数理解析研究所講究録
第 325 巻 1978 年 161-181

Permutation groups of some special degrees

A preliminary report on some joint work with P.M. Neumann

by Jan Saxl

In an impressive series of papers some fifteen years ago Noboru Ito considered transitive permutation groups of degree $p = 2q+1$, where p and q are prime numbers and $p > 11$, and proved that such groups are either soluble (and therefore well known) or very nearly 4-transitive. In this paper we want to use this remarkable result and a theorem of R. Brauer to obtain an extension to groups of degree kp with $k > 1$.

Throughout G will be a primitive permutation group on a set Ω, where $|\Omega| = n = kp = k(2q+1)$ with p and q prime numbers, $p > 11$ and $k > 1$. Let P be a Sylow p-subgroup of G. Our first result brings q into play.

Proposition 1. If $k < 10$ and $k \neq 8$ then either q divides the order of $N(P)$ or $PSL(2,n-1) \leqslant G \leqslant P\Gamma L(2,n-1)$.

Once we know that q does divide the order of G we can start the work on the proof of our main result.

Theorem. If $k = 2$ then G is 7-transitive.

If $k = 3$ then G is 10-transitive.

If $k = 4$ then either G is A_n, S_n or $PSL(2,n-1) \leqslant G \leqslant P\Gamma L(2,n-1)$.

Let $\Gamma_1,\ldots,\Gamma_k$ be the P-orbits on Ω, and let H be the setwise stabilizer of each of these. The main step in the proof is to show that if $k \leqslant 4$ then H is insoluble. Then we know by Ito's theorem that H is 3-transitive (and in fact nearly 4-transitive) on each of the Γ_i, which enables us to obtain very high transitivity of G on Ω. It should be possible to deduce then that

G is alternating or symmetric, however we have not been able to do this yet when k is 2 or 3. The case k = 4 is easier since we can find a non-trivial element in G fixing a large number of points in Ω so that an old theorem of W.A. Manning can be applied.

We obtain the following corollaries:

Corollary 1. If G is a primitive group of degree $n = 2p = 4q+2 = r+3$ where r is also a prime number then G is A_n or S_n. Similarly for

$n = 2p = 4q+2 = 5r+3$ (eg. n = 118),

$n = 2p = 4q+2 = r+5$ (eg, n = 94),

$n = 3p = 6q+3 = r+4$ (eg. n = 141),

etc., etc.

Corollary 2. If G is 2-transitive of degree $3p+1$ with $p = 2q+1$ then G is alternating or symmetric.

Here the group is 2-primitive by a result of M.D. Atkinson [1, Cor.C], so G is 11-transitive by the theorem. An argument similar to that in the last section in the case $n = 4p$ then shows that G contains the alternating group.

Corollary 3. If any insoluble group of degree $p = 2q+1$ contains the alternating group then this is also true of any primitive group of degree 2p and 3p. This holds for instance if $q = 2r+1$ with r prime [15] or if $p \leq 4079$ [16].

It should be noted that some of the results in this paper have been also previously obtained by Izumi Miyamoto in [13]. In particular, the case k = 2 of the assertion in Section 2 as well as the case k = 2 of Corollary 3 are due to him.

1. Some preliminaries and proof of Proposition 1

We shall assume throughout that $k < 10$. Then we can clearly suppose that P is cyclic of order p and semi-regular on Ω. Whenever convenient, we shall assume that G is a simple group; this is justified by the following

Lemma. If X is a minimal normal subgroup of G then X is simple and primitive on Ω.

Proof. Since p divides the order of X but p^2 does not, the simplicity of X is clear. Suppose that X is imprimitive. Let B be a block of maximal size, say $|B| = m$, and let Σ be the corresponding system of imprimitivity. If $p \mid m$ then P lies in the kernel of X on Σ; but X is simple, so X must act trivially on Σ, which is impossible. Thus m divides k and $|\Sigma| = \frac{k}{m}p$.

Now G is primitive on Ω, so for some g in G we have $Bg \notin \Sigma$. Then Σg is another system of imprimitivity for X. Now X acts on Σ and Σg, and by induction (cf. the Theorem) together with a theorem of Ito [9, Satz 3], the actions of X on Σ and Σg are at least 2-transitive and are similar to each other. Therefore X_B stabilizes some block in Σg, and so has an orbit on $\Omega - B$ of size at most m. On the other hand, X_B is transitive on $\Sigma - \{B\}$, so all its orbits on $\Omega - B$ have size at least $p-1$. This is a contradiction.

Proof of Proposition 1. Suppose that q does not divide $|N(P)|$. Since P is cyclic of order p and since $p = 2q+1$, it follows that $|N(P)/C(P)|$ divides 2, and in fact is equal to 2, as we see from the Burnside transfer theorem. It now follows by a theorem of Brauer [4, Theorem 9.C] that every involution in G is conjugate to one in $N(P) - C(P)$. Therefore, if an involution of G fixes u points then $u \leq k$. Moreover, since $p \equiv 3 \pmod 4$ and $G \leq A_n$, we have $n \equiv -k \pmod 4$. Hence for k equal to $2, 3, 4, 5, 6, 7, 8, 9$,

the maximum possible value for u is $2, 1, 4, 3, 6, 5, 8, 7$.

If $k \leq 5$ then we can use the theorems of Buekenhout and Rowlinson [5] and deduce that G is PSL(2,n-1). If $|C(P)|$ is even then an involution in C(P) must be fixed-point-free on Ω, since if it fixed a point then it would fix pointwise the whole P-orbit containing that point. Hence such an involution is an odd permutation unless k is divisible by 4. Thus for $k \not\equiv 0 \pmod 4$ the order of C(P) is odd, so that there is only one conjugacy class of involutions in G, and another theorem of Rowlinson [17] applies.

This implies that $k = 8$ and the proposition is proved. It is perhaps worth observing that since a Sylow 2-subgroup S of G is semi-regular on the set of ordered (k+1)-subsets of Ω, the order of S divides $kp(kp-1)\cdots(kp-k)$. When $k = 2$ this implies that $|S|$ divides 8, while for $k = 8$ the Sylow 2-subgroups of G have order at most 2^{11}.

Some more notation. Let Q be a Sylow q-subgroup of N(P); then $Q \leq H$, where H is the setwise stabilizer of all the P-orbits Γ_i. We shall assume that Q is in fact a Sylow q-subgroup of G, because otherwise G is known to satisfy the conclusion of the theorem. Let Δ_0 be the set of fixed points of Q. We shall denote the k points of Δ_0 by $\alpha, \beta, ..$ Let Θ be the set of all Q-orbits, and let $\Theta_0 = \Theta - \Delta_0$. Let $\Theta_0 = \{\Delta_1, \ldots, \Delta_{2k}\}$, where $\Gamma_1 = \{\alpha\} \cup \Delta_1 \cup \Delta_2$, $\Gamma_2 = \{\beta\} \cup \Delta_3 \cup \Delta_4$, etc. Finally, let K, L be the kernel of the action of N(Q) on Δ_0, Θ_0, respectively.

2. The insolubility of H

Assume, to obtain a contradiction, that H is soluble. Then $H \leq N(P)$, and since it fixes every P-orbit, H is metacyclic of order pq or 2pq. Let $X = N(Q)/Q$ and $Y = C(Q)/Q$. Then X/Y is a cyclic group, which is non-trivial by the Burnside transfer theorem. Note also that 3 does not divide the order of X/Y, since $q \equiv 2 \pmod 3$.

Let $g \in N(Q)$ and assume that g is trivial on Θ. Then $g \in H$, so that $g \in N(P)$, and since g fixes all the Δ_i, we have $g \in Q$. Thus X is faithful in its action on Θ, so that $X \leq S_k \times S_{2k}$. It is this observation which is the key to our proof of the insolubility of H - it restricts the structure of X to only very few possibilities. We should also remark that in fact $X \leq A_{3k}$, since $G \leq A_n$.

The case k = 2. Here $X \leq (Z_2 \times S_4) \cap A_6$, and so X/Y is a non-trivial cyclic 2-group.

If $|X/Y| = 2$ then by [4, Theorem 9.C] all involutions of G are conjugate to involutions in $N(Q) - C(Q)$. Hence all involutions of G fix precisely two points of Ω. But G is 2-transitive on Ω by a theorem of Wielandt [20, 31.1], so that this contradicts a theorem of Hering [8]. It is perhaps worth mentioning that since 2p is 6 modulo 8 we can also deduce that 8 is the highest possible power of 2 dividing $|G|$ and obtain a contradiction this way.

Hence X/Y is a cyclic 2-factor of $(Z_2 \times S_4) \cap A_6$ of order at least 4. The normalizer of a Sylow 3-subgroup of $Z_2 \times S_4$ is $Z_2 \times S_3$, so by the Frattini argument we see that $3 \nmid |X|$. The Sylow 2-subgroup of A_6 is D_8, which does not have Z_4 as a factor. Thus $C(Q) = Q$ and $N(Q) = Q \cdot Z_4$. But then the normalizer of Q in G_α has order 2q. If all the involutions of G_α are conjugate then they fix precisely 2 points of Ω and we obtain a contradiction as before. Hence by [4, Theorem 9C] we have $O_{q'}(G_\alpha) \neq 1$. Since Q is self-centralizing, a q-element of G acts as a fixed-point-free automorphism on $O_{q'}(G_\alpha)$. Therefore $O_{q'}(G_\alpha)$ is nilpotent by a theorem of J.G. Thompson [18]. On the other hand, G_α is transitive and hence primitive of degree $4q+1$. It follows that $4q+1$ is a power of a prime. Now 3 divides $4q+1$, so $4q+1$ is an even power of 3, say $4q+1 = 3^{2s}$. Then $4q = (3^s-1)(3^s+1)$, which is impossible. Hence if $k = 2$ then H is insoluble.

The case $k = 3$. Here $X \leq (S_3 \times S_6) \cap A_9$. If g is in the kernel L of X on Θ_0 then either g is a 2-element and therefore is not in A_9, or g is a 3-element and so lies in $Y \cap L$. But $Y \cap L = 1$, so that $L = 1$ and $X \leq S_6$.

Now X is transitive on Δ_0 by the Jordan lemma, so X^{Δ_0} is a factor of X isomorphic to Z_3 or S_3. The normalizer in S_6 of a Sylow 5-subgroup has order prime to 3, so by the Frattini argument 5 does not divide the order of X. Hence X is a $\{2,3\}$-subgroup of S_6, and X/Y is a cyclic 2-group.

Let T be a Sylow 3-subgroup of Y. Then $T \neq 1$, since we have already noticed that 3 divides $|X|$ but does not divide $|X/Y|$. Hence $|T|$ is 3 or 9. If $|T|$ is 9 let T' be a Sylow 3-subgroup of the kernel K of X on Δ_0, otherwise let $T' = T$. Then the normalizer of T' inside S_6 is either $S_3 \times S_3$ or $(Z_3 \text{ wr } Z_2)\cdot Z_2$, neither of which has a subgroup with a 2-factor of order greater than 2. Hence $|X/Y| = 2$ by the Frattini argument. Then, using the theorem of Brauer [4] again, all involutions in G are conjugate to those in $N(Q) - C(Q)$, whence they fix at most five points of Ω.

If now $|C(Q)|$ is odd then G has only one class of involutions and we obtain a contradiction from [17]. Assume then that $|C(Q)|$ is even. If an involution in $C(Q)$ fixed a Δ_i setwise then it would fix it pointwise, which is not possible since $q > 5$. Hence the involutions of Y are semi-regular on Θ_0. It follows that $|Y|$ is twice an odd number, and so $|X|$ is 12 or 36.

Since the order of the normalizer of T in X is even by the Frattini argument, we have $T \triangleleft X$, and so also $T' = T \cap K \triangleleft X$. Note also that the semi-regularity of the involutions of Y on Θ_0 now implies that X is transitive on Θ_0. Thus X has index 1 or 3 in $(Z_3 \text{ wr } Z_2)\cdot Z_2$. Let t be an involution in K. Since t is even on Θ, it cannot be semi-regular on Θ_0. This forces K to be of order 6 with two orbits of size 3 on Θ_0, and therefore $K = S_3$ and $X = (Z_3 \text{ wr } Z_2)\cdot Z_2$. But now an inspection of $(Z_3 \times Z_2)\cdot Z_2$ shows that K cannot be a normal subgroup of X, a contradiction.

The case $k = 4$. First we shall show that, quite independently of the assumption on H, there is a subdegree of G which is 3 modulo q. Suppose that there is a G_α-orbit of size aq+1. Assume first that $a \geqslant 3$. Using the theorem of Weiss [19] extensively we see that the only possibilities are

7q+1, q+2,

6q+1, 2q+2,

6q+1, q+1, q+1,

5q+1, 3q+2,

4q+1, 3q, q+2,

and 3q+1, 2q, 2q, q+2.

We shall consider just the third case - all the other cases can be ruled out in the same way. Let Γ be the G_α-orbit of size 6q+1, and let Δ be one of the G_α-orbits of length q+1. Let $\delta \in \Delta$. Since the greatest common divisor of q+1 and 6q+1 divides 5, the $G_{\alpha\delta}$-orbits on Γ have size a multiple of (6q+1)/5. On the other hand q divides $|G_{\alpha\delta}|$. This implies that $G_{\alpha\delta}$ is transitive on Γ, which contradicts the primitivity of G (cf. the second part of the proof of Theorem 1 in [19]). This contradiction shows that $a \leq 2$, and in fact a = 1, because 2q+1 = p. Let us consider then the case where Γ is a G_α-orbit of length q+1. Then G_α^Γ is 2-transitive, so by [6] there is a G_α-orbit Σ of size cq with $3 \leq c \leq 6$. It also follows from [6] that G_α^Γ is not 3-transitive; hence $G_\alpha^\Gamma = PSL(2,q)$. But then the action of G_α^Γ on Σ implies that $q = 11$; this possibility is easily excluded by an ad hoc argument.

Hence we have shown that no non-trivial subdegree of G is 1 modulo q. This implies that one of the subdegrees is 3 modulo q, whence N(Q) is 2-transitive on Δ_0 by Witt's lemma. Hence $C(Q)^{\Delta_0} \geq A_4$, since $3 \nmid |N(Q)/C(Q)|$.

Let us return now to the proof of the insolubility of H in the case k = 4. Assume that the kernel L of X on Θ_0 is non-trivial. Then L is transitive on Δ_0. But $L \cap Y = 1$, so L is cyclic and therefore contains an odd permutation. Hence L = 1 and $X \leq S_8$. Moreover, we see as before that 5 and 7 do not divide the order of X by the Frattini argument. So X is a $\{2,3\}$-subgroup of S_8, and X/Y is a cyclic 2-group. Let T be a Sylow 3-subgroup of Y; then $|T| \leq 9$.

Assume first that $|T| = 9$. Then $T' = K \cap T$ has order 3. If $|X/Y| \geq 4$ then the Frattini argument shows that $N_{S_8}(T')$ has a 2-factor of order at least 4. But the normalizer of a group of order 3 in S_8 is either $S_3 \times S_5$ or $Z_2 \times (Z_3 \text{ wr } Z_2)\cdot Z_2$, so that $|X/Y| = 4$ and $N_X(T')$ is a subgroup of $S_3 \times S_4$ of order divisible by 9. However there is no subgroup in S_4 of order divisible by 3 with Z_4 as a factor, since the Sylow 3-normalizer in S_4 has order 6.

So $|X/Y| = 2$. Then, as before, a Sylow 2-subgroup S of Y is semi-regular on Θ_0. Hence X has order 72 or 144. Then $|K \cap Y|$ is 3 or 6, and so T' is characteristic in the normal subgroup $K \cap Y$, so that $T' \trianglelefteq X$ and $X \leq N_{S_8}(T')$. But $N_{S_8}(T')$ has orbits on Θ_0 of size 3 and 5 or 2 and 6, whereas Y is semi-regular of order at least 4.

Hence $|T| = 3$. Suppose first that $|X/Y| \geq 4$. Then by the Frattini argument, $N_X(T)$ has Z_4 as a factor. Thus T has 5 fixed points on Θ_0. Consider an element x of order 4 in $N_X(T)$. Then x either inverts T and therefore is of type 2,1,1 on Δ_0 and of type 4,2,1,1 on Θ_0, or it centralizes T and acts as a 4-cycle on Θ. In either case x is an odd permutation, which is not possible.

Hence $|X/Y| = 2$. Then [4, 9C] implies that all involutions fix at most 8 points of Ω. Notice that since 4p is 12 modulo 16, we see that 2^{10} does not divide $|G|$, so that G is known by various recent results. But let us argue directly.

We see again that a Sylow 2-subgroup of Y is semi-regular on Θ_0, so that $|Y|$ is 12 or 24 and $|X|$ is 24 or 48. Assume first that $|X| = 24$, $|Y| = 12$. Then Y has two orbits of size 4 on Θ_0 and therefore acts as A_4 on each. If X preserves the Y-orbits then X acts as S_4 on each of these and on Δ_0. But then an odd permutation in S_4 acts as an odd permutation on each of these and hence is odd on Θ. Hence X is transitive on Θ_0. But then any 2-element of X is semi-regular on Θ_0, so that involutions in X fix at most 4 points of Θ. Hence the involutions in G fix at most 4 points of Ω and so G is known [17], which leads to a contradiction. In fact, since 4p is 12 modulo 16, we see that 64 is the highest possible power of 2 dividing $|G|$, which gives an alternative argument.

Assume now finally that $|X| = 48$ and $|Y| = 24$. Here Y is transitive on Θ_0. If $|K| = 2$ then K has 4 orbits of size 2 on Θ_0, and X/K acts as S_4 on these and on Δ_0. Hence any involution of X fixes at most 4 points of Θ, and we arrive at a contradiction as before. So $|K| = 4$, and $X/K \simeq A_4$. Now A_4 has no subgroup of index 2, so K has four orbits of size 2 on Θ_0. Hence K is $Z_2 \times Z_2$ with two involutions of type $2^2 1^4$ on Θ_0 and one of type 2^4. Since X/K has no subgroup of index 2 this forces K to be central in X, which is impossible since K is not semi-regular on Θ_0.

3. The high transitivity of G

By the theorem of Ito [10] mentioned in the introduction, the insolubility of H, which we established in Section 2, implies that H is 3-transitive on each of the Γ_i. Then we know by another theorem of Ito [9, Satz 3] that the H-actions on $\Gamma_1, \ldots, \Gamma_k$ are isomorphic to each other. Our notation for the points of Ω will from now on be such that $\Gamma_1 = \{\alpha_1, \alpha_2, \ldots\}$, $\Gamma_2 = \{\beta_1, \beta_2, \ldots\}$, etc., with α_i, β_i etc. corresponding to each other under the action of H for each i. We shall also write α, β, etc., for α_1, β_1, etc. As before, α is chosen to be fixed by Q. Let R be a complement of Q in $H_{\alpha\Delta_1\Delta_2}$. Then any element in R other than 1 fixes precisely three points of Γ_1; one of these is α, the others will be α_2 and α_3.

We shall prove the theorem only for k = 2 and k = 4; the proof in the case k = 3 is similar. Our original proof relied on the 4-transitivity of H on each Γ_i. Unfortunately, as Professor Ito has noticed recently, there is a mistake in the last part of [10, III], which so far remains uncorrected. In the later stages of the proof we therefore have to work harder, using the following result which pushes the character theory in [10] just one step further:

Lemma (P.M. Neumann, unpublished). Let X be an insoluble group of degree $p = 2q+1$, with p and q prime numbers and $p > 11$. If X is not 4-transitive then the stabilizer $X_{\alpha\beta\gamma}$ of three points has two orbits on $\Omega - \{\alpha, \beta, \gamma\}$, each of size q-1. Moreover, the normalizer of a Sylow q-subgroup in X' has order $\frac{1}{2}q(q-1)$.

The case k = 2.

Step 1. G is 3-transitive.

We have already noticed that G is 2-transitive by [20, 31.1], and the action of Q implies that G is 2-primitive. Now H_α fixes β and has two 2-transitive orbits $\Gamma_1 - \{\alpha\}$ and $\Gamma_2 - \{\beta\}$. Since $p \nmid |G_\alpha|$ and G_α does not fix β, the assertion follows.

Step 2. G is 4-transitive.

From the action of $H_{\alpha_1\alpha_2}$ we see that the possibilities for the length of the $G_{\alpha_1\beta_1\alpha_2}$-orbits are 1, 2q-1, 2q-1,

2q, 2q-1,

1, 4q-2,

or 4q-1.

Now the second is clearly impossible, since $q \nmid |G_{\alpha_1\beta_1\alpha_2}|$. Consider the first and third case. Here the stabilizer of any 3 points in G fixes exactly 4 points. Hence we obtain a Steiner system S(3,4,n) on Ω. Clearly $\{\alpha_i,\beta_i,\alpha_j,\beta_j\}$ is a line for any pair i,j, and it is the unique line containing any triple in it. Hence the fourth point of the line on α_1, α_2, α_3 is not one of β_1,β_2,β_3, and so it is α_4 or β_4. Hence $H_{\alpha_1\alpha_2\alpha_3}$ fixes α_4, which contradicts the semi-regularity of R on $\Gamma_1 - \{\alpha_1,\alpha_2,\alpha_3\}$. Thus this is impossible, and so G is 4-transitive.

Step 3. G is 5-transitive.

Since $G_{\alpha_1\alpha_2\beta_1\beta_2}$ contains $H_{\alpha_1\alpha_2}$, the only alternative to this assertion is that $G_{\alpha_1\alpha_2\beta_1\beta_2}$ has two orbits of size p-2, which would imply that the order of $G_{\alpha_1\alpha_2\beta_1}$ is odd ([20, 3.13]). This is clearly impossible.

//

Step 4. G is 6-transitive.

By the Lemma at the beginning of this section, the $H_{\alpha_1\alpha_2\alpha_3}$-orbits on $\Omega - \{\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3\}$ have length divisible by q-1. By a theorem of Nagao [14], β_3 is not fixed by $G_{\alpha_1\alpha_2\alpha_3\beta_1\beta_2}$. Baring in mind that $q \nmid |G_{\alpha_1\alpha_3\alpha_2}|$, the possibilities for the length of the $G_{\alpha_1\alpha_2\alpha_3\beta_1\beta_2}$-orbits on $\Omega - \{\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2\}$ therefore are

$$2q-1, \quad q-1, \quad q-1,$$
$$2q-1, \quad 2q-2,$$
$$3q-2, \quad q-1,$$
$$\text{or} \quad 4q-3.$$

In the first three cases it follows from [19] that $G_{\alpha_1\alpha_2\beta_1\beta_2}$ is imprimitive. Let B be the block containing α_3. Then B is a union of $G_{\alpha_1\alpha_2\alpha_3\beta_1\beta_2}$-orbits, and since $|B|$ divides 4q-2, we have $|B| = 2q-1$ (this already excludes the third case). Let $\Lambda = B \cup \{\alpha_1, \alpha_2, \beta_1, \beta_2\}$. Then $G_{\{\alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2\}} \leq G_\Lambda$, and $G_{\alpha_1\alpha_2\beta_1\beta_2 B}$ is transitive on B. It follows that G_Λ is 5-transitive on Λ, so that $p \mid |G_\Lambda|$. This is impossible, since $p^2 \nmid |G|$.

Step 5. G is 7-transitive.

Since $H_{\alpha_1\alpha_2\alpha_3} \leq G_{\alpha_1\alpha_2\cdots\beta_3}$, all the $G_{\alpha_1\alpha_2\cdots\beta_3}$-orbits on the rest of Ω have length divisible by q-1. Hence the possibilities are

$$q-1, \quad q-1, \quad q-1, \quad q-1,$$
$$2(q-1), \quad q-1, \quad q-1,$$
$$2(q-1), \quad 2(q-1),$$
$$3(q-1), \quad q-1,$$
$$\text{or} \quad 4(q-1).$$

We now use a variation of an argument of M.D. Atkinson in [2, Lemma] to exclude the first three cases. Let U be a Sylow 3-subgroup of $G_{\alpha_1\alpha_2\cdots\beta_3}$, and let V be a Sylow 3-subgroup of $G_{\{\alpha_1,\alpha_2,\alpha_3\}\beta_1\beta_2\beta_3}$ containing U. Then $|V| = 3\cdot|U|$. But V normalizes $G_{\alpha_1\alpha_2\cdots\beta_3}$ and therfore permutes its orbits. Now $G_{\{\alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2,\beta_3\}}$ acts as S_6 on $\{\alpha_1,\dots,\beta_3\}$ and there are only at most four $G_{\alpha_1\alpha_2\dots\beta_3}$-orbits on $\Omega - \{\alpha_1,\dots,\beta_3\}$. It follows that V fixes these orbits setwise. But then, since $q-1 \equiv 1 \pmod 3$, we see that V fixes apart from $\beta_1, \beta_2, \beta_3$ also at least 1 or 2 points in each long $G_{\alpha_1\alpha_2\dots\beta_3}$-orbit. Hence V fixes at least six points, and since G is 6-transitive, V is conjugate to a subgroup of U. This is impossible, and so the first three cases cannot occur.

Consider now the fourth case. Here H is not 4-transitive, so the Lemma at the beginning of this section implies that R has order $\frac{1}{2}(q-1)$. Moreover, R has eight regular orbits Φ_i, and

$$\Delta_1 = \{\alpha_2\} \cup \Phi_1 \cup \Phi_2,$$
$$\Delta_2 = \{\alpha_3\} \cup \Phi_3 \cup \Phi_4,$$
$$\Delta_3 = \{\beta_2\} \cup \Phi_5 \cup \Phi_6,$$
$$\text{and} \quad \Delta_4 = \{\beta_3\} \cup \Phi_7 \cup \Phi_8.$$

Since H is not 4-transitive, the $H_{\alpha_1\alpha_2\alpha_3}$-orbits on $\Gamma_1 - \{\alpha_1,\alpha_2,\alpha_3\}$ are $\Phi_2 \cup \Phi_3$ and $\Phi_1 \cup \Phi_4$. Now the shorter $G_{\alpha_1\alpha_2\dots\beta_3}$-orbit is also an $H_{\alpha_1\alpha_2\alpha_3}$-orbit, so we can assume that this is $\Phi_2 \cup \Phi_3$.

Let S be a complement for Q in $N_G(Q)$ which contains R. Since R has small index in S, a subgroup R_0 of small index in R is normal in S. Then R_0 fixes precisely $\alpha_2, \alpha_3, \beta_2, \beta_3$ in $\Omega - \{\alpha, \beta\}$, so that the set $\{\alpha_2,\alpha_3,\beta_2,\beta_3\}$ is S-invariant, and is permuted in precisely the same way as $\{\Delta_1,\Delta_2,\Delta_3,\Delta_4\}$. Let x be an element in S which interchanges α and β; such an element exists by the Jordan lemma. Then $x \in G_{\{\alpha_1,\alpha_2,\dots,\beta_3\}}$, and so $(\Phi_2 \cup \Phi_3)x = \Phi_2 \cup \Phi_3$, so that $\{\Delta_1,\Delta_2\}$ and $\{\Delta_3,\Delta_4\}$ are x-invariant. But x involves $(\alpha\beta)$, and so it must be odd on $\Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4$ and hence also on $\{\Delta_1,\Delta_2,\Delta_3,\Delta_4\}$. It therefore involves precisely one of $(\Delta_1\Delta_2)$ or $(\Delta_3\Delta_4)$, and so acts differently on $\Delta_1 \cup \Delta_2$ and on $\Delta_3 \cup \Delta_4$. For instance, if x involves $(\Delta_1\Delta_2)$ then it fixes nothing in $\Delta_1 \cup \Delta_2$ but fixes β_2 and β_3 in $\Delta_3 \cup \Delta_4$.

On the other hand, let X be the setwise stabilizer in G of $\Gamma_1 - \{\alpha\}$ and $\Gamma_2 - \{\beta\}$. Let $\pi \in \Gamma_1 - \{\alpha\}$. Then $H_{\alpha\pi}$ fixes a point $\sigma \in \Gamma_2 - \{\beta\}$, and is transitive on $\Gamma_1 - \{\alpha,\pi\}$ and on $\Gamma_2 - \{\beta,\sigma\}$. Since $H_{\alpha\pi}$ has index 2 in X_π, it follows that $X_\pi = X_\sigma$, so that X acts in the same way on $\Gamma_1 - \{\alpha\}$ and $\Gamma_2 - \{\beta\}$. This is a contradiction, since $x \in X$. The case $k = 2$ of the Theorem is now proved.

The case $k = 4$.

Step 1. G is 2-primitive.

We have already established in Section 2 that one subdegree is 3 modulo q. Since $H_\alpha \leq G_\alpha$, the subdegrees are sums of 3, 2q, 2q, 2q, 2q. Now 3 is not a subdegree by [20, 18.4], and the possibilities 4q+3 and 6q+3 are ruled out by [19]. Finally, any group of degree 2q+3 whose order is divisible by q contains the alternating group by [20, 13.10], which rules out the possibility 2q+3. Hence G is 2-transitive, and in fact 2-primitive, since the highest common divisor of 3 and 8 is 1.

Step 2. G is 3-transitive.

Since $H_\alpha \leq G_{\alpha\beta}$, the $G_{\alpha\beta}$-orbits have size obtained out of 1, 1, 2q, 2q, 2q, 2q. Assume first that there are two of size 1 modulo q. Since G is 2-primitive and since $p \nmid |G_{\alpha\beta}|$, the only possibility is 4q+1, 4q+1. But then $|G_{\alpha\beta}|$ is odd by [20, 3.13], which is impossible as $|H_{\alpha\beta}|$ is certainly even. Hence one of the orbits has size 2 modulo q. Notice that $\{\gamma,\delta\}$ is not an orbit by [20, 18.7]. Hence the only possibilities are

2q+2, 6q,

4q, 4q+2,

or 8q+2.

The second is clearly impossible since $4q+2 = 2p$. In the first case, let Σ be the $G_{\alpha\beta}$-orbit of length $2q+2$. Then $\gamma, \delta \in \Sigma$, and since $H_\alpha \leq G_{\alpha\beta\gamma\delta}$, we see that $G_{\alpha\beta\gamma\delta}$ is 2-transitive on $\Sigma - \{\gamma, \delta\}$. Hence $G_{\alpha\beta}$ is 4-transitive on Σ, which contradicts [6].

Step 3. G is 4-transitive.

If $G_{\alpha\beta}$ has two blocks of imprimitivity then by a theorem of Grün (cf. [7, 35.5]), G_α has a normal subgroup N of index 2 which is rank 3 on $\Omega - \{\alpha\}$ with subdegrees 1, $4q+1$, $4q+1$. But then $|N|$ is odd by [20, 3.13], which is impossible since N must have a 2-transitive section of degree 2p.

Suppose next that $G_{\alpha\beta}$ has $4q+1$ blocks of imprimitivity. Then the stabilizer of any 3 points fixes precisely 4 points in Ω, and we obtain a Steiner system $S(3,4,n)$ on Ω. Let Λ be a line, say $\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$, and assume that λ_1 and λ_2 correspond to each other under the action of H, so that $H_{\lambda_1} = H_{\lambda_2}$. If $H_{\lambda_3} = H_{\lambda_1}$ then certainly also $H_{\lambda_4} = H_{\lambda_1}$. Therefore $H_{\lambda_3} \neq H_{\lambda_1}$ implies $H_{\lambda_4} \neq H_{\lambda_1}$, and hence $H_{\lambda_3} = H_{\lambda_4}$, since H fixes Λ, whereas $H_{\lambda_1\lambda_3}$ has orbits of size $p-2$ on the set of points of Ω not corresponding to λ_1, λ_3. Thus in either case, $H_{\lambda_1} = H_{\lambda_2}$ implies $H_{\lambda_3} = H_{\lambda_4}$. Consider now the line $\Lambda = \{\alpha_1, \alpha_2, \alpha_3, \omega\}$. Then ω is not fixed by $H_{\alpha_1\alpha_2\alpha_3}$ by the above remarks, since R is semi-regular on the set of points in Ω not corresponding to $\alpha_1, \alpha_2, \alpha_3$ under the action of H.

Hence G is 3-primitive. Now one of the non-trivial subdegrees of G is $2cq+1$ with $1 \leq c \leq 4$. Certainly $c \neq 1$ since $2q+1 = p$, and $c = 2$ and $c = 3$ are excluded by [19]. Thus G is 4-transitive.

Step 4. G is 5-transitive.

Since $H_\alpha \leq G_{\alpha\beta\gamma\delta}$, all the $G_{\alpha\beta\gamma\delta}$-orbits on $\Omega - \{\alpha, \beta, \gamma, \delta\}$ have length divisible by $2q$. If one of these does have length $2q$ then the other must be $6q$ by

[6], since G is clearly 4-primitive. Hence the possibilities are

$$2q,\quad 6q,$$
$$4q,\quad 4q,$$
$$\text{or}\quad 8q.$$

The Atkinson argument used in Step 5 of the case k = 2 excludes the second case, while an analogues argument with respect to 4 rules out the first case: Let U be a Sylow 2-subgroup of $G_{\alpha\beta\gamma\delta}$, let V be a Sylow 2-subgroup of $G_{\{\alpha,\beta,\gamma,\delta\}}$ containing U. Then $|V| = 8\cdot|U|$, since G is 4-transitive. Now V normalizes $G_{\alpha\beta\gamma\delta}$, and so preserves the two long $G_{\alpha\beta\gamma\delta}$-orbits. Since each of these has size 2 modulo 4, V has an orbit of size 2 in each. Let W be the pointwise stabilizer in V of two V-orbits of size 2; then the index of W in V is at most 4. On the other hand, W fixes at least four points of Ω, and since G is 4-transitive, this means that W is conjugate to a subgroup of U. This is a contradiction.

Step 5. G is 6-transitive.

Consider the length of the $G_{\alpha\beta\gamma\delta\alpha_2}$-orbits. These are sums of 1, 1, 1, 2q-1, 2q-1, 2q-1, 2q-1. Since 8q-1 is divisible by 3, the Atkinson argument implies that $\beta_2, \gamma_2, \delta_2$ are all in the same orbit Σ.

Assume first that $|\Sigma| = 3$. Then G acts on a Steiner system S(5,8,n). The line containing α, β, γ and any two of $\alpha_2, \beta_2, \gamma_2, \delta_2$ is $\{\alpha, \beta, \gamma, \delta, \alpha_2, \beta_2, \gamma_2, \delta_2\}$. Similarly the line containing α, β, γ and two of $\alpha_3, \beta_3, \gamma_3, \delta_3$ must be $\{\alpha, \beta, \gamma, \delta, \alpha_3, \beta_3, \gamma_3, \delta_3\}$. Consider now the line Λ on $\alpha, \beta, \gamma, \alpha_2, \alpha_3$. Then by the above observations Λ meets $\Omega - \{\alpha, \beta, \dots, \delta_3\}$ in precisely three points $\omega_1, \omega_2, \omega_3$. Then $\{\omega_1, \omega_2, \omega_3\}$ must be a $G_{\{\alpha,\beta,\dots,\delta_3\}}$-invariant subset of $\Omega - \{\alpha, \beta, \dots, \delta_3\}$. This is contrary to our knowledge of the action of $H_{\alpha_1\alpha_2\alpha_3}$.

Let $|\Sigma| = 2q+2$. Then $G_{\alpha\beta\dots\delta_2}$ is transitive, and in fact primitive,

$\Sigma - \{\beta_2, \gamma_2, \delta_2\}$, because it contains $H_{\alpha_1\alpha_2}$. It follows by [20, 13.2] that $G_{\alpha_1\beta_1\gamma_1\delta_1\alpha_2}$ is 4-transitive on Σ, which is impossible since q does not divide its order.

Suppose now finally that $|\Sigma| = 4q+1$. Then $H_{\alpha_1\alpha_2}$ has two ~~primitive~~ primitive orbits Σ_1, Σ_2 on $\Sigma - \{\beta_2, \gamma_2, \delta_2\}$ of size 2q-1. Since q ~~and p~~ does ~~do~~ not divide $|G_{\alpha_1\beta_1\gamma_1\delta_1\alpha_2}|$ we see that $G_{\alpha_1\beta_1\gamma_1\delta_1\alpha_2}$ is imprimitive on Σ and $\{\beta_2, \gamma_2, \delta_2\}$ is a block of imprimitivity. Consider any other block B of size 3. Then one of $B \cap \Sigma_1$, $B \cap \Sigma_2$ is a non-trivial block of $H_{\alpha_1\alpha_2}$ on Σ_1 or Σ_2, contradicting its primitivity there.

Step 6. G is 7-transitive.

The $G_{\alpha_1\beta_1\gamma_1\delta_1\alpha_2\beta_2}$-orbits have sizes obtained out of 1, 1, 2q-1, 2q-1, 2q-1, 2q-1. Now the Atkinson argument with respect to 4 (cf. Step 4) shows that all the $G_{\{\alpha_1,\beta_1,\ldots,\beta_2\}}$-orbits have even length and in fact only one has length not divisible by 4. Since none is divisible by p or q, the only possibilities are 2 and 8q-4 or 8q-2.

In the first case $G_{\{\alpha_1,\beta_1,\ldots,\alpha_2\}}$ has blocks of imprimitivity on $\Omega - \{\alpha_1,\beta_1,\ldots,\alpha_2\}$ of size 3, and $\{\beta_2, \gamma_2, \delta_2\}$ is one of these. Now the block containing α_3 must contain 3 points out of $\{\alpha_3, \beta_3, \gamma_3, \delta_3\}$, as we see from the action of $H_{\alpha_1\alpha_2\alpha_3}$. But this must be also true of the blocks containing β_3, γ_3 and δ_3, which gives a contradiction.

In the second case, $G_{\{\alpha_1,\ldots,\beta_2\}}$ is transitive on $\Omega - \{\alpha_1,\ldots,\beta_2\}$, and since $G_{\{\alpha_1,\ldots,\beta_2\}}/G_{\alpha_1\ldots\beta_2}$ is S_6, we see that either G is 7-transitive or $G_{\alpha_1\ldots\beta_2}$ has two orbits of size 4q-1. But the latter is impossible by [20, 3.13].

Step 7. G is 8-transitive.

Consider the $G_{\alpha_1\ldots\gamma_2}$-orbits. Note that $\{\delta_2\}$ is not an orbit by [14], and also that q does not divide the order of $G_{\alpha,\dots,\delta_2}$. Hence the possibilities

are $\qquad 4q-1, \quad 2q-1, \quad 2q-1,$

$\qquad 4q-1, \quad 4q-2,$

$\qquad 6q-2, \quad 2q-1,$

or $\quad 8q-3.$

The first two are excluded by the Atkinson argument with respect to 4. In the third case it follows from [19] that G is not primitive. This is however impossible, because the blocks would have size 2q. Hence the assertion.

Step 8. G is 9-transitive.

Here all the $G_{\alpha\dots\delta_2}$-orbits have length divisible by 2q-1. The Atkinson argument with respect to 4 implies directly that $G_{\{\alpha,\dots,\delta_2\}}$ is transitive on $\Omega - \{\alpha,\dots,\delta_2\}$. Since G is 8-transitive, this shows that G is 9-homogeneous on Ω. Since $G_{\{\alpha,\dots,\delta_2\}}/G_{\alpha\dots\delta_2}$ is S_8, we see that either G is 9-transitive or $G_{\alpha\dots\delta_2}$ has two orbits of size 4q-2 on $\Omega - \{\alpha,\dots,\delta_2\}$. In the latter case it follows that if Σ is any subset of Ω of size 9 then G_Σ^Σ is A_9 (and not S_9). This implies that any involution of G fixes at most ~~seven~~ two points, which is clearly impossible.

Step 9. More on the action of N(Q) on $\mathcal{E}$.

Let $N = N_G(Q)$, and let K and L be the kernels of N on $\Delta_0, \mathcal{E}_0$ respectively. Then $L \leq K$: Otherwise $LK > K$, so $1 \neq LK/K \triangleleft N/K$. Now $N/K = S_4$, so $LK/K \geq V_4$. But this implies that $L \cap C(Q) \not\leq Q$, and since Q is self-centralizing on its long orbits, this is not possible.

Let $X = N/L$, $Y = LC(Q)/L$. We shall write $\overline{K}$ for K/L. Then $X \leq S_8$ and $X^{\Delta_0} = S_4$, so $X \not\leq A_8$. By [20, 15.1], any 3-element of X acts on $\mathcal{E}_0$ as a product of two 3-cycles, since we know that all the 3-elements of X lie in Y. Now the normalizer in S_8 of such a 3-element is $Z_2 \times (Z_3 \text{ wr } Z_2) \cdot Z_2$, which has an elementary abelian Sylow 2-subgroup. Hence $X/Y \leq Z_2$ by the Frattini argument. If an involution of $C(Q)$ ~~a 2-element of Y~~ fixed a point in Θ_0 then, being even, it would have degree at most 6q+2; this is not possible by a theorem of Luther [11]. Hence the 2-elements in Y are semiregular on Θ_0. Therefore $|X|$ is 24 or 48. Furthermore, if $|X| = 24$ then $X = S_4$. If X has two orbits of size 4 on Θ_0 then the permutations odd on Δ_0 are even on Θ_0 and hence are odd on Ω, and the same is true if X is transitive on Θ_0. If X has orbits of size 2 and 6 then the involutions of Y cannot all be semi-regular. Hence $|X| = 48$ and $\widetilde{K}$ is Z_2 acting semi-regularly on Θ_0. Finally, note that we may assume that K normalizes R. Then $\{\alpha_2, \beta_2, \ldots, \delta_3\}$ is K-invariant.

Step 10. Let $D = G_{\{\alpha_2, \beta_2, \ldots, \delta_3\}}$. Then D is 4-transitive on $\Omega - \{\alpha_2, \ldots, \delta_3\}$. For, from the analysis in Step 9 it follows that $D_{\{\alpha, \beta, \gamma, \delta\}}$ is transitive on $\Omega - \{\alpha, \beta, \ldots, \delta_3\}$. Moreover, the lengths of the D_α-orbits on $\Omega - \{\alpha_2, \beta_2, \ldots, \delta_3, \alpha\}$ are obtained out of 3, 2(q-1), 6(q-1), and in fact all the $D_{\alpha\beta\gamma\delta}$-orbits on $\Omega - \{\alpha, \beta, \ldots, \delta_3\}$ have length divisible by 2(q-1), as we see from the action of K.

Since G is 9-transitive on Ω, the Atkinson argument with respect to 9 (cf. Step 4) shows that there are at most two D_α-orbits, because $6(q-1) \equiv 6 \pmod 9$. So the possibilities are

3, 8(q-1),

2q+1, 6(q-1),

2(q-1), 6q-3,

or 8q-5.

The first case is impossible by a theorem of Bannai [3, Theorem 2]. In the second case D is primitive, contrary to [19]. In the third case, D is imprimitive by [19], so the blocks must have size 2q-1. Now 6q-3 is odd, so $D_{\delta_3\alpha}$ is still transitive on the D_α-orbit of length 6q-3. It now follows from [1, Lemma 2] that $G_{\{\alpha_2,\beta_2,\ldots,\delta_3\}}$ acts as a 2-transitive group on a Steiner system S(2,2q,8q-3), which is impossible since q does not divide its order. Hence D is 2-transitive.

Now the $D_{\alpha\beta}$-orbits have length obtained out of 2, 2(q-1), 2(q-1), 2(q-1), 2(q-1), 2(q-1). Then the Atkinson argument with respect to 3 shows that $D_{\alpha\beta}$ is transitive. Similarly, the only possibilities for the length of the $D_{\alpha\beta\mu}$-orbits are 2q-1, 6(q-1),

or 8q-7.

In the first case though $D_{\alpha\beta}$ is primitive and the suborbit of size 2q-1 is 2-transitive, and a contradiction now comes from [5, II, Theorem 3]. Hence D is 4-transitive on $\Omega - \{\alpha_2,\beta_2,\ldots,\delta_3\}$.

Conclusion. We know that the orbits of $G_{\alpha_2\beta_2\ldots\delta_3\alpha\beta\mu}$ on $\Omega - \{\alpha_2,\ldots,\delta_3,\alpha,\beta,\mu\}$ have length combined out of 1 and eight times q-1. But $G_{\alpha_2\beta_2\ldots\delta_3\alpha\beta\mu}$ is normal in $D_{\alpha\beta\mu}$, and $D_{\alpha\beta\mu}$ is transitive on $\Omega - \{\alpha_2,\beta_2,\ldots,\delta_3,\alpha,\beta,\mu\}$. Hence G is 12-transitive on Ω. But G contains a 3-element in C(Q) fixing 2q+1 points of Ω. Hence by a result of W.A. Manning [12, p.596], G is alternating or symmetric. This concludes the proof of the theorem.

References

1. M.D. Atkinson, Two theorems on doubly transitive permutation groups, J. London Math. Soc. 6(1973), 269-274.
2. M.D. Atkinson, Doubly transitive but not doubly primitive permutation groups, J. London Math. Soc. 7(1974), 632-634.
3. Eiichi Bannai, On some triply transitive permutation groups, Geometriae Dedicata 6(1977), 1-11.
4. Richard Brauer, Some applications of the theory of blocks of characters of finite groups, III, J. Algebra 3(1966), 225-255.
5. Francis Buekenhout and Peter Rowlinson, On (1,4)-groups, III, J. London Math. Soc. 14(1976), 487-495.
6. P.J. Cameron, Permutation groups with multiply transitive suborbits, Proc. London Math. Soc. 25(1972), 427-440; II, Bull. London Math. Soc. 6(1974), 136-140.
7. C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New York 1962.
8. C. Hering, Zweifach transitive Permutationsgruppen, in denen zwei die maximale Anzahl von Fixpunkten von Involutionen ist, Math. Z. 104(1968), 150-174.
9. Noboru Ito, Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten, Acta Sci. Math. (Szeged) 21(1960), 206-217.
10. Noboru Ito, Transitive permutation groups of degree $p = 2q+1$, p and q being prime numbers, Bull. Amer. Math. Soc. 69(1963); II, Trans. Amer. Math. Soc. 113(1964), 454-487; III, Trans. Amer. Math. Soc. 116(1965), 151-166.
11. C.F. Luther, Concerning primitive groups of class u, II, Amer. J. Math. 55(1933), 611-618.
12. W.A. Manning, The degree and class of multiply transitive groups, Trans. Amer. Math. Soc. 35(1933), 585-599.
13. Izumi Miyamoto, On primitive permutation groups of degree $2p = 4q+2$, p and q being prime numbers, J. Fac. Sci. Univ. Tokyo 22(1975), 17-23.
14. H. Nagao, On multiply transitive groups, Osaka J. Math. 2(1965), 327-341.
15. P.M. Neumann, Transitive permutation groups of prime degree, II: A problem of Noboru Ito, Bull. London Math. Soc. 4(1972), 337-339.
16. E.T. Parker and Paul J. Nicolai, A search for analogues of the Mathieu groups, Math. Tables Aids Comput. 12(1958), 38-43.
17. Peter Rowlinson, Simple permutation groups in which an involution fixes a small number of points, J. London Math. Soc. 4(1972), 655-661.
18. John Thompson, Finite groups with fixed-point-free automorphisms of prime order, Proc. Nat. Acad. Sci. 45(1959), 578-581.
19. Marie J. Weiss, On simply transitive primitive groups, Bull. Amer. Math. Soc. 40(1934), 401-405.
20. Helmut Wielandt, Finte permutation groups, Academic Press, New York 1964.

Downing College,
Cambridge CB2 1DQ