J. Austral-Math. Soc. 19 (Series A) (1975), 129–145.

A CLASS OF SIMPLE GROUPS WITH NO DOUBLY TRANSITIVE REPRESENTATIONS

R. J. CLARKE

(Received 4 May 1970)

Communicated by G. E. Wall

1. Introduction

The first counterexample to the conjecture that all non abelian simple groups have doubly transitive permutation representations was pointed out by Parker in (1954), where he showed that the unitary group $PSU(4,4)$ had no doubly transitive representations. In this paper we generalize Parker's result to give an infinite class of simple groups having no doubly transitive permutation representations. Specifically, we prove

THEOREM 1. *The projective symplectic group $PSp(4,q)$ has no doubly transitive permutation representation for $q > 2$.*

Using the results of Srinivasan (1968) on characters of symplectic groups one could prove this result quite quickly. However, it may be of interest to give a proof not relying on the character table of $Sp(4,q)$. Our proof may be generalized to deal with a slightly larger class of groups.

2. Notation and Preliminaries

Throughout this paper G^* will denote the symplectic group $Sp(4,q)$, the subgroup of the general linear group $GL(4,q)$ consisting of all matrices A satisying $A'JA = J$, where

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

We write $q = p^t$ with p prime.

Factoring this group by its centre, the subgroup of scalar matrices, gives the projective symplectic group $G = PSp(4, q)$. We denote elements of G by matrices surmounted by a bar.

The order of G^* is $q^4(q^2-1)(q^4-1)$ and that of G is $q^4(q^2-1)(q^4-1)/d$, where $d = (2, q-1)$.

If H is any finite group, a character of H means a non-negative integral combination of the complex irreducible characters of H. The trivial character of H is denoted by 1_H. If H is a subgroup of G and ϕ is a character of H, ϕ^G denotes the character of G induced from ϕ.

If $S \subset H$, the centralizer of S is denoted by $C_H(S)$ and the normalizer of S by $N_H(S)$. Finally, the order of any set X is denoted by $|X|$.

We now give various small results which we shall require.

LEMMA 1. *Let $A \in K = GL(m, q)$ have the following form:*

$$A = \begin{bmatrix} C_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & C_r \end{bmatrix},$$

each $C_i \in GL(m_i, q)$, C_i and C_j for $i \neq j$ not conjugate in any linear group and each C_i of order r_i dividing $q^{m_i} - 1$ but not dividing

$$\prod_{l=1}^{m_i - 1} (q^l - 1). \qquad \textit{Then}$$

$$|C_K(A)| = \prod_i (q^{m_i} - 1).$$

PROOF. By considering the possible conjugacy classes of matrices of order prime to q we see that C_i is a power of an element of $GL(m_i, q)$ of order $q^{m_i} - 1$. The result now follows from Schur's lemma and Theorem 7.3 on page 187 of Huppert (1967).

LEMMA 2. *Let K be a finite group having a $k-$ply transitive permutation representation of degree n on a set Ω. Let L be the subgroup of K fixing k points and let U be a subgroup of L. Let Γ be the subset of Ω consisting of all point fixed by U and suppose that $|\Gamma| = m$. Then*

$$|N_K(U)| \leqq m(m-1)\cdots(m-k+1)\,|N_L(U)|.$$

Equality holds if and only if every subgroup of L conjugate to U in G is conjugate to U in L. In this case

$$(K : N_K(U)) = (L : N_L(U))\frac{n(n-1)\cdots(n-k+1)}{m(m-1)\cdots(m-k+1)},$$

and $N_K(U)$ acts k -- ply transitively on the set Γ.

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

PROOF. The first statement results from the fact that $N_K(U)$ acts as a group of permutations on Γ, and $N_L(U)$ is the subgroup of $N_K(U)$ fixing k points. The second part is the Lemma of Witt (1937; Satz 3.).

Clearly, if U is pronormal in K the conditions of equality hold. So equality holds if U is a Sylow subgroup of L.

LEMMA 3. *Let the finite group K have a doubly transitive permutation representation of degree n on a set Ω. Let $\alpha, \beta \in \Omega$ and write $K_{\alpha\beta}$ for the subgroup of K fixing α and β. Suppose there exists a prime p dividing $n-1$ and $|K_{\alpha\beta}|$. If Q is a Sylow p-subgroup of $K_{\alpha\beta}$ then $Q = 0_p(N_K(Q))$, that is Q is the maximal normal p-subgroup of its normalizer.*

PROOF. Let $P = 0_p(N_K(Q))$ and suppose Q fixes exactly m points of Ω. $N_K(Q)$ acts doubly transitively on these m points and, as $P \lhd N_K(Q)$, P acts either trivially or transitively on them. Now $m \equiv n \equiv 1 \pmod{p}$. Hence P, being a $p-$ group, cannot act transitively on m points. Hence P acts trivially on them, which means $P \subset K_{\alpha\beta}$. Thus $P = P \cap K_{\alpha\beta} = Q$.

LEMMA 4. *Let a group K have a permutation representation on a set Ω and let Γ be an orbit of some $y \in K$. Let s be a power of a prime s_0 such that s divides the order of y and let y^n have order s. Then if y^n fixes any point of Γ it fixes all points of Γ, while otherwise $s_0 \| \Gamma |$.*

The proof of this lemma is straightforward.

3. Symplectic Groups as Chevalley Groups

G is isomorphic to the Chevalley group $C_2(q)$, and we identify the two groups. We shall use freely the papers of Carter (1965) and Tits (1964) on Lie algebras, Chevalley groups and groups with a BN-pair. We shall also need the following results of Curtis (1966).

THEOREM A. *Let G be the Chevalley group $L(q)$. Let Σ be the set of fundamental roots of L and $J, K \subset \Sigma$. Define the subgroup W_J of W to be the group generated by the fundamental reflections for the roots in J and put $G_J = BW_JB$. Write $\psi_J = (1_{W_J})^W$ and $\chi_J = (1_{G_J})^G$. Then the mapping*

$$\theta: \psi = \sum_J a_J \psi_J \to \chi = \sum_J a_J \chi_J$$

is an isometry between the complex vector spaces generated by the ψ_J and the χ_J. In fact the scalar product

$$\begin{aligned}(\chi_J, \chi_K) &= \text{number of } (G_J, G_K) \text{ double cosets in } G \\ &= \text{number of } (W_J, W_K) \text{ double cosets in } W \\ &= (\psi_J, \psi_K).\end{aligned}$$

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

The Lie algebra C_2 has fundamental roots p_1 and p_2 and positive roots $p_1, p_2, p_1 + p_2$ and $2p_1 + p_2$. For the corresponding elements $x_r(t)$ of $C_2(q)$ we may write

$$x_{p_1}(t) = \begin{bmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -t & 0 & 1 \end{bmatrix}, \qquad x_{p_2}(t) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$x_{p_1+p_2}(t) = \begin{bmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -t & 0 & 1 \end{bmatrix}, \qquad x_{2p_1+p_2}(t) = \begin{bmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and

$$x_{-r}(t) = (x_r(t))'.$$

The subgroup U generated by the root subgroup X_r, for r a positive root, is a Sylow p-subgroup of G. $|U| = q^4$. The subgroup $B = N_G(U)$ has order $q^4(q-1)^2/d$. $B = UH$, where H is the subgroup of G consisting of elements of form

$$\begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda^{-1} & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu^{-1} \end{bmatrix}$$

where λ and μ are non zero elements of $GF(q)$.

The Weyl group W of C_2 is $\langle \omega_1, \omega_2 ; \omega_1 = \omega_2^2 = (\omega_1\omega_2)^4 = 1 \rangle$. Here

$$\omega_1(p_1) = -p_1, \omega_1(p_2) = 2p_1 + p_2$$

$$\omega_2(p_1) = p_1 + p_2, \omega_2(p_2) = -p_2.$$

We now apply Theorem A to find some characters of G.

They Weyl group of C_2 has subgroups $W_\phi = \{1\}$, $W_\Sigma = W$, $W_{\{p_1\}} = \langle \omega_1 \rangle$ and $W_{\{p_2\}} = \langle \omega_2 \rangle$.Using the notation of Theorem A, write ψ_1 for $\psi_{\{p_1\}}$, and so on. The conjugacy classes of W are $C_0 = \{1\}$, $C_1 = \{(\omega_1\omega_2)^2\}$, $C_2 = \{\omega_1\omega_2, \omega_2\omega_1\}$, $C_3 = \{\omega_1, \omega_2\omega_1\omega_2\}$ and $C_4 = \{\omega_2, \omega_1\omega_2\omega_1\}$. For the characters ψ_J,

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

	C_0	C_1	C_2	C_3	C_4
ψ_Σ	1	1	1	1	1
ψ_1	4	0	0	2	0
ψ_2	4	0	0	0	2
ψ_ϕ	8	0	0	0	0

The entries in the following table are the scalar products of these characters.

	ψ_Σ	ψ_1	ψ_1	ψ_ϕ
ψ_Σ	1	1	1	1
ψ_1	1	3	2	4
ψ_2	1	2	3	4
ψ_ϕ	1	4	4	8

By Theorem A a similar table is valid for the characters χ_Σ, χ_1, χ_2 and χ_ϕ of G. Using it we see that there are irreducible characters ϕ, ψ, ψ' and χ of G such that

$$\chi_\Sigma = 1_G$$

$$\chi_1 = 1_G + \phi + \psi$$

$$\chi_2 = 1_G + \phi + \psi'$$

and

$$\chi_\phi = 1_G + 2\phi + \psi + \psi' + \chi,$$

so that

$$\chi = \chi_\phi - \chi_1 - \chi_2 + \chi_\Sigma.$$

It is well known and easy to show that $\deg \chi = q^4$.

Consider $K = G_{\{p_2\}} = \rho B, n_w \sigma$. By Carter (1965; page 214) we have

$$n_{\omega_2} = x_{p_2}(1)x_{-p_2}(-1)x_{p_2}(1)$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Now G may be considered as the group of all collineations of a 3 dimensional projective space P over $GF(q)$ which commute with a certain skew symmetric form on P. We see from the form of B and n_{ω_2} that K fixes the point

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

$$x = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

of P. As K is maximal, it must be the subgroup of G fixing x. Now G has rank 3 action on P. The orbits of K consists of the point x, the $q + q^2$ points other than x on the orthogonal hyperplane to x and the q^3 points of P outside this hyperplane. See for these results Higman and McLaughlin (1965).

We shall use the results of Higman (1964) to obtain the degrees of characters ϕ and ψ', the non trivial irreducible constituents of $(1_K)^G$.

In the notation of Higman (1964; page 146), $k = q + q^2$, $l = q^1$ and $k < l$.

We calculate the parameters λ and μ. We have by Higman (1964; page 148),

$$\mu l = k(k - \lambda - 1).$$

Hence

$$\mu q^3 = (q + q^2 - \lambda - 1)$$

and

$$q^2 \mid (q - \lambda - 1).$$

As $\lambda \leqq k$, $\lambda = q + q^2 - 1$ or $\lambda = q - 1$. In the former case $\mu = 0$. But as K is maximal in G, the rank 3 representation of G is primitive. Hence $\mu \neq 0$ Higman (1964; page 149). So we have

$$\lambda = q - 1, \ \mu = q + 1.$$

Write $D = (\lambda - \mu)^2 + 4(k - \mu) = 4q^2$. For the degrees f_2 and f_3 of ϕ and ψ' we have in some order

$$\begin{aligned} f_2, f_3 &= [2k + (\lambda - \mu)(k + l) \mp \sqrt{D}(k + l)]/(\mp 2\sqrt{D}) \\ &= \pm \tfrac{1}{2}q^2 + \tfrac{1}{2}q(q^2 + q + 1). \end{aligned}$$

Hence as $q > 2$, $p \mid f_2, f_3$. Thus p divides the degrees of the irreducible non trivial constituents of $(1_B)^G$.

4. The Proof of the Main Theorem

We prove Theorem 1 in several stages. We have $G = PSp(4, q)$, $q = p^t > 2$, p a prime, as before. Suppose G has a doubly transitive permutation representation ρ on a set Ω with $|\Omega| = n$. G^* has an action on Ω via the map $G^* \to G$ which it will at times be convenient to consider. If $\alpha \in \Omega$ and $g \in G$ we write $g\alpha$ for $\rho(g)\alpha$. Let G_α be the subgroup of G fixing α.

(A) *If $p \nmid n$ then G_α is a maximal parabolic subgroup of G.*

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

PROOF. We recall that a parabolic subgroup of a group G with a BN-pair (B, N) is a subgroup conjugate to one containing B. As $p \nmid n$ we may take the Sylow p-subgroup U of G to be contained in G_α. As $HG_\alpha \geqq HU = B$, HG_α is a parabolic subgroup of G. Now G_α is maximal in G as G acts doubly transitively on Ω. Hence either $HG_\alpha = G_\alpha$ or $HG_\alpha = G$. In the first case we have the required result. In the second case, H acts transitively on Ω. Now H normalises each root subgroup X_r, and if r is a positive root, $X_r \subset U \subset G_\alpha$.

Let $\beta \in \Omega$. Then there is an $h \in H$ such that $\beta = h\alpha$. Then

$$X_r = hX_rh^{-1} \subset hG_\alpha h^{-1} = G_\beta$$

Thus $X_r \subset \cap_{\beta \in \Omega} G_\beta = \{1\}$, as G is a simple group, contradiction. We note that this result holds for an arbitrary Chevalley group.

(B) $p \mid n$

PROOF. If $p \nmid n$, G_α is a maximal parabolic subgroup of G. Hence G_α is conjugate either to $G_{\{p_1\}}$ or $G_{\{p_2\}}$. But as G acts doubly transitively on Ω, there are two G_α double cosets in G, that is $(1_{G_\alpha})^G = 1_G + \zeta$ for some irreducible character ζ. This contradicts our information about the characters χ_1 and χ_2 above.

(C) $n \mid |B| = q^4(q-1)^2/d$.

PROOF. We have that $(1_{G_\alpha})^G = 1_G + \zeta$ and

$$(1_B)^G = 1_G + 2\phi + \psi + \psi' + \chi,$$

where ζ, ϕ, ψ, ψ' and χ are irreducible characters. Now ζ has degree $n-1$ coprime to p. But we know that ϕ, ψ, ψ' and χ each have degree divisible by p. Hence ζ is distinct from these characters, so we have

$$((1_B)^G, (1_{G_\alpha})^G) = 1.$$

This is equivalent to $BG_\alpha = G$. Hence $n = (G: G_\alpha) \mid |B|$.

(D) $n \equiv 1$ *or* $2 \ (mod\,(q^2+1)/d)$.

PROOF. Write $GL = GL(4, q)$, $\overline{GL} = GL(4, q^4)$ and $\bar{G} = Sp(4, q^4)$. Let κ be a primitive $q^4 - 1$ th root of unity in the Galois field $GF(q^4)$. Put $\zeta = \kappa^{q^2-1}$. Write

$$X = \begin{bmatrix} \kappa & & & \\ & \kappa^{q^2} & & \\ & & \kappa^q & \\ & & & \kappa^{q^3} \end{bmatrix} \in \overline{GL}, \quad Y = X^{q^2-1} = \begin{bmatrix} \zeta & & & \\ & \zeta^{-1} & & \\ & & \zeta^q & \\ & & & \zeta^{-q} \end{bmatrix}$$

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

Finally, put

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \in \bar{G}.$$

We have $AXA^{-1} = X^q$. Given any matrix $E \in \overline{GL}$, write $Z^{(q)}$ for the matrix obtained from Z by raising all its entries to the qth power. Using a theorem of Lang (1956) we see that $\exists B \in G$ such that $A^{-1} = B^{-1}B^{(q)}$.

Put $x = BXB^{-1}$, $y = BYB^{-1}$, $a = BAB^{-1}$. Then

$$\begin{aligned} x^{(q)} &= B^{(q)}X^{(q)}B^{2(q)} \\ &= B^{(q)}AXA^{-1}B^{-(q)}, \text{ as } X^{(q)} = X^q \\ &= BXB^{-1} \\ &= x. \end{aligned}$$

Thus $x \in GL$. Similarly y and $a \in GL$. In fact y and a are in $GL \cap \bar{G} = G^*$.

Write $N = \langle y, a \rangle$. Then N has defining relations

$$y^{q^2+1} = 1, \; aya^{-1} = y^q, \; a^4 = y^{(q^2+1)/d}.$$

If b is any integer not divisible by $(q^2 + 1)/d$,

$$\begin{aligned} C_{G^*}(y^b) &= G^* \cap C_{GL}(y^b) \\ &= G^* \cap \langle x \rangle, \text{ by Lemma 1,} \\ &= \langle y \rangle, \end{aligned}$$

for $x^m \in G^*$ if and only if $x^m \in \bar{G}$ which happens if and only if m is divisible by $q^2 - 1$, that is $x^m \in \langle y \rangle$. Hence $N = N_{G^*}\langle y^b \rangle$.

To complete the proof of (D) we consider the action of G^* on Ω. Let s be a prime power dividing $(q^2 + 1)/d$ and write $s = s_0^e$ for s_0 a prime. Now s_0 is prime to $(G^* : \langle y \rangle)$, so the Sylow s_0-subgroup of $\langle y \rangle$, which is cyclic, is a Sylow s_0-subgroup of G^*. If $S = \langle y^b \rangle$ is the unique subgroup of order s of $\langle y \rangle$, S is the unique subgroup of order s of any Sylow subgroup of G^* containing S. Hence S is a pronormal subgroup of G^*.

Let Γ_s be the set of points of Ω fixed by S. If $|\Gamma_s| = m_s$ and $m_s \geqq 2$, we see from Lemma 2 that $N = N_{G^*}(S)$ acts doubly transitively on Γ_s.

LEMMA 5. *Let N have a doubly transitive permutation representation σ of degree m on a set Γ such Γ such that $a^4 \in \ker \sigma$. Then either,*

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

(*i*) $m = 2$ *and* $\ker\sigma = \langle y, a^2\rangle$ *or*

(*ii*) $m = 3$ *or* 5, $m \mid (q^2+1)/d$, $y^m \in \ker\sigma$ *and* $\langle y\rangle$ *acts transitively on* Γ.

PROOF. $\sigma(\langle y\rangle)$ is a normal subgroup of a doubly transitive group, so is either trivial or transitive.

If $\sigma(y) = 1$, the abelian group $N/\langle y\rangle$ acts doubly transitively on Γ. Hence $m = 2$ and we have case (i).

Suppose $\sigma(\langle y\rangle)$ is transitive. As $\langle y\rangle$ is abelian, y acts regularly on Γ. Hence $m \mid (q^2+1)/d$ and $y^m \in \ker\sigma$. Now $|\sigma(N)|$ divides $(N: \langle y^m, a^4\rangle) = 4m$ and $m(m-1)$ divides $|\sigma(N)|$. Thus $(m-1) \mid 4$ and $m \neq 2$ as $(q^2+1)/d$ is odd. This gives case (ii) and proves the lemma.

We see from Lemma 5 that we have one of the following cases for m_s:

(1) $m_s = 0$.

(2) $m_s = 1$. Then y fixes exactly one point of Ω.

(3) $m_s = 2$ and y fixes Γ_s. Then y fixes no other point of Γ.

(4) $m_s = 3$ or 5 and $\langle y\rangle$ acts transitively on Γ_s. Then y fixes no points of Ω.

If (1) holds we have from Lemma 4 that $s_0 \mid n$. But $|B|$ and $(q^2+1)/d$ are coprime, $s_0 \mid (q^2+1)/d$ and $n \,\|\, |B|$, contradiction.

If (2) holds it is clear that $m_u = 1$ for every prime power u dividing $(q^2+1)/d$. Let Δ be an S-orbit of Ω of length greater than one. Suppose $s \nmid |\Delta|$. Then $|\Delta| = s_0^f$ for some $f < e$. But then $y^{bs_0 f}$ has order s_0^{e-f} and fixes all points of Δ, contradiction. Hence $s \,\|\, |\Delta|$. Thus $s \mid (n-1)$. As this holds for every prime power dividing $(q^2+1)/d$ we have, as required,

$$(q^2+1)/d \mid (n-1).$$

If (3) holds it is clear that $m_u = 2$ for every prime power u dividing $(q^2+1)/d$.) Reasoning similar to that of case (2) gives

$$(q^2+1)/d \mid (n-2).$$

Suppose (4) holds and write $u = m_s$. As u is a prime dividing $(q^2+1)/d$, $m_u = 3$ or 5. Now Γ_s and Γ_u are each y-orbits of Ω. We have two cases.

(i) $\Gamma_s = \Gamma_u$. Then $u = m_u$ and, as $u \mid (n - m_u)$ by Lemma 4, we have $u \mid n$, contradiction.

(ii) $\Gamma_s \neq \Gamma_u$. Let be the *l.c.m.* of m_s and m_u. Then y^h fixes all points of $\Gamma_s \cup \Gamma_u$. So no odd prime divides the order of y^h, for otherwise y^h would fix only the points in one y-orbit. Thus $y^{2h} = 1$. But then $(q^2+1) \mid 2h \leqq 2.3.5$. Hence $q = 2$ or 3. But in neither of these cases is $(q^2+1)/d$ divisible by two distinct primes, contradiction. This completes the proof of (D).

(E) *We have the following two possibilities*:

(*a*) $q = 3, 4, 5, 8$ *or* 11 *and* $n = |\Omega| = \frac{1}{2}q(q-1)^2$

(*b*) $n = |\Omega| = q^4$.

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

PROOF. We have

$$n \equiv c(\mathrm{mod}\,(q^2+1)/d),$$

where $c = 1$ or 2, $q = p^t$, p a prime. We may write

$$n = q^i p^{-b} m,$$

where $1 \leqq i \leqq 4$, $0 \leqq b < t$, $p \nmid m$, and

$$i = 2l - j,$$

where $1 \leqq l \leqq 2$ and $0 \leqq j < 2$. Now

$$1/q^2 \equiv -1(\mathrm{mod}\,(q^2+1)/d).$$

Hence

$$m \equiv nq^{-2i}q^j p^b \equiv c(-1)^l q^j p^b (\mathrm{mod}\,(q^2+1)/d).$$

Write

$$m = k(q^2+1)/d + (-1)^l c q^j p^b.$$

Then $m \mid (q-1)^2/d$ from part (*C*). We must consider various cases.

Case (1): $l = 2$. Then $k \leqq 0$.

(i) *Suppose* $k = 0$.

We have $m = cq^j p^b$ and m is coprime to p. Hence $b = j = 0$ and $m = c$. Thus

$$n = cq^4.$$

If $c = 1$ we have (*b*). If $c = 2$,

$$n - 1 = (_2q^4 - 1) \mid (q-1)^2(q+1)^2(q^2+1)/d,$$

since $n(n-1) \parallel G \mid$. But

$$n - 2 = 2(q^4 - 1) = 2(q-1)(q+1)(q^2+1).$$

Thus $(n-1) \mid 1/d$. So $n = 2$, and G is the cyclic group of order 2, contradiction.

(ii) *Suppose* $k < 0$.

As $m > 0$ we have $q^2 + 1 < cdq^j p^b \leqq cdq^{j+1}/p$. Thus $p < cdq^{j-1}$. The only possibility, as $j \leqq 1$, is $p = 3$, $j = 1$, $c = d = 2$ and $b = t - 1$. Then

$$2m = -(q^2+1) + 4q^2/3 = (q^2-3)/3,$$

which must divide $(q-1)^2$. Therefore $q = 3$, $m = 1$ and

$$n = q^{2l-j} p^{-b} m = 27.$$

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

However then $n-1 = 26 \nmid |PSp(4,3)|$, contradiction.

Case (2): $l = 1$. Then as $m > 0$ we have $k > 0$. Now

$$dm = [k(q^2+1) - cdq^j p^b] \,|\, (q-1)^2 = q^2 - 2q + 1.$$

Hence, as $k \geqq 1$, $2q \leqq cdq^j p^b \leqq cdq^{j+1}/p$. Hence $p \leqq cdq^j/2$, so $j = 1$.

(i) *Let* $k = 1$.

$$dm = (q^2 + 1 - cdqp^b) \,|\, (q-1)^2.$$

Thus $dm \,|\, (q-1)^2 - dm = (cdp^b - 2)q$. Evidently $cdp^b \geqq 2$, for otherwise $dm > (q-1)^2$.

(α) *Suppose* $cdp^b = 2$. Then

$$dm = q^2 + 1 - 2q = (q-1)^2,$$
$$n = q(q-1)^2/dp^b.$$

Now if $dp^b = 1$, $n = q(q-1)^2$. But $(n-1) \,\|\, G|$, and $n-1$ is coprime to $q(q-1)$ and q^2+1. Thus $(n-1) \,|\, (q+1)^2$, which is false for all $q > 2$. Hence $dp^b = 2$ and $c = 1$. Then $n = \frac{1}{2}q(q-1)^2$. As $n(n-1) \,\|\, G|$, $(n-1) \,|\, (q+1)^2(q^2+1)$. But $n - 1 = \frac{1}{2}(q-2)(q^2+1)$. Thus $(q-2) \,|\, 2(q+1)^2$. So, as h.c.f. $(q-2, q+1) \,|\, 3$, $(q-2) \,|\, 2.3^2$. Hence

$$q = 3, 4, 5, 8 \text{ or } 11.$$

This gives case (a).

(β) *Suppose* $cdp^b > 2$. Then

$$dm = (q^2 + 1 - cdp^b q) \,|\, (cdp^b - 2)q.$$

But $(dm, q) = 1$, so that $dm \,|\, (cdp^b - 2)$. Hence $dm \leqq cdp^b - 2$. Thus

$$(q^2+3)/(q+1) \leqq cdp^b \leqq cdq/p.$$

But we have $dm \geqq 0$, so $cdp^b \leqq (q^2+1)/q$. Hence

$$q - 1 + 4/(q+1) \leqq cdp^b \leqq q + 1/q.$$

Since cdp^b is an integer we have $cdp^b = q$. Then

$$dm = q^2 + 1 - cdp^b q = 1.$$

Thus $d = m = 1$ and $n = mqp^{-b} = c = 2$, contradiction.

(ii) *Let* $k > 1$. Then

$$dm = (k-1)(q^2+1) + q(q - cdp^b) + 1 \leqq (q-1)^2.$$

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

Therefore $q < cdp^b$, from which follows $c = d = 2$, $p = 3$, $p^b = q/3$. Then we have

$$\begin{aligned} 2m &= 2(q^2 + 1) - 4q^2/3 \\ &= 2(q^2 + 3)/3 \,|\, (q - 1)^2. \end{aligned}$$

Now $(q^2 + 3, q - 1)$ 4 and so $2(q^2 + 3)/3 \,|\, 4^2$, that is $(q^2 + 3) \,|\, 24$. But then

$$2m = 2(3^2 + 3)/3 \,|\, (3 - 1)^2, \text{ which is false.}$$

We have now proven (**E**). We complete the proof of Theorem 1 by eliminating the remaining possibilities.

1. q = 3, n = 6.

$|PSp(4,3)| = 2^6 3^4 5$, and $|S_6| = 6! = 2^4 3^2 5$. If G had a doubly transitive permutation representation of degree 6 it would be isomorphic to a subgroup of S_6, which it is not.

2. q = 5, n = 40, or q = 11, n = 550.

Let α and β be distinct elements of Ω. Then

$$\begin{aligned} |G| &= 2^6 3^2 5^4 13, \quad q = 5, \\ |G| &= 2^6 3^2 5^2 11^4 61, \quad q = 11, \\ |G_{\alpha\beta}| &= 2^3 3 \cdot 5^3, \quad q = 5, \\ |G_{\alpha\beta}| &= 2^5 11^3, \quad q = 11. \end{aligned}$$

Let Q be a Sylow q-subgroup of $G_{\alpha\beta}$ and let Q fix exactly m points of Ω. $(G_\alpha : N_{G_\alpha}(Q)) = (G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q))(n - 1)/(m - 1)$ is integral and by Sylow's Theorem

$$\begin{aligned} (G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q)) &= 1 \text{ or } 6, \quad q = 5, \\ (G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q)) &= 1, \quad q = 11. \end{aligned}$$

Consider $q = 11$. $m = 11k$ for some $k < 50$, and by integrality $(11k - 1) \,|\, (550 - 1)$. There is no such k. Hence this case does not occur.

Consider $q = 5$. $m = 5k$ for some $k < 8$, and either $(5k - 1) \,|\, (40 - 1)$ or $(5k - 1) \,|\, 6(40 - 1)$.

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

Hence $k = 2$ and $(G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q)) = 6$. Now

$$\begin{aligned} |N_G(Q)| &= |N_{G_{\alpha\beta}}(Q)|m(m-1) \\ &= 2^2 5^3 10 \cdot 9 \\ &= 2^3 3^2 5^4, \end{aligned}$$

by Lemma 2. Now $|Q| = 5^3$ and $|U| = 5^4$. Hence we may assume that Q is a normal subgroup of U with cyclic factor group. We have that the derived group $U' \subset Q$.

From the Chevalley commutator formula (Carter (1965; page 211)), we have that

$$U' = X_{p_1+p_2} X_{2p_1+p_2}.$$

So

$$Q = \langle U', x_{p_1}(t_1) x_{p_2}(t_2) \rangle,$$

where $t_1, t_2 \in GF(q)$ are not both zero.

We consider two cases.

(1) *Suppose* $t_1 \neq 0$. Then $Q' = X_{2p_1+p_2}$ and $C_Q(Q') = X_{p_1+p_2} X_{2p_1+p_2}$. These groups are each characteristic in Q, so

$$N_G(Q) \subset N_G(X_{2p_1+p_2}) \cap N_G(X_{p_1+p_2} X_{2p_1+p_2}) = M.$$

Now using the formula $n_\omega X_r n_\omega^{-1} = X_{\omega(r)}$ of Carter (1965; page 214) we see that $M = B$. Thus

$$|N_G(Q)| \, |B| = 2^3 5^4, \text{ a contradiction.}$$

(2) *Suppose* $t_1 = 0$. Then $Q = X_{p_1} X_{p_1+p_2} X_{2p_1+p_2}$. It is easily calculated that

$$N_G(Q) = B \cup B n_{\omega_1} B.$$

Now $|B n_{\omega_1} B| = |B| q^m$, where m is the number of positive roots of C_2 transformed by ω_1 into negative roots (Carter (1965; page 220)). Thus

$$\begin{aligned} |N_G(Q)| &= |B|(1+q) \\ &= \tfrac{1}{2} 5^4 (5-1)(1+5) \\ &= 2^8 3 \cdot 5^4, \end{aligned}$$

a contradiction.

3. $\mathbf{q = 4,\ n = 18}$

Let α and β be distinct elements of Ω. Then

$$|G| = 2^7 3^2 5^2 17, \quad |G_{\alpha\beta}| = 2^7 5^2.$$

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

Let P be a Sylow 5-subgroup of $G_{\alpha\beta}$ and suppose P fixes exactly m points of Ω. Then as $m \equiv 18 (\mathrm{mod}\, 5)$, $m = 3$ or 8. By Sylow's Theorem $(G_{\alpha\beta} : N_{G_{\alpha\beta}}(P)) = 1$ or 2^4. Now $(G_\alpha : N_{G_\alpha}(P)) = (G_{\alpha\beta} : N_{G_{\alpha\beta}}(P))(n-1)/(m-1)$ is integral, so we have $m = 3$ and $G_{\alpha\beta} : N_{G_{\alpha\beta}}(P)) = 2^4$. By Lemma 2

$$\begin{aligned} \left|N_G(P)\right| &= \left|N_{G\alpha\beta}(P)\right| m(m-1) \\ &= 2^4 3 \cdot 5^2. \end{aligned}$$

Since $G = G^* = Sp(4,4)$ we are in fact working with matrices. P, being a Sylow 5-subgroup of G may be considered as generated by matrices

$$a = \begin{bmatrix} A & O \\ O & I_2 \end{bmatrix}, \qquad b = \begin{bmatrix} I_2 & O \\ O & A \end{bmatrix},$$

where $A \in SL(2,4)$ has order 5. By Lemma 1 we have $\left|C_{GL(4,4)}(ab^2)\right| = (4^2-1)^2$. In fact the centralizer of ab^2 consists of matrices

$$c = \begin{bmatrix} C & O \\ O & D \end{bmatrix},$$

where $C, D \in C_{GL(2,4)}(A)$, a group generated by a matrix of order 15 with determinant a primitive cube root of unity. Now $c \in G$ if and only if $C, D \in SL(2,4)$. Thus $\left|C_G(ab^2)\right| = 5^2$ and $\left|C_G(P)\right| = 5^2$. So $C_G(P) = P$.

The only elements of P with the same eigenvalues as a are a, b, a^{-1} and b^{-1}. Thus if $g \in N_G(P)$, $gag^{-1} = a, b, a^{-1}$ or b^{-1}. There are the same choices for gbg^{-1}. Since gag^{-1} and gbg^{-1} generate P we see that $(N_G(P) : P) \leqq 8$. This is a contradiction.

4. $\mathbf{q = 8,\ n = 196}$

Let α and β be distinct elements of Ω. Then

$$\left|G\right| = 2^{1}\,^{2}3^4 5 \cdot 7^2 13, \quad \left|G_{\alpha\beta}\right| = 2^{10}3^3.$$

Let Q be a Sylow 3-subgroup of $G_{\alpha\beta}$ and P a Sylow 3-sub-group of G containing Q. We may take $P = \langle a, b \rangle$, where

$$a = \begin{bmatrix} A & O \\ O & I_2 \end{bmatrix}, \qquad b = \begin{bmatrix} I_2 & O \\ O & A \end{bmatrix},$$

with $A \in SL(2,8)$ an element of order 9. As in the preceding case we have $C_G(P) = P$. In fact $C_G(a^i b^j) = P$ unless $3 \mid i$, $3 \mid j$ or $3 \mid (i-j)$. Clearly Q must contain elements other than those of form a^i, b^i and $(ab)^i$. Hence $C_G(Q) = P$. Thus $N_G(Q) \subset N_G(C_G(Q)) = N_G(P)$ and so $P \lhd N_G(Q)$, contradicting Lemma 3.

5. n = 1, any q.

Let $\alpha \in \Omega$ and let U be the upper unitriangular subgroup of G. U is a Sylow p-subgroup of G, and $G = UG_\alpha$. We take the elements of U as a transversal for G_α in G.

Let $\theta \in GF(q)$ be of maximal multiplicative order such that

$$h = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \theta & 0 \\ 0 & 0 & 0 & \theta^{-1} \end{bmatrix}$$

is in some G_α. $\theta \neq 1$, as $(q-1)^2/d \,\|\, |G_\alpha|$. Now h normalizes U, so if $u \in U$, $hUG_\alpha = huh^{-1}G_\alpha$. Thus the number of points of Ω fixed by h is $|C_m(h)|$. Put

$$u = x_{p_1}(t_1)x_{p_2}(t_2)x_{p_1+p_2}(t_3)x_{2p_1+p_2}(t_4).$$

Then

$$huh^{-1} = x_{p_1}(\theta^{-1}t_1)x_{p_2}(\theta^2 t_2)x_{p_1+p_2}(\theta^{-3})x_{2p_1+p_2}(t_4).$$

Thus either $\theta^2 \neq 1$ and h fixes exactly q points of Ω or $\theta^2 = 1$ and h fixes exactly q^2 points of Ω. In the latter case it is clear that $q = 3$. We consider this case later.

(1) *Suppose* $\theta^2 \neq 1$. Write $S = \langle h \rangle$. By Lemma 2,

$$\begin{aligned} |N_G(S)| &\leqq |N_L(S)| q(q-1), \ L = G_{\alpha\beta}, \ \beta \neq \alpha \\ &\leqq |L| q(q-1) = q(q-1)^2(q+1)^2/d. \end{aligned}$$

But h is centralised by the elements

$$\left[\begin{array}{ccc|c} & & & 0 & 0 \\ & A & & 0 & 0 \\ 0 & & 0 & \lambda & 0 \\ 0 & & 0 & 0 & \lambda^{-1} \end{array}\right]$$

of G, where $A \in SL(2,q)$, $\lambda \in GF(q)$, $\lambda \neq 0$. Thus

$$\begin{aligned} |C_G(S)| &\geqq (q-1)|PSL(2,q)| \\ &= q(q-1)^2(q+1)/d. \end{aligned}$$

https://doi.org/10.1017/S144678870002944X Published online by Cambridge University Press

Also the element

$$\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{array}\right]$$

normalises S. Thus we have a contradiction.

(2) *Suppose* $\theta^2 = 1$, $q = 3$. Then Then h fixes 9 points of Ω and, writing $S = \langle h \rangle$ and $L = G_{\alpha\beta}$ with $\beta \neq \alpha$, we have as in (1)

$$\begin{aligned} \left|N_G(S)\right| &\leqq \left|L\right| 9(9-1) \\ &= 2^5 3^2. \end{aligned}$$

But h is centralised by the elements

$$\left[\begin{array}{cc} A & 0 \\ 0 & B \end{array}\right]$$

of G, where $A, B \in SL(2,3)$. Hence

$$\begin{aligned} \left|C_G(S)\right| &\geqq \tfrac{1}{2}\left|SL(2,3)\right|^2 \\ &= 2^5 3^5. \end{aligned}$$

As in (1) we deduce $\left|N_G(S)\right| > 2^5 3^2$, a contradiction. This proves Theorem 1.

Our proof may be generalised to give a similar result for a slightly larger class of groups. In fact one can prove

THEOREM 2. *The group* $PSp(2^r, q)$ *has no doubly transitive permutation representation for* $r \geqq 2$, *excepting for each* r *at most a finite number of values of* q.

Many parts of the above proof need only slight modification. To prove the corresponding part (*C*) we need the unpublished result of D. G. Higman that the degrees of the non trivial irreducible constituents of $(1_\beta)^G$ are almost always divisible by p. More complex manipulation with special subgroups of G is needed to eliminate certain special cases which arise.

The material in this paper was part of my thesis submitted for the degree of Ph.D. at the University of Warwick. I should like to express my gratitude to Professor J. A. Green for his help and encouragement.

I gratefully acknowledge the support of a British Council Commonwealth Scholarship.

References

R. W. Carter (1965), 'Simple groups and simple Lie algebras', *J. London Math. Soc.* **40**, 193–240.

C. W. Curtis (1966), 'The Steinberg character of a finite group with a BN-pair', *J. Algebra* **4**, 433–441.

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

D. G. Higman and J. E. McLaughlin (1965), 'Rank 3 subgroups of finite symplectic and unitary groups', *J. reine u. angew. Math.* **218**, 174–189.

B. Huppert (1967), *Endliche Gruppen I* (Springer-Verlag, Berlin 1967).

S. Lang (1956), 'Algebraic groups over finite fields', *Amer. Math. J.* **78**, 555–563.

E. T. Parker, 'A simple group having no multiply transitive representation', *Proc. Amer. Math. Soc.* **5**, 606–611.

Bhama Srinavasan (1968), 'The characters of the finite symplectic group Sp (4, q)', *Trans. Amer. Math. Soc.* **131**, 488–425.

J. Tits (1964), 'Algebraic and abstract simple groups', *Ann. of Math.* **80**, 313–339.

E. Witt (1937), 'Die 5-fach transitiven Gruppen von Mathieu', *Abh. Math. Sem. Univ.* Hamburg **12**, 256–264.

Department of Pure Mathematics
University of Adelaide
South Australia