_δ is imprimitive on Γ_3). If m_3 is 4 we have a contradiction to [5] while if m_3 is 6 then $m = 17$, contradicting [20] 11.6 and 11.7. If $m_1 = 6$ then since m_2 is even $m_2 = 30$, a contradiction by Lemma 2.3 and [20] 18.2.

Thus $s = 2$ and (z_1, z_2) is $(1,5)$, $(2,4)$, or $(3,3)$. Consider the case $(1,5)$. By [4, 17], $m_2 = m_1(m_1 - 1)/k$ where $k \leqslant 3$. It follows from the minimality of m and [20] 17.7 that X_δ is imprimitive on Γ_2, and by Lemma 2.3 and [20] 18.2, $m_2 = 5m_1$; so $m_1 = 5k + 1$. Since m_1 is odd $k = 2$ and $m = 67$, a contradiction to [20] 11.6 and 11.7.

Next consider the case $z_1 = 2$, $z_2 = 4$. Suppose first that X_δ is primitive on Γ_1. Then by Lemma 2.5 and [20] 17.7, X_δ is 4-transitive on Γ_1 or $m_1 \leqslant 6$ and X_δ is 2-transitive on Γ_1, and X_δ is imprimitive on Γ_2. By [4], $m_2 = m_1(m_1 - 1)/k$ where k is 1 or 2. Suppose that $m_1 < m_2/4$ and that $\gamma \in \Gamma_1$. By Lemma 2.3, $X_\delta^{\Gamma_2}$ involves a 2-transitive representation of degree $m_2/2$ or $m_2/4$, and so by [8] Hilfsatz 1, all orbits of $X_{\delta\gamma}$ in Γ_2 have length a multiple of $m_2/4$. Now if $\Gamma(\gamma)$ is the orbit of X_γ of length m_1 then $X_{\delta\gamma}$ is transitive on $\Gamma_1 - \{\gamma\}$ and $\Gamma(\gamma) - \{\delta\}$ and it follows from [7] Corollary 3 that $\Gamma(\gamma) - \{\delta\} \subseteq \Gamma_2$. Hence $m_1 - 1 \geqslant m_2/4$, contradiction. Therefore $m_1 \geqslant m_2/4 = m_1(m_1 - 1)/4k$, where $k = 1$ or 2, and so (m_1, m_2) is $(8,28)$, $(6,15)$, $(4,12)$, $(4,6)$ or $(2,2)$. Now m_2 is divisible by 4, so m_1 is 4 or 8 and $X_\delta^{\Gamma_1}$ is alternating or symmetric. By [4], $k = 1$, so $m = 17$, a contradiction to [20] 11.6, 11.7. Hence X_δ is imprimitive on Γ_1. If $m_2 < \frac{1}{2}m_1$ and if $\gamma \in \Gamma_2$, then all orbits of $X_{\delta\gamma}$ in Γ_1 have length a multiple of $\frac{1}{2}m_1$ (by Lemma 2.3 and [8] Hilfsatz 1). If $\Gamma_2(\gamma)$ is the orbit of X_γ of length m_2, then if $m_2 < \frac{1}{2}m_1$ we must have $\Gamma_2(\gamma) - \{\delta\} \subseteq \Gamma_2$. Hence $\Gamma_2 \cup \{\delta\}$ is fixed setwise by $\langle X_\delta, X_\gamma \rangle = X$, contradiction. Thus $m_2 \geqslant \frac{1}{2}m_1$. If X_δ is primitive on Γ_2 then by Lemma 2.5 it is 2-transitive and hence by [4], $m_1 = m_2(m_2 - 1)/k \geqslant m_1(m_2 - 1)/2k$, that is $k \geqslant (m_2 - 1)/2$. By [4], m_2 is 3 or 5, a contradiction since m_2 is even. Hence X_δ is imprimitive on both Γ_1 and Γ_2 and $m_1 \leqslant 2m_2$. Suppose first that $X_\delta^{\Gamma_2}$ satisfies Lemma 2.3(i) or (ii). Then by [20] 18.2, $m_1 = 2x$, $m_2 = 4x$ for some odd $x \geqslant 3$, and $m = 1 + 6x$. Since m is not prime $x \geqslant 9$. As above we can show that A_x is not involved; hence $x = 2^r - 1 \geqslant 15$, and we show as above that $e = 3x - 2$ divides $(6x + 1)x^6 6^c$, for some $c \geqslant 0$, a contradiction. Thus $X_\delta^{\Gamma_2}$ satisfies Lemma 2.3(iii), and by the minimality of m either the representation of degree $y = \frac{1}{2}m_2$ is 5-transitive or $y \leqslant 6$. If $y \leqslant 6$ then by [20] 18.4, (m_1, m_2) is (6, 8) or (10, 12). The first case is impossible by [18] since S_6 on pairs has no subgroup fixing $e = 5$ pairs; in the other case it is also impossible since $m = 23$ is prime. Thus $y \geqslant 8$ and so by [20] 11.3, 12.1, $X_\delta^{\Gamma_2}$ has a composition factor S which is 4-transitive of degree y. If S is not a composition factor of $X_\delta^{\Gamma_1}$ then the kernel Y of X_δ on Γ_1 has two orbits of length y in Γ_2 (by [20] 13.1), and is 4-transitive on each. If $\gamma \in \Gamma_1$ and $\Gamma_1(\gamma)$, $\Gamma_2(\gamma)$ are the orbits of X_γ of length m_1, m_2 respectively, then $\mu = |\Gamma_2 \cap \Gamma_2(\gamma)|$ is 0, y, or $2y$. By [7] Corollary 3, $\mu = y$. Thus Y has 1 orbit of length y in $\Gamma_1(\gamma)$ and fixes the remaining points of $\Gamma_1(\gamma)$. Since the lengths of the orbits of $X_{\delta\gamma}$ in $\Gamma_1(\gamma)$ are either 1, 1, $\frac{1}{2}m_1 - 1$, $\frac{1}{2}m_1 - 1$, or 1, $\frac{1}{2}m_1 - 1$, $\frac{1}{2}m_1$, and since Y is normal in $X_{\delta\gamma}$ and y is even, it follows that y is $\frac{1}{2}m_1 - 1$. Then as Y is 4-transitive on this orbit of length y it follows that $X_\delta^{\Gamma_1}$, involves the alternating group of degree $\frac{1}{2}m_1 = y + 1$, a contradiction to [20] 18.2. Thus S is a composition factor of $X_\delta^{\Gamma_1}$ hence is either A_x where $x = \frac{1}{2}m_1$ is odd or $GL(r, 2)$ where $m_1 = 2(2^r - 1) \geqslant 14$. Since S is 4-transitive of even degree y we have a contradiction.

The final case is $s = 2$, $z_1 = z_2 = 3$. By Lemma 2.4, [20] 17.7, and since $m \geqslant 15$, X_δ is not primitive on both suborbits. We may therefore assume that X_δ is imprimitive on Γ_1. If X_δ is also imprimitive on Γ_2 then by Lemma 2.3, [20] 18.2 and 18.4, $m_1 = m_2$. If A_x, $x = m_1/3$ odd, is involved then by considering a 7-element as before, $x \leqslant 7$, but then m is prime. Hence $m_1/3 = 2^r - 1 \geqslant 7$. If r is 3 then m is prime; if r is 4 then $e = \frac{1}{2}(m - 5) = 43$ divides $|X|$, a contradiction to [23] 13.10. If $r \geqslant 5$ then arguing as before we can show that $e = 3x - 2$ divides $(6x + 1)x^6 6^c$ for some $c \geqslant 0$, a contradiction. Thus X_δ is primitive on Γ_2 and by Lemmas 2.4 and 2.5 is either 3-transitive, or m_2 is 9, 5 or 3 and X_δ is soluble, by [20] 18.3. In the latter case $m_1 = 9$, and so only the primes 2 and 3 divide $|X_\delta|$; thus m_2 is 3 or 9. Since $m \geqslant 15$, m_2 is 9 and then $m = 19$ is prime. Thus X_δ is 3-transitive on Γ_2 and $m_2 \geqslant 5$. If $m_2 < m_1/3$ and if $\gamma \in \Gamma_2$ then all orbits of $X_{\delta\gamma}$

in Γ_1 have length a multiple of $m_1/3 \geqslant m_2$ by [8] Hilfsatz 1; hence Γ_1 is also an orbit for X_γ, a contradiction as before. So $m_2 \geqslant m_1/3$ and both m_1 and m_2 are odd. By [4] it follows that $m_1 = 21$, $m_2 = 7$. In this case $X_\delta^{\Gamma_2} \geqslant A_7$ and we have a contradiction to [4]. This completes the proof of Lemma 2.6.

Thus the proof of Theorem 1 is complete.

3. Proof of Theorem 3 and its corollary

In this section we prove the following generalizations of Theorem 3 and its corollary for transitive groups.

THEOREM 3′. *Let G be a transitive permutation group on a set Ω of n points and let K be a nontrivial subgroup of G such that* $\mathrm{fix}_\Omega K$ *is nonempty. Assume that K satisfies*

(*) *If $g \in G$ is such that* $\mathrm{fix}_\Omega K \cap \mathrm{fix}_\Omega K^g \neq \varnothing$ *then K is conjugate to K^g in* $\langle K, K^g \rangle$.

Then $f = |\mathrm{fix}_\Omega K| \leqslant \frac{1}{2}n$, *and if* $f = \frac{1}{2}n$ *either*

(i) $\mathrm{fix}_\Omega K$ *is a block of imprimitivity for G, or*

(ii) *G has a set Σ of m blocks of imprimitivity in Ω such that G^Σ is A_m or S_m, or* $\mathrm{AGL}(d, 2)$ *in its natural representation where* $m = 2^d \geqslant 8$. *Moreover K fixes half the blocks pointwise and is transitive on the remaining blocks.*

COROLLARY TO THEOREM 3′. *Let G be a transitive permutation group on a set Ω of n points, let p be a prime dividing $|G|/n$, and let K be a Sylow p-subgroup of the stabilizer G_α of the point Ω. Then* $f = |\mathrm{fix}_\Omega K| \leqslant \frac{1}{2}n$ *if* $f = \frac{1}{2}n$ *then K is semiregular on Ω and either*

(i) $\mathrm{fix}_\Omega K$ *is a block of imprimitivity for G, or*

(ii) *G has a set Σ of $2p$ blocks of imprimitivity in Ω such that* $G^\Sigma \supseteq A_{2p}$.

PROOF OF THEOREM 3′. Let G, K be as in Theorem 3′. Suppose first that, for all g in G, $\mathrm{fix}_\Omega K \cap \mathrm{fix}_\Omega K^g$ is nonempty. Then by assumption K and K^g are conjugate in $\langle K, K^g \rangle$, that is K is pronormal in G. Thus by Theorem 1, $f < \frac{1}{2}n$. So suppose that K has a conjugate K^g such that $\mathrm{fix}_\Omega K$ and $\mathrm{fix}_\Omega K^g$ are disjoint. Then $n \geqslant |\mathrm{fix}_\Omega K \cup \mathrm{fix}_\Omega K^g| = 2f$ so that $f \leqslant \frac{1}{2}n$. If $f = \frac{1}{2}n$ then clearly $\mathrm{supp}_\Omega K^g = \mathrm{fix}_\Omega K$.

To complete the proof we must examine the case $f = \frac{1}{2}n$ more closely. Let $\alpha \in \mathrm{fix}_\Omega K$ and define $H = \langle K^g \mid K^g \leqslant G_\alpha, g \in G \rangle$. Let $\mathcal{C}$ denote the conjugacy class of K in G and if L is a subgroup of G let $\mathcal{C} \cap L$ denote the set of conjugates of K contained in L. Then $\mathcal{C} \cap G_\alpha$ is a generating set of H. Let $B = \mathrm{fix}_\Omega H$. Then clearly if $\beta \in B$, $\mathcal{C} \cap G_\alpha = \mathcal{C} \cap G_\beta$. Suppose that $g \in G$ is such that $B \cap B^g \neq \varnothing$,

https://doi.org/10.1017/S1446788700027348 Published online by Cambridge University Press

say $\beta^g = \gamma$ for some $\beta, \gamma \in B$. Then $(\mathcal{C} \cap G_\alpha)^g = (\mathcal{C} \cap G_\beta)^g = \mathcal{C} \cap G_\gamma = \mathcal{C} \cap G_\alpha$, that is g fixes setwise a set of generators of H. Thus $g \in N_G(H)$ and so $B^g = B$. We have therefore shown that B is a block of imprimitivity for G in Ω. Now B is a subset of $\operatorname{fix}_\Omega K$ and if $B = \operatorname{fix}_\Omega K$ then part (i) is true. So assume that B is a proper subset of $\operatorname{fix}_\Omega K$. Then there is a conjugate K^h of K such that $K^h \leqslant G_\alpha$ and $\operatorname{fix}_\Omega K \neq \operatorname{fix}_\Omega K^h$, that is $\operatorname{fix}_\Omega K^h$ contains points of both $\operatorname{fix}_\Omega K$ and $\operatorname{supp}_\Omega K$.

Let $\Sigma = \{B^g \mid g \in G\}$ and consider the action of G on Σ. The setwise stabilizer X of B in G is $N_G(H)$, for clearly $N_G(H) \subseteq X$, and if $x \in X$, say $\alpha^x = \beta \in B$, then $(\mathcal{C} \cap G_\alpha)^x = \mathcal{C} \cap G_\beta = \mathcal{C} \cap G_\alpha$ so that $x \in N_G(H)$. Let $K' \in \mathcal{C} \cap X$. If $\operatorname{fix}_\Omega K' \cap \operatorname{fix}_\Omega K \neq \varnothing$ then K' and K are conjugate in $\langle K', K \rangle \leqslant X$. If not then $\operatorname{fix}_\Omega K' = \operatorname{supp}_\Omega K$, and the subgroup K^h defined above is such that $\operatorname{fix}_\Omega K^h$ contains points of $\operatorname{fix}_\Omega K$ and $\operatorname{fix}_\Omega K'$. It follows that K' and K are conjugate in $\langle K', K^h, K \rangle \leqslant X$. Thus all conjugates of K contained in X are conjugate to K in X. By [20] 3.5, $N_G(K)$ is transitive on $\operatorname{fix}_\Sigma K$, and so K fixes pointwise all members of $\operatorname{fix}_\Sigma K$.

Let Δ be an orbit of X in $\Sigma - \{B\}$. Suppose that K acts trivially on Δ and let $C \in \Delta$. By our remark above $C \subseteq \operatorname{fix}_\Omega K$. Let $K' \in \mathcal{C} \cap G_\alpha \subseteq \mathcal{C} \cap X$. Then $K' = K^x$ for some $x \in X$ and so $(K')^\Delta = (K^x)^\Delta = (K^\Delta)^x = 1$. Thus $C \in \operatorname{fix}_\Sigma K'$ and so $C \subseteq \operatorname{fix}_\Omega K'$. Hence C is fixed pointwise by all members of a generating set for H, and so $C \subseteq \operatorname{fix}_\Omega H = B$, a contradiction. Thus $K^\Delta \neq 1$ and in particular $X^\Delta \neq 1$. So X^Δ is a transitive group with nontrivial pronormal subgroup K^Δ (by Lemma 1.4) and so by Theorem 1, $f_\Delta = |\operatorname{fix}_\Delta K| \leqslant \frac{1}{2}(|\Delta| - 1)$. Thus $\frac{1}{2}|\Sigma| = |\operatorname{fix}_\Omega K|/|B| = |\operatorname{fix}_\Sigma K| = 1 + \Sigma f_\Delta \leqslant 1 + \Sigma \frac{1}{2}(|\Delta| - 1) = \frac{1}{2}(|\Sigma| + 1 - r) \leqslant \frac{1}{2}|\Sigma|$, where r is the number of orbits of X in $\Sigma - \{B\}$. It follows from Theorem 1 that X is transitive on $\Sigma - \{B\}$ and $X^{\Sigma - \{B\}}$ is alternating or symmetric, or is $\mathrm{GL}(d, 2)$ for some $d \geqslant 3$. In the former case G^Σ is alternating or symmetric. In the case of $\mathrm{GL}(d, 2)$, K^Σ is a 2-group and by O'Nan's result [13] Theorem A, $G^\Sigma = \mathrm{AGL}(d, 2)$. This completes the proof of Theorem 3'.

Proof of Corollary to Theorem 3'. Let G be a transitive permutation group on Ω of degree n, let $\alpha \in \Omega$, let p be a prime dividing $|G_\alpha|$, and let K be a Sylow p-subgroup of G_α. It is easy to check that K satisfies condition $*$ of Theorem 3' and so $f = |\operatorname{fix}_\Omega K| \leqslant \frac{1}{2}n$. Suppose that $f = \frac{1}{2}n$. We showed in the proof of Theorem 3' that in this case K has a conjugate K' such that $\operatorname{fix}_\Omega K = \operatorname{supp}_\Omega K'$. Then $\langle K, K' \rangle = K \times K'$ is a p-subgroup of G containing K and for all $\beta \in \operatorname{fix}_\Omega K$, $K \times K'_\beta \leqslant G_\beta$. Since K is a Sylow p-subgroup of G_β we must have $K'_\beta = 1$. Thus K' and hence K are semiregular on the points they permute.

Finally we must consider the action of G on the set Σ of blocks of imprimitivity in case (ii) of Theorem 3'. Let H, B, Σ and X be as in the proof of Theorem 3'. Let Y be the pointwise stabilizer of B. Then $K \leqslant Y$ and $Y \trianglelefteq X$. Now $X^{\Sigma - \{B\}}$ is A_{m-1}

https://doi.org/10.1017/S1446788700027348 Published online by Cambridge University Press

or S_{m-1}, or GL$(d, 2)$ where $|\Sigma| = m$, and $|\Sigma| = 2^d \geqslant 8$ respectively. Since K acts nontrivially on Σ it follows that $Y^{\Sigma - \{B\}}$ contains A_{m-1} or GL$(d, 2)$ respectively. Since K is a Sylow p-subgroup of Y and fixes half the blocks of Σ, the groups GL$(d, 2)$ do not arise, and in the case of A_{m-1} and S_{m-1}, n must be $2p$. This completes the proof.

References

[1] M. Aschbacher, 'The nonexistance of rank three permutation groups of degree 3250 and subdegree 57', *J. Algebra* **19** (1971), 538–540.

[2] E. Bannai, 'Doubly transitive permutation representations of the finite projective special linear groups PSL(n, q)', *Osaka J. Math.* **8** (1971), 437–445.

[3] W. Burnside, *Theory of groups of finite order* (Cambridge University Press, London, 1911, reprinted Dover, New York, 1955).

[4] P. J. Cameron, 'Permutation groups with multiply transitive suborbits', *Proc. London Math. Soc.* (3) **25** (1972), 427–440.

[5] P. J. Cameron, 'Primitive groups with most suborbits doubly transitive', *Geometricae Dedicata* **1** (1973), 434–446.

[6] P. Dembowski, *Finite geometries* (Ergebnisse der Mathematik 44, Springer-Verlag, Berlin-Heidelberg-New York, 1968).

[7] D. G. Higman, 'Finite permutation groups of rank 3', *Math. Z.* **86** (1964), 145–156.

[8] N. Ito, 'Über die Gruppen PSL$_n(q)$, die eine Untergruppe von Primzahlindex enthalthen', *Acta Sci. Math.* (*Szeged*) **21** (1960), 206–217.

[9] W. M. Kantor, '2-Transitive designs', *Combinatorics, Part* 3, *Combinatorial group theory*, ed. by M. Hall, Jr. and J. H. van Lint (Math. Centre Tracts 57, Amsterdam, 1974, 44–97).

[10] E. Maillet, 'Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés', *J. Math. Pures Appl. Ser.* (5) **1** (1895), 5–34.

[11] M. O'Nan, "A characterisation of $L_n(q)$ as a permutation group,' *Math. Z.* **127** (1972), 301–314.

[12] M. O'Nan, "Normal structure of the one-point stabilizer of a doubly transitive permutation group II', *Trans. Amer. Math. Soc.* **214** (1975), 43–74.

[13] M. O'Nan, 'Estimation of Sylow subgroups in primitive permutation groups', *Math. Z.* **147** (1976), 101–111.

[14] C. E. Praeger, 'Doubly transitive permutation groups which are not doubly primitive', *J. Algebra* **44** (1977), 389–395.

[15] C. E. Praeger, 'Doubly transitive automorphism groups of block designs', *J. Combinatorial Theory Ser. A* **25** (1978), 258–266.

[16] C. E. Praeger, 'Sylow subgroups of transitive permutation groups,' *Math. Z.* **134** (1973), 179–180.

[17] C. E. Praeger, 'On primitive permutation groups with a doubly transitive suborbit', *J. London Math. Soc.* (2) **17** (1978), 67–73.

[18] C. C. Sims, 'Computational methods in the study of permutation groups', *Computational problems in abstract algebra* (Oxford, 1967), ed., by J. Leech (Pergamon Press, Oxford-London-Edinburgh, 1970, 169–184).

[19] M. J. Weiss, 'On simply transitive groups,' *Bull. Amer. Math. Soc.* **30** (1928), 333–359.

[20] H. Wielandt, *Finite permutation groups* (Academic Press, New York-London, 1964).
[21] W. J. Wong, 'Determination of a class of primitive permutation groups,' *Math. Z.* **99** (1967), 235–246.

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