J. Austral. Math. Soc. **21** (Series A) (1976), 428–437.

ON THE FIXED POINTS OF SYLOW SUBGROUPS OF TRANSITIVE PERMUTATION GROUPS

Dedicated to George Szekeres on his 65th birthday

MARCEL HERZOG and CHERYL E. PRAEGER

(Received 6 December 1974)

Communicated by Jennifer Seberry Wallis

Abstract

Let G be a transitive permutation group on a set Ω of n points, and let P be a Sylow p-subgroup of G for some prime p dividing $|G|$. If P has t long orbits and f fixed points in Ω, then it is shown that $f \leqq tp - i_p(n)$, where $i_p(n) = p - r_p(n)$, $r_p(n)$ denoting the residue of n modulo p. In addition, groups for which f attains the upper bound are classified.

Let G be a finite permutation group on a set Ω of n points which is transitive on Ω, and let P be a Sylow p-subgroup of G for some prime p dividing $|G|$. In Praeger (1973) the following question was asked: Can we bound the number of points of Ω fixed by P? It was shown there that the number of fixed points f is at most $\frac{1}{2}(n-1)$. This is the "best possible" bound in terms of the degree n, for the alternating group A_{2p-1} on $2p-1$ points has $f = p-1 = \frac{1}{2}(n-1)$.

In this paper we obtain upper bounds for f in terms of the number of long P-orbits, (that is, orbits containing at least two points), and the length of the longest P-orbit. Of course these new bounds must coincide with the previous bound for the group A_{2p-1}. In addition we classify those groups for which f attains the upper bounds.

Most notation is standard and the reader is referred to Wielandt's book (1964). If G acts on a set Σ with kernel K, then the constituent of G on Σ is denoted by $G^\Sigma \simeq G/K$; and we shall denote by $\mathrm{fix}_\Sigma\, G$, $\mathrm{supp}_\Sigma G$, the set of fixed points of G in Σ, and the set of points of Σ permuted nontrivially by G, (that is, the "support of G"), respectively. If the set Σ is clear from the context we shall often omit the subscript and write simply fix G, and supp G. For an integer n and a prime p, $i_p(n)$ will denote the integer satisfying $n + i_p(n) \equiv 0 \pmod p$, $1 \leqq i_p(n) \leqq p$. Also $r_p(n)$ will denote the residue of n mod p, that is, $i_p(n) + r_p(n) = p$.

https://doi.org/10.1017/S1446788700019261 Published online by Cambridge University Press

The alternating and symmetric groups of degree n are written as A_n and S_n as usual, and $\mathrm{PSL}(m+1,q)$, $\mathrm{ASL}(m,q)$ will denote respectively the projective and affine special linear groups of dimension m over a field of q elements.

We shall prove the following results:

THEOREM 1. *Let G be a transitive permutation group on a set Ω of n points, and let P be a Sylow p-subgroup of G for some prime p dividing $|G|$. If P has t long orbits and f fixed points in Ω, then*

$$f \leqq tp - i_p(n).$$

COROLLARY 2. (a) $f \leqq \frac{1}{2}(n - i_p(n)) \leqq \frac{1}{2}(n-1)$.

(b) *If the t long P-orbits have length $p^{\alpha_1}, \cdots, p^{\alpha_t}$, then* $f \leqq \frac{1}{2}(n - \Sigma(p^{\alpha_i} - p) - i_p(n)) \leqq \frac{1}{2}(n - p^{\alpha} + p - i_p(n))$ *where* $\alpha = \max_{1 \leqq i \leqq t}\{\alpha_i\}$.

COROLLARY 3. *If $f \geqq n/(p+1)$ then P has an orbit of length p.*

COROLLARY 4. *If G is d-transitive, where $d \geqq 2$, then either* (i) *P has order p, or* (ii) *$f \leqq \alpha_d n$ where α_d is* 3/8, 1/3, 1/4, *when d is at least* 2, 3, 4 *respectively, or* (iii) $G \supseteq A_n$.

(*Note that similar results may be proved if $d > 4$*).

THEOREM 5. *Let G be a transitive permutation group on a set Ω of n points, and let P be a Sylow p-subgroup of G for some prime p dividing $|G|$. Suppose that P has t long orbits and f fixed points in Ω, and suppose that $f = tp - i_p(n)$. Then*

(i) *if G is imprimitive then $t > 1$, $n = t(2p - y)$, where $ty = i_p(n) < p$, and P has t orbits of length p. Also G "involves" A_{2p-y} (see Remark 6(b)).*

(ii) *if G is primitive then $t = 1$, $f = r_p(n)$, and G is $(f+1)$-transitive. Further if the long P-orbit has length p then $G \supset A_n$ provided that $f \geqq 3$, or $p \leqq 3$.*

REMARKS 6. (a) By Corollary 2(a) we see that the bound obtained in Praeger (1973) can be deduced from Theorem 1.

(b) In Theorem 5, if G is imprimitive, then G has the following structure:

(i) G has a set of blocks of imprimitivity in Ω, $\Sigma_1 = \{B_1 = B, \cdots, B_r\}$ such that $1 \leqq |B| < p$.

(ii) G^{Σ_1} has a set of blocks of imprimitivity in Σ_1, $\Sigma_2 = \{C_1 = C, \cdots, C_s\}$, (where each C is a subset of Σ_1), such that $|\Sigma_2| = s \geqq 1$, $|C| = 2p - y$, and $s|B| = t \leqq ty = i_p(n) < p$.

(iii) P lies in the kernel K of the action of G on Σ_2. For each C in Σ_2, K acts on C as a primitive group of degree $2p - y$ containing a p-element of degree p. If p is 2 or 3 then $K^C \supseteq A_{2p-y}$ by Wielandt (1964) 13.3, while if $p \geqq 5$ then, (since $y \leqq \frac{1}{2}ty \leqq \frac{1}{2}p$), the p-element fixes at least 3 points and again $K^C \supseteq A_{2p-y}$, by Wielandt (1964) 13.9.

COROLLARY 7. *If* $f = \frac{1}{2}(n-1)$ *then* $f = p-1$, $t = 1$, $n = 2p-1$ *and* $G \supseteq A_n$.

1. Proof of Theorem 1 and the corollaries

Let G, P, f, t be as in the statement of Theorem 1. We first note some properties of the function i_p.

LEMMA 1.1. (a) *If* $n = ab$, *where* a *and* b *are positive integers, then* $i_p(n) \leqq a i_p(b)$, *and equality holds if and only if* $a i_p(b) \leqq p$.

(b) *If* $n = \Sigma a_j$, *for positive integers* a_j, $1 \leqq j \leqq r$, *then* $i_p(n) \leqq \Sigma i_p(a_j)$ *and equality holds if and only if* $\Sigma i_p(a_j) \leqq p$.

(c) $i_p(n-j) = i_p(n) + j$ *for any integer* j *satisfying* $0 \leqq j \leqq r_p(n)$.

PROOF. (a) Since $i_p(n) - a i_p(b) \equiv -n + ab \equiv 0 \pmod p$ and $i_p(n) - a i_p(b) \leqq p-1$, it follows that $i_p(n) \leqq a i_p(b)$, and the condition for equality is clear.

(b) Since $i_p(n) - \Sigma i_p(a_j) \equiv 0 \pmod p$, and $i_p(n) - \Sigma i_p(a_j) \leqq p-1$, the result (b) follows.

(c) Set $n = tp - i_p(n)$. Then $n - j = tp - (i_p(n) + j)$ where $1 \leqq i_p(n) \leqq i_p(n) + j \leqq i_p(n) + r_p(n) = p$. Hence by the definition of i_p, $i_p(n-j) = i_p(n) + j$.

Before proving the theorem we shall prove some results about Sylow subgroups of transitive imprimitive groups.

LEMMA 1.2. *Suppose that* G *is transitive and imprimitive on* Ω *and let* $\Sigma = \{B_1 = B, \cdots, B_r\}$ *be a set of blocks of imprimitivity for* G *in* Ω, *where* $|\Sigma| = r$, $|B| = b$. *Let* P *be a Sylow* p*-subgroup of* G *for a prime* p *dividing* $|G|$. *Let* Γ *be a long* P*-orbit of length* p^a *containing a point of a block* B *of* Σ, *and let* P_B *be the setwise stabiliser of* B *in* P. *Then*

(a) $\Gamma \cap B$ *is a block of imprimitivity for* P, P_B *is transitive on* $|\Gamma \cap B|$, *and* $|\Gamma| = |P : P_B| \, |\Gamma \cap B|$.

(b) *If the orbit of* P *in* Σ *corresponding to the orbit* Γ *in* Ω *has length* p^b *then* P *has an orbit of length at least* p^{a-b} *in any block of* Σ *fixed setwise by* P.

(c) P *acts "similarly" on each block of* Σ *which it fixes setwise, that is, if* B, C *are two blocks in* $fix_\Sigma P$, *then there is an element* g *in* $N(P)$ *such that* $B^g = C$ *and* g *induces a correspondence between* P*-orbits in* B and P-orbits in C.

(d) $|fix_\Omega P| = |fix_\Sigma P| \, |fix_B P|$, *where* B *is any block of* $fix_\Sigma P$.

PROOF. (a) Let $g \in P$ and suppose that $(\Gamma \cap B) \cap (\Gamma \cap B)^g$ contains a point α. Then $\alpha \in B \cap B^g$ and hence $B^g = B$. Also $\Gamma^g = \Gamma$ and so $(\Gamma \cap B)^g = \Gamma \cap B$ and $\Gamma \cap B$ is a block of imprimitivity for P in Γ. Clearly P_B is the setwise stabiliser of $\Gamma \cap B$ in P, and hence $|\Gamma| = |\Gamma \cap B| \, |P : P_B|$. If $\alpha \in \Gamma \cap B$ then P_α

https://doi.org/10.1017/S1446788700019261 Published online by Cambridge University Press

is a subgroup of P_B and $|\Gamma| = |P : P_\alpha| = |P : P_B|\,|P_B : P_\alpha|$. Hence the length of the P_B-orbit containing α is $|P_B : P_\alpha| = |\Gamma \cap B|$ and so P_B is transitive on $\Gamma \cap B$.

(b) Now $|P : P_B|$ is the length of the P-orbit in Σ corresponding to Γ. Hence $|P : P_B| = p^b$ and $|\Gamma \cap B| = p^{a-b}$. Assume that fix P is nonempty, (otherwise the result is vacuously true). Let $C \in \operatorname{fix}_\Sigma P$; then P is a Sylow p-subgroup of G_C, the setwise stabiliser of C. Let P' be a Sylow p-subgroup of G_B containing P_B, and let $g \in G$ be such that $B^g = C$. Then $P'^g \leqq G_C$ and we can choose h in G_C such that $P'^{gh} = P$. Then the P-orbit in C containing $(\Gamma \cap B)^{gh}$ has length at least p^{a-b}.

(c) If $B, C \in \operatorname{fix}_\Sigma P$ then P is a Sylow p-subgroup of both G_B and G_C. Choose g in G such that $B^g = C$ and then $P^g \leqq G_C$. Then choose h in G_C such that $P^{gh} = P$. Then $gh \in N(P)$ and $B^{gh} = C$.

(d) Clearly all the points in $\operatorname{fix}_\Omega P$ lie in $\cup\{B \mid B \in \operatorname{fix}_\Sigma P\}$, and by (c) each block in $\operatorname{fix}_\Sigma P$ fixes the same number, $|\operatorname{fix}_B P|$ (where $B \in \operatorname{fix}_\Sigma P$), of points. The result follows.

Proof of Theorem 1. Our proof is by induction on the degree n. The result is clearly true if n is 2 or 3, so assume that the result is true for transitive groups of degree less than n. The result is true if $f = 0$ so assume that $f > 0$.

Suppose first that G is imprimitive on Ω and let $\Sigma = \{B_1, \cdots, B_r\}$ be a set of blocks of imprimitivity for G, where $|B_i| = b$, $|\Sigma| = r$. Set $f_\Sigma = |\operatorname{fix}_\Sigma P|$, $f_B = |\operatorname{fix}_B P|$, for B in $\operatorname{fix}_\Sigma P$, and let t_Σ, t_B be the number of long P-orbits in Σ and B respectively. Suppose first that for B in $\operatorname{fix}_\Sigma P$, P acts nontrivially on B. Then by induction $f_B \leqq t_B P - i_p(b)$. Also the number of long P-orbits in blocks fixed by P is $f_\Sigma t_B \leqq t$, and we have by 1.1, that $f_\Sigma i_p(b) \geqq i_p(f_\Sigma b) = i_p(n)$ (since $n = rb \equiv f_\Sigma b \pmod p$). Thus $f = f_\Sigma f_B \leqq f_\Sigma(t_B p - i_p(b)) \leqq tp - i_p(n)$. If on the other hand P fixes pointwise each block in $\operatorname{fix}_\Sigma P$, then $f = bf_\Sigma$, and by 1.2(b) it follows that $t = bt_\Sigma$. Hence $f = bf_\Sigma \leqq b(t_\Sigma p - i_p(r)) = tp - bi_p(r) \leqq tp - i_p(n)$, (by induction and 1.1).

Hence we may assume that G is primitive. Let $\alpha \in \operatorname{fix} P$ and let $\Gamma_1, \cdots, \Gamma_r$ be the long G_α-orbits, $r \geqq 1$. Then by Wielandt (1964) 18.4, P acts nontrivially on each Γ_j. Let P have t_j long orbits and f_j fixed points in Γ_j, and let $|\Gamma_j| = n_j$, $1 \leqq j \leqq r$. Then by induction,

$$f = 1 + \Sigma f_j \leqq 1 + \Sigma(t_j p - i_p(n_j)) = 1 + tp - \Sigma i_p(n_j) \leqq tp + 1 - i_p(n-1) = tp - i_p(n)$$

(by 1.1). This completes the proof.

Proof of Corollary 2. It is sufficient to prove part (b). Since $n = \Sigma p^{\alpha i} + f$, it follows that $\frac{1}{2}(n - p^\alpha + p - i_p(n)) \geqq \frac{1}{2}(n - \Sigma(p^{\alpha i} - p) - i_p(n)) = \frac{1}{2}(f + tp - i_p(n)) \geqq f$.

https://doi.org/10.1017/S1446788700019261 Published online by Cambridge University Press

Proof of Corollary 3. Suppose that $f \geqq n/(p+1)$, and that all long P-orbits have length at least p^2. Then $tp^2 \leqq n - f \leqq pf \leqq p(tp - i_p(n)) < tp^2$, a contradiction.

Proof of Corollary 4. Assume that $f > \alpha_d n$, that G is not alternating or symmetric, and that P has order at least p^2. If $p = 2$, then $n \leqq f/\alpha_d \leqq 4f \leqq 4$, so $G \supseteq A_n$. Hence $p \geqq 3$, and therefore $\alpha_d \geqq 1/(p+1)$. So by Corollary 3, P has an orbit Δ of length p. Let Q be the pointwise stabiliser of Δ in P; then $|P:Q| = p$ so Q is nontrivial. Also let $|\text{fix } Q| = f + qp$; that is, Q fixes q orbits of P of length p. Let $M = N(P) \cap N(Q)$, and let $l = |N(P):M|$ be the number of conjugates of Q by elements of $N(P)$. Now distinct conjugates of Q fix disjoint sets of long P-orbits, so there are at least ql orbits of P of length p. By Praeger (1974), P has an orbit of length at least p^2. Hence if P has t long orbits then $3l \leqq qlp < tp \leqq n - f \leqq f(\alpha_d^{-1} - 1) \leqq 3f$, that is, $l < f$. Now by Wielandt (1964) 3.7, $N(P)$ is 2-transitive on fix P, and so (by Ito (1960) Hilfsatz 1) M is transitive on fix P. We shall show that $N(Q)$ is transitive on fix Q : let $\alpha \in \text{supp } P \cap \text{fix } Q$, and let P' be a Sylow p-subgroup of G_α containing Q. Then P', P are both Sylow p-subgroups of $N(Q)$ and so $P'^g = P$ for some g in $N(Q)$. Hence αg lies in fix P, and so the $N(Q)$-orbit containing fix P also contains α. Since α was chosen arbitrarily, $N(Q)$ is transitive on fix Q.

Thus by Theorem 1, $f \leqq qp - i_p(f) < qp$; and so $|\text{supp } Q| = n - qp - f \leqq n - 2f - i_p(f) < n(1 - 2\alpha_d) - 1$. By results of Bochert on minimal degree (Wielandt (1964) 15.1, or de Séguier (1912), 52–54) it follows that $G \supseteq A_n$, contradiction. This completes the proof.

2. Proof of Theorem 5

Let G, P, t, f be as before. The next two lemmas deal with the cases where t and f are as small as possible, that is, $t = 1$, and $f = r_p(n)$.

Lemma 2.1. *Suppose that G is transitive and P is a Sylow p-subgroup of G for a prime p dividing $|G|$. If P has only one long orbit then the number of points f fixed by P is $r_p(n)$ and G is $(f+1)$-transitive.*

Proof. The result is trivially true if P has no fixed points so assume that $f > 0$. Let Γ be the long P-orbit in Ω. We shall show that G is primitive. Let B be a block of imprimitivity for G containing a point α of Γ. If B also contains a point of fix P, then B is fixed setwise by P, and since P is transitive on Γ it follows that B contains Γ. However this means that P fixes each block in the set $\Sigma = \{B^g, | g \in G\}$ setwise and so by 1.2 (d) fixes the same number of points in each block in Σ. Since the unique long P-orbit Γ lies in B it follows that $B = \Omega$. If on the other hand B is a subset of Γ then B is a block of imprimitivity for the

https://doi.org/10.1017/S1446788700019261 Published online by Cambridge University Press

transitive group P^{Γ} and so $|B| = p^x$ for some $x \geqq 0$. Since $f \neq 0$, then n is not divisible by p, and since $|B|$ divides n it follows that $x = 0$ and $B = \{\alpha\}$. Hence the only blocks of imprimitivity for G are trivial and so G is primitive. Hence G is a Jordan group. From Kantor (to appear), either G is $(f+1)$-transitive (and hence $f = r_p(n)$), or G is an affine or projective linear group or a Mathieu group and it is easy to check that the Sylow p-subgroups of such groups have more than one long orbit, (if $f > 0$). This completes the proof.

LEMMA 2.2. *Let G be as in Theorem 5.*

(a) *If $f = r_p(n)$ then $t = 1$ and G is $(f+1)$-transitive.*

(b) *If G is d-transitive for some integer $d \geqq 1$, then either $f = r_p(n)$, or $d \leqq r_p(n)$.*

PROOF. (a) If $tp = f + i_p(n) = r_p(n) + i_p(n) = p$, then $t = 1$ and (a) follows from 2.1.

(b) If $d > r_p(n)$, and if H is the stabiliser in G of $r_p(n) + 1 \leqq d$ points of Ω, then p divides $|G : H|$ and it follows that $f = r_p(n)$.

Thus if either $t = 1$ or $f = r_p(n)$, then by Remark 6(c), and 2.1 and 2.2, the conclusions of Theorem 5 are valid, so assume that $t \geqq 2$, and $f > r_p(n)$. Our proof is by induction on the degree n. If n is 2 or 3, the theorem is true so we assume that the result is true for transitive groups of degree less than n. First we deal with the imprimitive case.

LEMMA 2.3. *If G satisfies the conditions of Theorem 5, and if G is imprimitive then the conclusions of the theorem hold.*

PROOF. Let $\Sigma = \{B_1 = B, \cdots, B_r\}$ be a set of nontrivial blocks of imprimitivity for G, where $|\Sigma| = r$ and $|B| = b$. Suppose first that for B in $\mathrm{fix}_\Sigma P$, P acts nontrivially on B. Let t_B, t_Σ, f_B, f_Σ be as in the proof of Theorem 1. Then by Theorem 1 and 1.2,

$$tp - i_p(n) = f = f_\Sigma f_B \leqq f_\Sigma(t_B p - i_p(b)).$$

Now $f_\Sigma t_B$ is the number of long P-orbits in the set of blocks in $\mathrm{fix}_\Sigma P$; hence $f_\Sigma t_B \leqq t$ and equality holds if and only if P acts trivially on Σ. Hence

$$tp - i_p(n) \leqq tp - f_\Sigma i_p(b) \leqq tp - i_p(f_\Sigma b) = tp - i_p(n)$$

by 1.1 and since $n \equiv f_\Sigma b \pmod p$. Thus it follows that $f_B = t_B p - i_p(b)$, $f_\Sigma i_p(b) = i_p(n)$, and that P acts trivially on Σ. Hence $f_\Sigma = r$ and $r i_p(b) = i_p(n)$. By induction $b = t_B(2p - y)$ where $t_B y = i_p(b)$. Thus $n = rb = r t_B(2p - y) = t(2p - y)$ where $ty = r(t_B y) = r i_p(b) = i_p(n)$. Also the structure of G follows from the induction hypothesis.

Hence we may assume that for B in $\mathrm{fix}_\Sigma P$, P acts trivially on B. Thus $f_B = b$ and $t_\Sigma = t/b$. Since P acts nontrivially on Σ, it follows from Theorem 1 that $f = f_B f_\Sigma \leqq b(t_\Sigma p - i_p(r)) = tp - bi_p(r) \leqq tp - i_p(n)$. Hence $f_\Sigma = t_\Sigma p - i_p(r)$ and $bi_p(r) = i_p(n)$. The rest then follows by induction as in the previous case.

Thus we assume that G is primitive, and that $t \geqq 2$ and $f > r_p(n)$. By the results of the next two lemmas it will follow that G is $(r_p(n)+1)$-transitive, which contradicts 2.2(b), thus completing the proof of Theorem 5.

LEMMA 2.4. *Suppose that G satisfies the conditions of Theorem 5. If G is d-primitive, for some $1 \leqq d \leqq r_p(n)$ then G is $(d+1)$-transitive.*

PROOF. If $d > 1$ let H be the stabiliser in G of $d-1$ points of fix P, $\alpha_1, \cdots, \alpha_{d-1}$, and let $\Delta = \Omega - \{\alpha_1, \cdots, \alpha_{d-1}\}$. If $d = 1$ let $H = G$ and $\Delta = \Omega$. Then H is primitive on Δ. Assume that H is not 2-transitive and let $\Gamma_1, \cdots, \Gamma_r$ be the long H_α-orbits where $\alpha \in \mathrm{fix}_\Delta P$ (since $f > r_p(n) \geqq d$, $\mathrm{fix}_\Delta P$ is non-empty), and $r \geqq 2$. By Wielandt (1964) 18.4, P acts nontrivially on each Γ_i. Let $|\Gamma_i| = n_i$ and let P have t_i long orbits and f_i fixed points in Γ_i for $1 \leqq i \leqq r$. Then by Theorem 1, $tp - i_p(n) = f = d + \Sigma f_i \leqq d + \Sigma(t_i p - i_p(n_i)) = tp + d - \Sigma i_p(n_i) \leqq tp - i_p(n)$ by 1.1. Hence for all i, $f_i = t_i p - i_p(n_i)$, and $\Sigma i_p(n_i) = i_p(n) + d$.

By induction $n_i = t_i(2p - y_i)$ where $t_i y_i = i_p(n_i)$. Thus $|\mathrm{supp}\, P| = \Sigma(t_i p) \leqq (\Sigma t_i y_i)p = (i_p(n) - d)p \leqq p^2$. Thus H contains a p-element of degree qp, $q \leqq t \leqq p$, and it follows from a result of Manning (1911), that

$$n - d + 1 = |\mathrm{supp}\, H| \leqq \max\{qp + q^2 - q, 2q^2 - p^2\}.$$

Since $2q^2 - p^2 \leqq q^2 < qp + q^2 - q$, we have

$$n - d + 1 = 1 + \Sigma t_i(2p - y_i) \leqq qp + q^2 - q \leqq tp + t^2 - t.$$

Now $\Sigma t_i(2p - y_i) \geqq 2tp - p$ and so $(p - t)(t - 1) \leqq -1$, a contradiction. Thus G is $(d+1)$-transitive.

LEMMA 2.5. *Suppose that G satisfies the conditions of Theorem 5 and that $f > r_p(n)$. If G is d-transitive for some $2 \leqq d \leqq r_p(n)$, then G is d-primitive.*

PROOF. Since $f > r_p(n)$, then by 2.2(b) $p > d \geqq 2$, and in particular $p \geqq 3$. Let H be the stabiliser in G of $d-1$ points of fix P, $\alpha_1, \cdots, \alpha_{d-1}$, and let $\Delta = \Omega - \{\alpha_1, \cdots, \alpha_{d-1}\}$. Suppose that H is imprimitive on Δ. Now $|\mathrm{fix}_\Delta P| = f - d + 1 = tp - i_p(n) - d + 1 = tp - i_p(n - d + 1)$ by 1.1, and so by induction, $n - d + 1 = t(2p - y)$ where $ty = i_p(n - d + 1)$ and $|\mathrm{supp}\, P| = tp$. Since H is imprimitive, $t \geqq 2$. Now if $t \leqq \frac{1}{2}(p-1)$ it follows from Wielandt (1964) 13.10 that $f = t(p - y) + d - 1 \leqq 4t - 4$, that is, $d + 3 + t(p - y - 4) \leqq 0$. Hence $p - 3 \leqq y = i_p(n - d + 1)/t \leqq (p-1)/t$, that is, $p \leqq 3 + 2/(t-1) \leqq 5$. Since also $2 \leqq t \leqq \frac{1}{2}(p-1)$ it follows that $t = 2$ and $p = 5$, a contradiction to Wielandt (1964) 13.10. Hence

$t \geqq \frac{1}{2}(p+1)$ and as $ty \leqq p$, also $y = 1$ and so H "involves" A_{2p-1} (see Remark 6(b)).

By Remark 6(b), H has a set of blocks in Δ, $\Sigma_1 = \{B_1 = B, \cdots, B_r\}$ such that $1 \leqq |B| < p$. Also H^{Σ_1} has a set of blocks $\Sigma_2 = \{C_1, \cdots, C_s\}$, (where each C is a subset of Σ_1), where $|C_i| = 2p-1$, $s|B| = t = i_p(n-d+1) < p$. Then P lies in the kernel K of the action of H on Σ_2, and for each C in Σ_2, $K^C \supseteq A_{2p-1}$. Since all long P-orbits have length p it follows from Praeger (1974) that P has order p, and hence K^{Σ_1} is isomorphic to A_{2p-1} or S_{2p-1}.

If $t \leqq 7$ then since $t \leqq i_p(n-d+1) \leqq p-1$, we have a contradiction (by Wielandt (1964) 13.10, Manning (1909), and Weiss (1928)). Thus we assume that $t \geqq 8$ and $p \geqq 11$. Next suppose that $b = |B| < \frac{1}{4}(p+1)$. Then by "Bertrand's Postulate" (Hall (1960), 68) there is a prime q satisfying $\frac{1}{4}(p+1) < q \leqq \frac{1}{2}(p+1) - 2 = \frac{1}{2}(p-3)$, if $\frac{1}{2}(p+1) \geqq 7$, that is if $p \geqq 13$. Then K contains an element g of order q which permutes exactly q blocks of Σ_1 in each block C of Σ_2. Then since $b < q$, g permutes exactly $(sb)q = tq$ points and fixes $d - 1 + t(2p-1-q) \geqq d - 1 + t(3q+5) > 3qt + 5$ points. This is a contradiction to Bochert's result on minimal degree (de Séguier (1964), 52–54). Hence if $p \geqq 13$ then $b \geqq \frac{1}{4}(p+1)$, and also if $p = 11$ then $b \geqq \frac{1}{4}(p+1)$, (unless $b \leqq 2$, but then there is an element of order 3 in K permuting $3t$ points and leaving $d - 1 + 18t$ points fixed, again a contradiction). Since $sb = t \leqq p-1$ it follows that $s \leqq 3$.

Now let q be any prime satisfying

$$q > s, \qquad 2q < 2p - 1\,. \tag{1}$$

Suppose, for all q-elements g in H, that if g fixes a block B of Σ_1 setwise, then g fixes B pointwise. Let g be an element of order q in K which permutes exactly q blocks of Σ_1 in each block of Σ_2. Then $|\operatorname{supp} g| = tq$. Since $2q < 2p-1$, there is a conjugate g' of g in K which permutes a set of blocks of Σ_1 which is disjoint from $\operatorname{supp}_{\Sigma_1} g$, and hence $\operatorname{supp}_\Omega g' \cap \operatorname{supp}_\Omega g$ is empty. On the other hand if g' is a conjugate of g such that $\operatorname{supp}_\Omega g' \cap \operatorname{supp}_\Omega g$ is nonempty, then clearly $\langle g', g\rangle$ fixes at least $d-1$ points of Ω, so we may assume that g' lies in H. Since $q > s$, then g' lies in K. If γ lies in $\operatorname{supp} g' \cap \operatorname{supp} g$ then the block B of Σ_1 containing γ is permuted nontrivially by both g and g', by our assumption about q-elements in H. If C is the block of Σ_2 containing B, then $\langle g', g\rangle$ permutes less than $2q$ blocks of Σ_1 in C. Hence $|\langle g', g\rangle^C|$ is not divisible by q^2, and since $K^C \simeq K^{\Sigma_1}$ it follows that $|\langle g', g\rangle^{\Sigma_1}|$ is not divisible by q^2. Finally our assumption about q-element implies that the kernel of K on Σ_1 is a q'-group, and so $|\langle g', g\rangle|$ is not divisible by q^2. Hence $\langle g'\rangle$ is conjugate to $\langle g\rangle$ in $\langle g', g\rangle$. Thus by a result of O'Nan, (Praeger (to appear) 1.5), G is $\mathrm{AGL}(m,2)$ for some m (since $G \not\supseteq A_n$), and so G is 3-transitive. Hence $d = 3 < p$. Now the stabiliser of a point α in fix P,

$G_\alpha = \mathrm{GL}(m,2) = \mathrm{PSL}(m,2)$ is 2-transitive on $n-1 = 2^m - 1$ points. Since $p > 3$ it is easy to show that fix $P - \{\alpha\}$ is a subspace of the projective space and hence $f = tp - i_p(n) = 1 + (2^a - 1) = 2^a$ for some $1 \leqq a < m$. Then $i_p(n) = n - 2f = 2^m - 2^{a+1} \leqq p$ and so $2^a = f \geqq (t-1)p \geqq (t-1)(2^m - 2^{a+1})$, that is $(t-1)(2^{m-a} - 2) \leqq 1$. It follows that $a = m-1$ and so $i_p(n) = 0$, a contradiction.

Thus if q is a prime satisfying (1) then there is a q-element in H which fixes a block B of Σ_1 setwise and permutes B nontrivially. Hence in particular, $q \leqq |B|$.

Now by Bertrand's Postulate there is a prime q satisfying $\frac{1}{2}p < q \leqq p-2$ and as $s \leqq 3$ clearly q satisfies (1). Hence $\frac{1}{2}p < q \leqq |B| = b$, and since $t = bs < p$ it follows that $s = 1$ and $b = t$. Again by Bertrand's Postulate, since $b \geqq 8$, there is a prime q satisfying $\frac{1}{2}(b-1) < q \leqq b-3$. Then (1) holds and so there is a q-element g permuting points of a block B in Σ_1. If $2q > b$ then g permutes exactly q points, so by 2.1 the action on B is multiply transitive, and by Wielandt (1964) 13.10 it is alternating or symmetric. If $2q \leqq b$ then we must have $b = 2q$; and then there is a prime q' such that $\frac{1}{2}b < q' \leqq b-2$. Since b is even $q' \leqq b-3$ and since (1) holds, there is a q'-element permuting points of a block B in Σ_1. Again it follows that the action on B is alternating or symmetric.

Now since $s = 1$ we have $H = K$ and if L is the setwise stabiliser of B in Σ_1, then $L^B \supseteq A_b$ and $L^{\Sigma_1 - B} \supseteq A_{2p-2}$. Let M be the kernel of the action of H on Σ_1; then $L/M \supseteq A_{2p-2}$ and so M has A_b as a factor, that is, for each B in Σ_1, $M^B \supseteq A_b$. Since M is 2-transitive on each of its orbits if follows from a result of O'Nan (to appear) (Theorem D) that $G_{\alpha_1 \cdots \alpha_{d-1}}$ is a normal extension of $\mathrm{PSL}(m,q)$ for some $m \geqq 3$ and prime power q, and that $\alpha \cup B$ is some subspace of the projective geometry. Thus $1 + (2p-1)b = (q^m - 1)/(q-1)$ and $1 + b = |\alpha \cup B| = (q^t - 1)/(q-1)$ for some $1 < t < m$. It follows that $q \leqq b < p$, and then it is easy to show that fix $P - \{\alpha_1, \cdots, \alpha_{d-1}\}$ is a subspace. Hence

$$f - d + 1 = 1 + (p-1)b = (q^s - 1)/(q-1)$$

for some $s > t$, and therefore $pb = q^{m-1} + \cdots + q^s$. However this means that b is divisible by q^s whereas $1 + b = (q^t - 1)/(q-1) < q^t < q^s$, a contradiction. This completes the proof of the lemma.

By our remarks preceding Lemma 2.4, the proof of Theorem 5 is complete.

Proof of Corollary 7. We assume that $f = \frac{1}{2}(n-1)$. Then the number of points permuted by P is $n - f = f + 1 \leqq tp$, by Theorem 1. It follows that all long P-orbits have length p and that $f = tp - 1$. If G is imprimitive then by Theorem 5, $n = t(2p - y)$ where $ty = i_p(n) = 1$, a contradiction to $t > 1$. Hence by Theorem 5, $t = 1$, $f = p - 1$, and $n = 2p - 1$. Since either $f \geqq 3$ or $p \leqq 3$ it follows that $G \supseteq A_n$.

https://doi.org/10.1017/S1446788700019261 Published online by Cambridge University Press

References

M. Hall, Jr. (1960), *The Theory of Groups*, (New York: Pergamon 1960).

N. Ito (1960), 'Über die Gruppen $PSL_n(q)$ die eine Untergruppe von Primzahlindex enthalten', *Acta Sci. Math.* **21**, 206–217.

W. M. Kantor 'Primitive groups having transitive subgroups of smaller, prime power degree', (to appear).

W. A. Manning (1909), 'On the order of primitive groups', *Trans. Amer. Math. Soc.* **10**, 247–258.

W. A. Manning (1911), 'On the limit of the degree of primitive groups', *Trans. Amer. Math. Soc.* **12**, 375–386.

M. E. O'Nan, 'Normal structure of the one-point stabiliser of a doubly transitive permutation group, II', (to appear).

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

C. E. Praeger (1974), 'On the Sylow subgroups of a doubly transitive permutation group', *Math. Z.* **137**, 155–171.

C. E. Praeger, 'Primitive permutation groups containing a p-element of small degree, p a prime', (to appear), *J. Algebra*.

J. A. de Séguier (1912), *Théorie des Groupes finis*, (Paris: Gauthier-Villars).

M. J. Weiss (1928), 'Primitive groups which contain substitutions of prime order p and of degree $6p$ or $7p$', *Trans. Amer. Math. Soc.* **30**, 333–359.

H. Wielandt (1964), *Finite Permutation Groups* (New Yorl-London: Academic Press 1964).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, Australia 2600.