FINITE GROUPS WITH A PROPER 2-GENERATED CORE

BY

MICHAEL ASCHBACHER[1]

ABSTRACT. H. Bender's classification of finite groups with a strongly embedded subgroup is an important tool in the study of finite simple groups. This paper proves two theorems which classify finite groups containing subgroups with similar but somewhat weaker embedding properties. The first theorem, classifying the groups of the title, is useful in connection with signalizer functor theory. The second theorem classifies a certain subclass of the class of finite groups possessing a permutation representation in which some involution fixes a unique point.

Given a finite group G, the *2-rank* of G, denoted by $m(G)$, is the number of generators of a maximal elementary 2-subgroup of G. Let S be a Sylow 2-subgroup of G, and k a positive integer. As defined by John Walter, the *k-generated core* of G containing S is

$$\Gamma_{S,2}(G) = \langle N_G(X) : X \leq S \text{ and } m(X) \geq k \rangle.$$

The main result of this paper is the classification of finite groups with a proper 2-generated core.

Theorem 1. *Let G be a finite group, S a Sylow 2-subgroup of G, and H a proper subgroup of G such that $\Gamma_{S,2}(G) \leq H$. Then one of the following holds:*
  (i) $m(G) \leq 1$.
  (ii) $m(G) = 2$ *and* $G = O(G)H$.
  (iii) $\overline{G} = G/O(G)$ *is isomorphic to* $GL_2(3)$, $\hat{S}_7$, *or* $\hat{A}_9$.
  (iv) $\overline{G}$ *is contained in the automorphism group of* $L_2(q)$, M_{11}, *or* J_1, *the Janko group of order* 175,560.
  (v) $\overline{G}$ *has a normal subgroup L isomorphic to* $L_2(q)$, $Sz(q)$, *or* $U_3(q)$, *q even,* $\hat{Sz}(8)$, $SL_2(5)$ *or* $SL_2(5)YSL_2(5)$. $K = C_{\overline{G}}(L)$ *has 2-rank at most 1 and if $m(K) = 1$ then LK contains all involutions in $\overline{G}$.*

$\hat{X}$ denotes a covering of X over Z_2.

A finite group G is *exceptional* if $m(G) \geq 3$, G has a proper 2-generated core, and G is on the list of groups in Theorem 1.

The following equivalence is useful in applying Theorem 1.

Lemma 1. *Let G be a finite group, let S be a Sylow 2-subgroup of G, and let H be a subgroup of G containing S. Then the following are equivalent:*

(1) $\Gamma_{S,2}(G) \leq H$.

(2) $H \cap H^g$ *has 2-rank at most one for each* $g \in G - H$.

The next result is crucial to the proof of Theorem 1.

Theorem 2. *Let G be a finite group, H a proper subgroup of G, and z an involution in the center of some Sylow 2-subgroup of G. Assume*

(i) $z \in H^g$ *if and only if* $g \in H$.

(ii) *If u is an involution with* $z \in C_G(u) = M \nleq H$ *then* $H \cap L$ *is strongly embedded in* $L = \langle z^G \cap M \rangle$.

Then $\langle z^G \rangle \cap H$ *is strongly embedded in* $\langle z^G \rangle$.

Finally there is the following corollary to Theorem 1.

Theorem 3. *Let G^Ω be a doubly transitive permutation group of odd degree in which a Sylow 2-subgroup of the stabilizer of two points is cyclic or quaternion. Then either*

(i) G^Ω *has a regular normal subgroup, or*

(ii) *G has a unique minimal normal subgroup L, $G \leq \text{Aut}(L)$, and L^Ω is permutation isomorphic to $L_2(q)$, $Sz(q)$, or $U_3(q)$, q even, in their natural doubly transitive representations, or $L_2(11)$ or M_{11} on 11 letters.*

The proof of Theorem 1 utilizes several results of Gorenstein and Walter on exceptional groups. The list of exceptional groups given above is slightly larger than their list in [7]. Large parts of the proof of Theorem 2 are adaptations of work of Suzuki and Bender on groups with a strongly embedded subgroup to the somewhat more general setting of Theorem 2. Theorem 2 can be used to shorten significantly the proof of an important theorem of Shult [8]. §7 ulilizes many ideas from the proof of that theorem and can be omitted if the result is assumed.

The author would like to thank Professor Ernest Shult for pointing out several errors in the original version of this manuscript and suggesting improvements to the proof.

1. Notation. Let G be a permutation group on a set Ω, $X \leq G$, and $\Delta \subseteq \Omega$. Denote by X_Δ, $X(\Delta)$, the pointwise, global stabilizer of Δ in X, respectively. Set $X^\Delta = X(\Delta)/X_\Delta$ with induced permutation representation. Denote by $F(X)$ the set of fixed points of X in Ω.

Given a prime p and a positive integer n, denote by n_p the highest power of p dividing n.

Given a p-group P set $\Omega_1(P) = \langle x \in P: x^p = 1 \rangle$ and $\mho^n(P) = \langle x^{p^n}: x \in P \rangle$.

For given prime p, $\theta(G) = O_\pi(G)$ where $\pi = \{2, p\}'$.

HYG is the central product of groups H and G with amalgamated center.

A group G is said to be *known* if G is one of the groups in the conclusion of Theorem 1. G is said to be *quasisimple* if G is perfect and $G/Z(G)$ is simple. $E(G)$ is the product of all subnormal quasisimple subgroups of G, known as the *components* of G, and $F^*(G)$ is the product of $E(G)$ with the Fitting group of G.

2. **Preliminary results.** We first give a proof of Lemma 1. Assume the hypothesis of Lemma 1, and let $\Gamma_{S,2}(G) \leq H$. Suppose $m(H \cap H^g) \geq 2$ and let T be a Sylow 2-subgroup of $H \cap H^g = D$. Then $N_G(T) \leq D$, so $T = S$ is Sylow in G. So S and $S^{g^{-1}} \leq H$ and thus $S^{g^{-1}} = S^h$ for some $h \in H$. Therefore $hg \in N_G(S) \leq H$, so $g \in H$. Thus (1) implies (2). Conversely assume $H \cap H^g$ has 2-rank at most one for $g \in G - H$. Let $X \leq G$ with $m(X) \geq 2$, and let $g \in N_G(X)$. Then $X \leq H \cap H^g$, so $g \in H$. That is $N_G(X) \leq H$. So $\Gamma_{S,2}(G) \leq H$ and therefore (2) implies (1).

Lemma 2.1. *Let X be a group of odd order and t an automorphism of X of order 2. Set $K = \{x \in X: x^t = x^{-1}\}$, let p be a prime, and let P a t-invariant Sylow p-subgroup of X. Then:*

(1) *If a, b, and $a^b \in K$, then $a^b = a$.*

(2) *$|P \cap K| = |K|_p$ and $|C_P(t)| = |C_X(t)|_p$.*

Proof. Lemma 2.1 of [2].

Lemma 2.2. *Let $S \in \mathrm{Syl}_2(G)$, $S' \leq T \leq S$, and $y \in S - T$. Assume for each $x \in \langle y \rangle$ that if $x^g \in S$ then $x^g \in xT$. Then G has a normal subgroup K with $G = KS$ and $y \in G - K$.*

Proof. See, for example, 2.9 in [2].

Lemma 2.3. *Let $H \leq G$, S a Sylow 2-subgroup of G contained in H, and z an involution in the center of S. Then*

(1) *If $\Gamma_{S,2}(G) \leq H$ then H controls fusion of its involutions.*

(2) *If $z \in H^g$ if and only if $g \in H$, then H controls fusion in S.*

Proof. (1) follows from Alperin's fusion theorem. So assume $z \in H^g$ if and only if $g \in H$. Represent G by conjugation on H^G. Then z fixes the unique point H in H^G.

Let $X, X^{g^{-1}} \subseteq S$. Then $z, z^g \in C(X)$. Let A and B be Sylow groups of $C_H(X)$ and $C_{H^g}(X)$ containing z and z^g respectively. Then $F(A) = F(z) = H$, so A is Sylow in $C_G(X)$. Also $F(B) = H^g$ and B is Sylow in $C(X)$. Let $y \in C(X)$ with $A^y = B$. Then $H^y = F(A)^y = F(B) = H^g$, so $h = yg^{-1} \in N(H) = H$. Also $X^h = X^{yg^{-1}} = X^{g^{-1}}$.

Theorem 2.4. *Let* $m(G) = 2$, *H a proper 2-generated core of G. Then either* $G = O(G)H$ *or* $\overline{G} = G/O(G)$ *is one of the following:*

(1) $\overline{G} \leq \operatorname{Aut}(L)$ *where L is isomorphic to* $U_3(4)$, $L_2(q)$ *or* M_{11}.

(2) $\overline{G} \cong \hat{S}_7$, *a covering of* S_7 *by* Z_2.

(3) $\overline{G} \cong GL_2(3)$.

(4) $E(\overline{G}) \cong SL_2(5)$, $O_2(\overline{G})$ *is cyclic, and* $F^*(\overline{G})$ *contains all involutions in* $\overline{G}$.

Proof. By induction we may take $O(G) = 1$. Set $Q = O_2(G)$. Clearly $m(Q) \leq$ 1. Suppose $Q = F^*(G)$. G is not a 2-group but $C_G(F^*(G)) = Z(Q)$, so $G/Z(Q) \leq$ $\operatorname{Aut}(Q)$, and as $m(Q) = 1$, $G \cong GL_2(3)$. So we may assume $F^*(G) \neq Q$. As $O(G) = 1$, $F^*(G) = QE(G)$. As $m(G) = 2$, $E(G) = L$ is quasisimple and either $Q = 1$ or Q is cyclic and $Q \cap L \neq 1$. If $F^*(G) \leq H$ then by a Frattini argument, $m(F^*(G)) = 1$. So $F^*(G) = L \cong SL_2(q)$ or $\hat{A}_7$ and there is an involution $a \in H - L$. But $C_G(L) = Z(L)$ and the outer automorphism group of $L_2(q)$ or A_7 is abelian. Therefore $G = LN_G(\langle a \rangle Z(L)) \leq H$, a contradiction. It follows that $H \cap L$ is a proper core of L.

Assume $Q \neq 1$. L is quasisimple of 2-rank at most 2, so L is isomorphic to $SL_2(q)$, $\hat{A}_7$, or $Sp_4(q)$, q odd [1], [6]. Set $\overline{G} = G/Z(L)$. Suppose $Q = \langle x \rangle$ has order greater than 2. Claim $L \cong SL_2(5)$. We may assume Q has order 4. Then if $\overline{a}$ is an involution in $\overline{L}$, $\langle a, x \rangle = X$ has 2-rank 2, so $C_{\overline{L}}(\overline{a}) = \overline{N_L(X)} \leq H$. So $\overline{L}$ has a strongly embedded subgroup.

Suppose $L \cong SL_2(q)$ and a is an involution in H inducing an outer automorphism on L. We may take $G = L\langle a \rangle$. Then $C_{\overline{G}}(\overline{a}) = N_G(\overline{\langle a, x \rangle}) \leq \overline{H}$. Further $C_{\overline{G}}(\overline{a})$ is a maximal subgroup of $\overline{G}$, so $\overline{H} = C_{\overline{G}}(\overline{a})$. But H controls fusion of its involutions, so the Z^*-theorem yields a contradiction.

To complete the proof of the case $Q \neq 1$, we may assume $G \cong Sp_4(q)$. Let $b \in H$ with $b^2 = x$. As $\overline{G}$ has 2 classes of involutions and no strongly embedded subgroup, $N_G(\langle b \rangle) = B$ has a proper core. But $m(O_{2',2}(B)) > 1$, a contradiction.

So we may take G isomorphic to $U_3(q)$, $L_3(q)$, or A_7. Then G has one class of involutions a^G. As G has no strongly embedded subgroup, $M = C_G(a)$ has a proper core, and then as $O_2(C(a)) \neq 1$, by induction M is of type (2)–(4). It follows that G is $L_3(3)$ or $L_3(5)$. Now H controls fusion of its involutions and $\Omega_1(S)$ is nonabelian where $S \in \operatorname{Syl}_2(G)$. Therefore $O_2(H/O(H)) = 1$. Then $H/O(H)$ contains a simple component $K/O(H)$ and as $m(G) = 2$, $K/O(H) = E(H/O(H))$. As $L_3(3)$ is a minimal simple group, G is not $L_3(3)$. H is transitive on its involutions so $\Omega_1(S) \leq K$. S is wreathed so $\Omega_1(S)$ is not Sylow in a simple group. But $|S : \Omega_1(S)| = 2$, so $S \in \operatorname{Syl}_2(K)$. But the only simple group with wreathed Sylow group and of smaller order than $L_3(5)$ is $U_3(3)$, and the order of $U_3(3)$ does not divide the order of $L_3(5)$.

The next three results are slight generalizations of theorems due to Gorenstein and Walter.

Theorem 2.5. *Let G be a fusion simple group, let S be a Sylow 2-subgroup of G, and let z be an involution in the center of S. Assume $M = C_G(z)$ is exceptional. Then $G \cong J_1$.*

Proof. Let H be a proper 2-generated core for M containing S. Proposition 4 in [7] handles all cases except the following: $\overline{M} = M/O(M)$ has a normal subgroup $\overline{L}$ such that $\overline{K} = C_{\overline{M}}(\overline{L})$ is of rank one and LK contains all involutions in M. Also either (i) $\overline{L} = \overline{L}_1 Y \overline{L}_2$, $\overline{L}_i \cong SL_2(5)$, and the components L_i are interchanged in M, or (ii) $\overline{L} \cong SL_2(5)$. Let $T = S \cap LK$.

First consider case (i). If x is an element of order 4 in $C(\overline{L}_1)$ either centralizing or inducing an outer automorphism of order 2 on $\overline{L}_2$, then let x_1 be an element of order 4 in $L_1 \cap S$ and $X = \langle z, xx_1 \rangle$. Then X is a 4-group and $\overline{L}_2 = \langle C_{\overline{L}_2}(X^t) : t \in T \rangle \leq \overline{H}$. So $\overline{SL} = \langle \overline{L}_2, \overline{S} \rangle \leq \overline{H}$ and then $\overline{M} = \overline{L} N_{\overline{M}}(\overline{T}) \leq \overline{H}$, a contradiction. So $|S:T| \leq 4$.

Now choose $y \in S - L$ to be an element of order 4 inducing an automorphism of order 2 on $\overline{L}$. If possible choose y to induce an outer automorphism of order 2 on each $\overline{L}_i$. If this is not possible then $|S:T| = 2$ and choose y to interchange L_1 and L_2. As T contains all involutions in S, 2.2 implies there exists $y^g \in S - yT$. Let $(y^g)^2 = t$. If $t = z$ then $g \in M$, impossible as $LK\langle y \rangle \trianglelefteq M$. So $t \neq z$ and then as t is not rooted in T, $|S:T| = 4$, and y^g interchanges L_1 and L_2. By Alperin's theorem on fusion we may choose $g \in N(U)$, where $\langle y, y^g \rangle \leq U \leq S$. As $z \in Z(U)$, $t = z^g \in Z(U)$ and then even $\Omega_1(Z(U)) = V = \langle t, z \rangle$. Thus as $C_G(V)$ has a normal 2-complement, we may assume $U = C_S(V)$. But now g normalizes $\Omega_1(U) = C_T(V) \cong Z_2 \times D_8$, and then also $\mho^1(C_T(V)) = \langle a \rangle$.

Next consider case (ii). M is exceptional so $m(M) \geq 3$ and then $T = (T \cap L)YQ$ with $T \cap L$ and Q quaternion. If $T \neq S$ then we find $y \in S - T$ with $y^2 = z$ and argue as in case (i) that $y^G \cap T$ is empty, so that 2.2 yields a contradiction. So $T = S$. By the Z^*-theorem, z is fused to some $t \neq z$ in T. But for each choice of t, z is rooted in $C_T(t)$ while t is not, a contradiction.

Lemma 2.6. *Let G be fusion simple and u an involution not in the center of any Sylow 2-subgroup of G. Assume $M = C_G(u)$ is exceptional. Then $\overline{M} = M/O(M)$ has a normal subgroup isomorphic to $L_2(q)$, $Sz(q)$, or $U_3(q)$, $q > 2$ even.*

Proof. If M is not as claimed then u is the unique involution in the center of a Sylow 2-subgroup of M. But this contradicts the hypothesis that u is not in the center of a Sylow group of G.

A group G is said to be *quasisimple* if G is perfect and $G/Z(G)$ is simple. G is *semisimple* if G is the central product of quasisimple groups. Finally the components of a group G are the quasisimple factors of the unique maximal semisimple subgroup $E(G)$ of G.

Lemma 2.7. *Let G be a group with $O(G) = 1$ and a proper 2-generated core. Assume all the components of G are either 2-generated or known. Then G is known.*

Proof. For $m(G) \geq 3$ see Proposition 3′ in [7]. For $m(G) < 3$ see Theorem 2.4. Recall that G is *known* if it is one of the groups in the conclusion of Theorem 1.

Lemma 2.8. *Let G be a solvable group, S a Sylow 2-subgroup of G, and k a positive integer. Assume $H = \Gamma_{S,k}(G) \neq G$. Then $m(G) \leq k$.*

Proof. Assume G is a counterexample. Let Q be maximal with respect to $Q \leq H$ and $Q \trianglelefteq G$. Let K/Q be minimal normal in G/Q, and E an elementary 2-subgroup of S of rank $k + 1$. Set $\overline{G} = G/Q$. $\overline{K}$ is a p-subgroup for some prime p, and as H contains a Sylow 2-subgroup of G, $p \neq 2$. Further $m(Q) \leq k - 1$, so $m(\overline{E}) \geq 2$. Thus

$$\overline{K} = \langle C_{\overline{K}}(\overline{X}) : m(\overline{X}) = m(\overline{E}) - 1 \rangle.$$

It follows that $K \leq \Gamma_{S,k}(G)Q = H$, contradicting the choice of Q.

Lemma 2.9. *Let H be strongly embedded in G, let z be an involution in H, and represent G on the set Ω of cosets of H in G. Assume $E(G/O(G))$ is a Bender group and P is a p-subgroup of H fixing 3 or more points of Ω with $P \cap O(G) \in \mathrm{Syl}_p(O(G))$. Then $z^H \cap N(P)$ is nonempty.*

Proof. As $O(G) = G_\Omega$, we may assume G acts faithfully on Ω. Then G is an extension of a Bender group so a Sylow 2-subgroup Q of H is normal in H and regular on $\Omega - \{H\}$. Then $C_Q(P)$ is transitive on $F(P) - \{H\}$, so as $|F(P)| \geq 3$, $C_Q(P) \neq 1$. Finally each involution in $C_Q(P)$ is in z^H.

3. Proof of Theorem 1. In this section G is a minimal counterexample to Theorem 1.

Lemma 3.1. $O(G) = 1$. $m(G) \geq 3$.

Proof. Assume $K = O(G) \neq 1$. Then either $G = HK$ or G/K satisfies the hypothesis of Theorem 1. In the first case let S be a Sylow 2-subgroup of G. Then $\Gamma_{S,2}(KS) < KS$, so by 2.8, $m(G) = m(KS) \leq 2$, so G is known.

In the second case minimality of G implies G/K, and thus also G, is known. Theorem 2.4 implies $m(G) \geq 3$.

Lemma 3.2. G is quasisimple.

Proof. If not minimality of G implies all components of G are either 2-generated or known. Thus 2.7 implies G is known.

Theorem 3.3. *G is simple.*

Until the proof of Theorem 3.3 is completed, we assume $E = Z(G) \neq 1$. As $G = C_G(E) \nleq H$, $m(E) = 1$. Let e be the involution in E. Set $\overline{G} = G/\langle e \rangle$.

Lemma 3.4. $E = \langle e \rangle$.

Proof. E has 2-rank 1 and is in the center of G, so $E = \langle x \rangle$ is cyclic. Suppose $x \neq e$. A Sylow 2-subgroup T of $H \cap H^g$ is cyclic or quaternion for $g \in G - H$. Further $E \leq T$, so as $e \neq x \in Z(T)$, T is cyclic. Thus $\overline{H} \cap \overline{H}^g$ has cyclic Sylow 2-subgroups for all $\overline{g} \in \overline{G} - \overline{H}$, so $\overline{G}$ satisfies the hypothesis of Theorem 1. Thus $\overline{G}$, and therefore G, is known.

Let S be a Sylow 2-subgroup of G contained in H.

Lemma 3.5. S *contains a normal 4-group* $\langle e, z \rangle$. $C_{\overline{G}}(\overline{z}) \leq \overline{H}$, *and* $\overline{H}$ *controls fusion in* $\overline{S}$.

Proof. By 3.1, $m(G) \geq 3$, so the normal 4-group exists. Then $C_{\overline{G}}(\overline{z}) = N_G(\langle e, z \rangle) \leq \overline{H}$. $\overline{H}$ controls fusion in $\overline{S}$ by 2.3 and 4.1.

For the remainder of the proof of Theorem 3.3 let $\overline{u}$ be an involution in $\overline{H}$ with $\overline{M} = C_{\overline{G}}(\overline{u}) \nleq \overline{H}$. Then $\overline{u}$ is the image of an element u of order 4, and M is the normalizer of the subgroup generated by u.

Lemma 3.6. *We may choose* u *so that* M *contains a normal subgroup* L *with* $L/O(L) \cong SL_2(5)$.

Proof. Let $S_1 = C_S(z)$. $|S : S_1| \leq 2$. If $u^G \cap S_1$ is empty, then considering the transfer of G to S/S_1, G has a subgroup of index two, contradicting 3.2. Thus we may assume $z \in C_S(u)$. (Recall $\overline{H}$ controls fusion in $\overline{S}$.)

Suppose $m(M) \leq 2$. As $\langle u \rangle$ is normal in M, minimality of G implies either M is known of type (v) or $M = (M \cap H)O(M)$. Thus we may assume M is of the latter type. Set $X = O(M)$. Then $X \nleq H$.

Claim $\langle \overline{z}^{\overline{G}} \cap \overline{M} \rangle \leq \overline{X}\langle \overline{z} \rangle$. For assume not. Let $T \geq S \cap M$ be Sylow in M. Then there exists an involution $t \in T$ with $t \neq z$ or ze. $m(T) = 2$, so we may assume $\langle t, z \rangle$ is dihedral of order 8. z inverts tz, so $tz \neq u$. Also $(tz)^2 = e$ so $X = C_X(t)C_X(z)C_X(tz)$. $\langle C_X(z), C_X(t) \rangle \leq H$ and $X \nleq H$, so $C_X(tz) \nleq H$. Suppose $tz \in C(u)$. Then as $tz \neq u$, $\langle tz, u \rangle$ contains a 4-group A and $C_X(tz) = C_X(A) \leq H$ as $m(A) = 2$. So $tz \notin C(u)$. Thus $\langle z, e \rangle = \Omega_1(C_T(u))$, and we may choose $T \leq S$. As $m(G) > 2$, T is of index 2 in some $R \leq S$. As $|S : S_1| = 2$ we can choose $r \in (R - T) \cap C(z)$. Set $v = u^r$. As $r \in C(z)$, if any two of $C_T(w)$, $w = u, v, z$, are equal, then all are equal. In that case, as $m(T) = 2$, $\langle u, v \rangle = \langle u, z \rangle$ and $uz \in u^G$. But $t^z = te = t^u$, so $\langle t, z \rangle \leq C_S(uz)$, contradicting $\Omega_1(C_S(u)) = \langle z, e \rangle$.

Thus $C_T(u)$, $C_T(v)$, and $C_T(z)$ are all distinct. But as each has index two in T, T is the union of the three groups. Thus t lies in one of the three, a contradiction.

Next assume $m(M) \geq 3$. Then minimality of G implies M is exceptional. As $|O_2(M)| \geq 4$, M has a normal subgroup L with $L/O(L) \cong L_2(q)$, $Sz(q)$, $U_3(q)$, $S\hat{z}(8)$, or $SL_2(5)$. Further, except in the last case, EL contains all involutions in M, so that $\langle \overline{z}^{\overline{G}} \cap \overline{M} \rangle \cap \overline{H}$ is strongly embedded in $\langle \overline{z}^{\overline{G}} \cap \overline{M} \rangle = \overline{L}$.

Therefore if no involution $\overline{u}$ exists with M as claimed, then $\overline{G}$ satisfies the hypothesis of Theorem 2. So as $\overline{G}$ is simple by 3.2 and 3.4, Theorem 2 implies $\overline{H}$ is strongly embedded in $\overline{G} = \langle \overline{z}^{\overline{G}} \rangle$. Thus $\overline{G}$, and therefore also G, is known. So we may choose u as claimed.

We now complete the proof of Theorem 3.3 by showing $G \cong \hat{A}_9$.

Let u be the element which exists by 3.6, and L the normal subgroup of M with $L/O(L) \cong SL_2(5)$. Set $K/O(M)$ equal to the centralizer of $LO(M)/O(M)$ in $M/O(M)$. K has 2-rank 1 and LK contains all involutions in M. Let T be Sylow in M and let $Q = T \cap L$. Then Q is quaternion of order 8, and $T = PQ$ where $P \cap Q = E$ and $m(P) = 1$. Further $P_1 = P \cap K$ has index at most two in P. T contains a conjugate of z, which lies in $P_1 Q - Q$, so $P_1 \neq \langle E \rangle$.

Suppose P is cyclic. $u \in P$ and $P_1 \neq \langle E \rangle$, so $u \in P_1 = Z(T)$. Thus $\langle u \rangle$ is characteristic in T and then $T \in \mathrm{Syl}_2(G)$. But as P_1 is cyclic, $m(T) = 2$. So P is quaternion.

Suppose $P = P_1$. If $|P| > 8$ then u is contained in $\mho^1(T)$, which is cyclic, so again $T = S$. In this case $\overline{S}$ is nonabelian dihedral cross a 4-group, and [5] implies $\overline{G}$ is not simple. So $|P| = 8$, and we may assume $T = N_S(P)$. As $\overline{G}$ has at least two classes of involutions, [10] implies $\overline{S}$ is not abelian, so $T \neq S$. So there exists $x \in S - T$ with $P^x = Q$ and $x^2 \in T$. T is characteristic in $\langle T, x \rangle$, so as $T = N_S(P)$, we get $S = \langle T, x \rangle$. As $\overline{G}$ has no subgroup of index two we may assume $\overline{x}$ is an involution. But now Lemma 8.5 of [4] implies $\overline{G}$ has a subgroup of index two.

Thus $P \neq P_1$. If $|P| > 16$ then $u \in \mho^2(T)$, which is cyclic, so $T = S$ and $\overline{G}$ has a subgroup of index two. If $|P| = 8$ then $\overline{T} = \langle \overline{u} \rangle \times \overline{D}$ where $\overline{Q} \leq \overline{D}$ is dihedral of order 8. Let $\langle \overline{v} \rangle = Z(\overline{D})$. Then uv is an involution, so $\overline{u}\,\overline{v} \notin \overline{u}^{\overline{G}}$. Thus $T = S$ and $\overline{G}$ has a subgroup of index two. So P has order 16.

Then $\overline{T} = (\overline{P}_1 \times \overline{Q})\langle \overline{y} \rangle$ with $\overline{y}$ an involution and $\overline{P} = \langle \overline{P}_1, \overline{y} \rangle$ and $\langle \overline{Q}, \overline{y} \rangle$ dihedral of order 8. If $T = S$ then Lemma 8.5 of [4] implies $\overline{G}$ has a subgroup of index two. So let $x \in S - T$ with $x^2 \in T$. $P_1 Q$ is characteristic in T, so $P_1^x = Q$. Further either we may choose $x^2 = y$, or x^2 centralizes $\overline{P_1 Q}$ and we can choose $\overline{x}$ to be an involution commuting with $\overline{y}$. In any case $\overline{P_1 Q}$ is the unique normal

abelian subgroup of $\langle \overline{x}, \overline{T} \rangle$ of rank 4, so $\overline{P_1 Q}$ is characteristic in $\langle \overline{x}, \overline{T} \rangle$. Therefore as $\overline{T} = N_{\overline{S}}(\overline{P}_1)$ and P_1 and Q are the only conjugates of Q in T, $S = \langle T, x \rangle$.

Suppose $y = x^2$. As $\overline{G}$ has no subgroup of index two, $\overline{y} \in \overline{u}^{\overline{G}}$. But $\overline{u}^{\overline{x}} = \overline{uz}$, while for any $w \in S$ with $w^2 = u$, $\overline{y}^{\overline{w}} = \overline{yu}$, a contradiction. Thus we can choose $\overline{x}$ to be an involution commuting with $\overline{y}$. So $\overline{S}$ is isomorphic to, and has the fusion pattern of a Sylow group of A_9. Further the centralizer $\overline{M}$ of a noncentral involution $\overline{u}$ has an A_5 section. It follows from Theorem A of (3) that $\overline{G} \cong A_9$. Therefore $G \cong \hat{A}_9$.

This completes the proof of Theorem 3.3.

Let z be an involution in the center of a Sylow 2-subgroup S of G contained in H. If $C_G(z) \not\leq H$, then minimality of G and 3.5 imply $C_G(z)$ is exceptional. But then Theorem 2.1 yields a contradiction. Thus we have shown:

Lemma 3.7. $C_G(z) \leq H$.

Lemma 3.8. *Let u be an involution in H with $M = C_G(u) \not\leq H$. Then $\langle z^G \cap M \rangle \cap H$ is strongly embedded in $\langle z^G \cap M \rangle$.*

Proof. As H controls fusion of its involutions, we may let $T \leq S$ be a Sylow group of M. Suppose $m(T) = 2$. Then as $z \in Z(S)$, $\langle u, z \rangle = \Omega_1(T)$. The Z^*-theorem implies $uz \in u^G$, and therefore $\langle z^G \cap M \rangle \leq Z^*(M)$. Next assume $m(T) \geq 3$. Then minimality of G implies M is exceptional so 2.2 implies M has a normal subgroup L with $L/O(L) \cong L_2(q)$, $Sz(q)$, or $U_3(q)$, q even. Let $K/O(M)$ be the centralizer in $M/O(M)$ of $LO(M)/O(M)$. Set $R = T \cap L$ and $U = K \cap T$. Then UR contains all involutions in T and U has 2-rank one. Further $N_L(R)$ is transitive on $R^{\#}$: So T has three M-classes of involutions: $\{u\}, \{z^L\}$ and $\{(uz)^L\}$. The Z^*-theorem implies $uz \in u^G$. Thus $H \cap L$ is strongly embedded in $L = \langle z^G \cap M \rangle$.

Now 3.7, 3.8, and Theorem 2 imply that H is strongly embedded in $G = \langle z^G \rangle$. So [2] implies G is known.

This final contradiction completes the proof of Theorem 1.

4. Preliminaries to Theorem 2.

Hypothesis 1. *G is a finite group, H a proper subgroup of G, and z an involution in H. Further*

(i) *if $z \in H^g$ then $g \in H$, and*

(ii) *if u is an involution with $z \in M = C_G(u) \not\leq H$ then $\langle z^G \cap M \rangle \cap H$ is strongly embedded in $\langle z^G \cap M \rangle$.*

Set $\Omega = \{H^g : g \in G\}$ and let G act on Ω by conjugation.

Hypothesis 2. *G satisfies Hypothesis 1 and z is in the center of some Sylow 2-subgroup of G.*

Lemma 4.1. *Let G be a finite group, $H \leq G$ and z an involution in H. Then the following are equivalent:*

(1) *If $z \in H^g$ then $g \in H$.*

(2) *$C_G(z) \leq H$ and $z^G \cap H = z^H$.*

Proof. Assume (1), and let $g \in C_G(z)$. Then $z \in H^g$, so $g \in H$. Thus $C_G(z) \leq H$. If $z^x \in H$ then $z \in H^{x^{-1}}$ so $x \in H$. Thus $z^G \cap H = z^H$. Next assume (2). $z \in H^g$ implies $z^{g^{-1}} \in H$, so $z^{g^{-1}} = z^h$ for some $h \in H$. Thus $hg \in C_G(z) \leq H$. So $g \in H$.

Lemma 4.2. *Assume Hypothesis 1. Let $t, s \in z^G$ and u an involution with $z \in C_G(u) \nleq H$. Then:*

(1) *$uz \notin z^G$.*

(2) *If tz has even order then $t \in H$.*

(3) *If $1 \neq ts \in C_G(z)$ then t and s are in H.*

Proof. If $uz \in z^G$, then $u \in \langle z^G \cap C(u) \rangle = L$. But by hypothesis $H \cap L$ is strongly embedded in L, so L has one class of involutions, a contradiction. Next assume tz has even order, and let v be the involution in $\langle tz \rangle$. Then $t, z \in C(v)$. So if $C(v) \leq H$ then $t \in H$, while if $C(v) \nleq H$ then $t, z \in L = \langle z^G \cap C(v) \rangle$ and $H \cap L$ is strongly embedded in L, yielding a contradiction as above. Finally assume $1 \neq ts \in C_G(z)$, with $t \notin H$. Then as above, $x = ts$ has odd order. So $x^t = x^{-1} \neq x$ while $x^z = x$, so t is not conjugate to z in $\langle C_G(x), t \rangle$. Thus tz has even order, so (2) yields a contradiction.

Lemma 4.3. *Assume Hypothesis 1. Let $m = |z^H|$, $\alpha, \beta \in \Omega$, $H = G_\alpha$, and $D = G_{\alpha\beta}$. Then*

(1) *there are exactly m elements $t \in z^G$ with cycle (α, β).*

Assume Hypothesis 2 and let $t \in z^G$ have cycle (α, β), and set $D^* = \langle D, t \rangle$. Then:

(2) *$t \in Z^*(D^*)$.*

(3) *Let $K = \{x \in O(D): x^t = x^{-1}\}$. Then $H = C_G(z)K$ and $|K| = m$.*

Proof. Let t_i, $1 \leq i \leq k$, be the elements of z^G with cycle (α, β). Suppose $t_i t_j \in C_G(z)$ for $i \neq j$. Then by 4.2, $t_i \in H$, a contradiction. Thus the elements $k_i = t_1 t_i$, $1 \leq i \leq k$, are distinct modulo $C_G(z)$. So $k \leq |H : C_G(z)| = |z^H| = m$ by 4.1. Set $n = |\Omega|$. Then $|z^G| = mn$, so $|z^G - H| = (n - 1)m$. But we have shown that $k = |Hx \cap z^G| \leq m$ for any coset $Hx \neq H$. So $k = m$.

Now assume Hypothesis 2, and set $t = t_1$, and $s = t_2$. Let $t \in H_1 = H^g$. If $[t, s] = 1$, then $u = ts \in H$ and $t \in M = C(u)$. As z is in the center of a Sylow group of G and $u \in H$, we may assume $z \in M$, contradicting the remarks above.

Thus t commutes with no conjugate in D^*, so the Z^*-theorem implies $t \in Z^*(D^*)$. Thus $K = \{k_i : 1 \leq i \leq m\}$. We showed above that $H = C_G(z)K$ and $|K| = m$.

Lemma 4.4. *Assume Hypothesis 2 and let $K \leq G$. Then:*

(1) *If K is a normal subgroup of G of odd order then either $G = HK$ or G/K satisfies Hypothesis 2.*

(2) *If $z \in K \nleq H$ then K satisfies Hypothesis 2.*

Proof. The proof of (1) is straightforward. Let K satisfy the hypothesis of (2). Set $J = H \cap K$. Clearly $z \in J^k$ implies $k \in J$. Let u be an involution in K with $z \in M = C_K(u) \nleq J$. Then $C_G(u) \nleq H$, so $L \cap H$ is strongly embedded in $L = \langle z^G \cap C(u) \rangle$. $V = \langle z^K \cap M \rangle \leq L$. $M \nleq J$ so let $x \in M - J$. Then $z^x \in J^x \neq J$, so $z^x \notin J$. Thus $V \nleq J$. So $V \cap J$ is strongly embedded in V. Therefore K satisfies Hypothesis 1 and it remains to show z is in the center of some Sylow group of K. Set $a = |a^K|$ and $b = |z^J|$. z is contained in a unique conjugate of J, so a is odd and $|z^K| = ab$. By 4.3 b is the order of Γ, the set of elements in z^K with cycle (α, β). Further $\Gamma \leq Z^*(D^*)$, so $b = |X : C_X(t)|$ is odd, where $t \in \Gamma$ and $X = O(\langle\langle \Gamma \rangle\rangle)$. Thus $|z^K| = ab$ is odd, so z is in the center of a Sylow group of K.

For the remainder of this paper let $m = |z^H|$, let $\alpha, \beta \in \Omega$ with $H = G_\alpha$ and $D = G_{\alpha\beta}$, let $t \in z^G$ have cycle (α, β), let $D^* = \langle D, t \rangle$, and set $n = |\Omega|$.

Lemma 4.5. *Assume Hypothesis 2, and let p be a prime. Then:*

(1) *t normalizes a Sylow p-subgroup P of D, and $|t^P| = m_p$.*

(2) *Assume $[P, t]$ fixes 3 or more points of Ω and let M be a p-subgroup of G maximal with respect to fixing 3 or more points and being normalized by some $s \in z^G$ with $|s^M| = m_p$. Then s fixes a point of $\Delta = F(M)$.*

Proof. (1) follows from the fact that $t \in Z^*(D^*)$, 4.3, and 2.1. Assume (2) is false and let M be a counterexample. Clearly p is odd. We may assume $\alpha \in \Delta$ and $t \in N(M)$. Set $N = N_G(M)$, $L = \langle t^N \rangle$, $\{\gamma\} = F(t)$, and $H_1 = G_\gamma$. The proof involves several reductions.

(i) $t \in Z^*(N)$: Suppose $s \in t^N$ with $[s, t] = 1$. By 4.2, H_1 covers t, s, and ts. Let $A = M_\gamma$ and $B = N_M(A)$. As $\gamma \notin \Delta$, $B \nleq A$. But as H_1 covers t, s, and ts, $B = C_B(s)C_B(t)C_B(ts) \leq A$. Therefore by Glauberman's Z^*-theorem, $t \in Z^*(N)$.

(ii) Let $\alpha \neq \delta \in \Delta$. Then $\alpha^s = \delta$ for some $s \in t^N$: Assume $\delta \neq \alpha^s$ for any $s \in t^N$. Let Q be a Sylow group of $G_{\alpha\delta}$ containing M. $Q \neq M$ by (1). Further, maximality of M implies $F(Q) = \{\alpha, \delta\}$. Then $|\Delta| \equiv n \equiv |F(Q)| \equiv 2 \bmod p$. As $t \in Z^*(N)$, t normalizes a Sylow p-subgroup R of N, which we may assume contains $N_Q(M)$. As $|\Delta| \equiv 2 \bmod p$, R fixes 2 or more points σ and σ^t of Δ. $m_p = |t^M| \leq |t^R|$ by (1), so $[R, t] \leq M$. Thus t centralizes R/M and then normalizes $N_Q(M)$.

Maximality of M implies $\{\sigma, \sigma^t\} = F(N_Q(M)) = \{\alpha, \delta\}$. So $\alpha^t = \delta$.

(iii) $O(L) \leq H$: If $x \in O(L) - H$ then by (ii) there exists $s \in t^N \cap (H \cap L)x$, so $s \in O(L)$.

We now derive a contradiction and establish 4.5. For it follows from (i) and (iii) that $\alpha^L = \{\alpha, \beta\}$ has order 2, contradicting (ii).

Lemma 4.6. *Let p be a prime, and set $\gamma = \beta^z$. Then D_γ contains a Sylow p-subgroup of D if and only if z normalizes a p-subgroup X of D with $|z^X| \geq m_p$.*

Proof. Let S be a z-invariant Sylow group of D_γ containing X. Then $|S : C_S(z)| \geq m_p = |D : C_D(z)|_p$ by 4.3. Further $C_D(z) \leq D_\gamma$, so $|C_D(z)|_p = |C_S(z)|_p$. Thus $|S| = |D|_p$. The converse follows from 4.5.1.

Lemma 4.7. *Assume Hypothesis 2. Let p be an odd prime and P a maximal p-subgroup of H fixing 2 or more points. Then either*

(1) $\Delta = F(P)$ has order 2 and G^Ω is doubly transitive, or

(2) $N_G(P)^\Delta$ is transitive and $z^G \cap N_H(P)$ is nonempty.

Proof. Assume first Δ has order greater than 2. Then maximality of P implies P is Sylow in $G_{\alpha\beta}$ for all $\beta \in \Delta$, so by 4.5.1 there exists $t \in z^G \cap N(P)$ with cycle (α, β). Thus $N(P)^\Delta$ is transitive and by 4.5, if $P \leq H$ then $z^G \cap N_H(P)$ is nonempty.

So assume Δ has order 2. If a Sylow p-subgroup of $G_{\alpha\beta}$ fixes exactly 2 points for every $\beta \in \Omega - \{\alpha\}$ then G^Ω is doubly transitive. So choose β so that a Sylow p-subgroup Q of D fixes 3 or more points. By 4.5, $Q^t = Q$ for some $t \in z^G$ with cycle (α, β). Choose M maximal in the sense of 4.5, and containing Q. Set $\Gamma = F(M)$ and $N = N_G(M)$. 4.5 implies there exists $t \in z^G \cap N$ fixing a point $\gamma \in \Gamma$. Let R be a Sylow p-subgroup of G_γ containing M. As $|\Delta| = 2$, R fixes exactly two points, γ and δ. Let S be a t-invariant Sylow group of $G_{\gamma\delta}\delta^t$ containing M. Then $K = \{k \in M : k^t = k^{-1}\} \subseteq S$ and has order m_p by choice of M. Therefore $|S : C_S(t)| \geq m_p$, so by 4.6, S is Sylow in $G_{\gamma\delta}$. But a Sylow group R of $G_{\gamma\delta}$ fixes only 2 points, a contradiction.

Lemma 4.8. *Assume Hypothesis 2. Let $E = D_\beta z$. Then $D = O(D)E$ and $O(E) \leq O(D)$.*

Proof. By 4.3, $D = C_D(z)O(D)$. But $C_D(z) \leq E$.

Lemma 4.9. *Assume Hypothesis 2 with $G = HO(G)$. Then $z \in Z^*(G)$.*

Proof. Set $X = O(G)$. Suppose $w \in z^G$ centralizes z. Then $C_G(w)$ and $C_G(z)$ are contained in H. Also by 4.2, $C_G(wz) \leq H$. Thus $X = C_X(z)C_X(w)C_X(wz) \leq H$,

so $G \leq H$, a contradiction. Thus the Z^*-theorem implies $z \in Z^*(G)$.

5. Proof of Theorem 2. For the remainder of this paper G is a minimal counterexample to Theorem 2. Define α, β, D, etc. as in §4. Let $E = D_\beta z$.

Lemma 5.1. *G is simple.*

Proof. Minimality of G, 4.4, and 4.9, imply $O(G) = 1$. Similarly $G = \langle z^G \rangle$. Suppose $1 \neq O_2(G) = Q$. By hypothesis z is in the center of a Sylow 2-subgroup of G, so z centralizes Q. Thus $G = \langle z^G \rangle$ centralizes Q. Let u be an involution in Q. Then $C_G(u) = G \nleq H$, so by hypothesis H is strongly embedded in $G = \langle z^G \rangle$. Thus $O_2(G) = 1$.

Let M be a minimal normal subgroup of G. If $z \in M$, then $M = G$ is simple. So assume $z \notin M$. Let S be a Sylow 2-subgroup of M. If $M \leq H$, let $t \in z^G - H$, and $M_1 = \langle z, t, M \rangle$. Set $K = N_{M_1}(S)$. We may assume $z, t \in K$, so minimality of G implies $z \in Z^*(K)$. Therefore $\langle z, S \rangle = S_1$ is Sylow in M_1 and $z^G \cap S_1 = \{z\}$. Thus the Z^*-theorem implies $z \in Z^*(M_1)$ and so $[z, M] = 1$. Therefore M is in the center of G, a contradiction.

So $M \nleq H$. If $G \neq \langle M, z \rangle$, then minimality of G implies $H \cap \langle z^M \rangle$ is strongly embedded in $\langle z^M \rangle$. But $\langle z^M \rangle$ has a subgroup of index 2, so again $[M, z] = 1$, a contradiction. So $G = \langle M, z \rangle$.

Let u be an involution centralizing z with $C_G(u) = C \nleq H$. Such an involution exists by [2]. If $t \in z^G$ then $tz \in M$, so $tz \notin z^G$. Thus $z \in Z^*(C)$. Let v be an involution in $C \cap M$ in the center of a Sylow group S of G containing z. If $v = u$ then $S \leq C$ and $z^G \cap S = \{z\}$, so $z \in Z^*(G)$, a contradiction. Thus $C_G(v) \leq H$. Set $X = O(\langle z^C \rangle)$. Let $A \leq X \cap H$ be maximal with respect to being normal in C, and B/A be a minimal normal subgroup of C/A contained in X. Then $B \nleq H$. But $C_B(v)$ and $C_B(z)$ are contained in H. Thus $C_B(vz) \nleq H$. But vz is in the center of S, yielding a contradiction as above.

Lemma 5.2. *Either $G = \langle z, t, [t, O(D)] \rangle$, or the following hold:*

(i) *$\langle z^H \rangle$ is abelian and $[t, O(D)]$ is cyclic.*

(ii) *If p is a prime divisor of m then a Sylow p-subgroup of G fixes exactly two points.*

(iii) *$E = C_D(z)$.*

Proof. Set $K = \langle z, t, [t, O(D)] \rangle$, and assume $K \neq G$. Then minimality of G implies $H \cap K$ is strongly embedded in K. By 4.3, $z^H = z^{[t, O(D)]} \subseteq K$. Let $B = \langle [a, b]: a, b \in z^H \rangle$. As $H \cap K$ is strongly embedded in K and $z \notin Z^*(G)$, $B \leq O(D)$. Clearly $B \trianglelefteq H$. If G^Ω is doubly transitive then $B \leq G_\Omega = 1$ by 5.1, so $\langle z^H \rangle$ is abelian. Then $[E, z] \leq \langle z^H \rangle \cap E = 1$, so $E = C_D(z)$. If a Sylow p-subgroup P of

$[t, O(D)]$ fixes 3 or more points, then by 4.5, P normalizes the conjugate Q of $\langle z^H \rangle$ containing t, so $P = [P, t] \leq Q$, a contradiction. So we may assume G^Ω is not doubly transitive and therefore by 4.7, for any prime p, some Sylow p-subgroup P of D is contained in a z invariant p-subgroup M of H fixing 3 or more points. $[z, MB/B] = 1$, so z normalizes PB. Thus $P \leq PB \leq E$. So $D \leq E$ and therefore $D = D^z$. So $z^H \subseteq Z^*(\langle D, z \rangle)$ by 4.3. Thus the Z^*-theorem implies $z \in Z^*(G)$, a contradiction.

Theorem 5.3. *Let p be a prime divisor of m. Then a Sylow p-subgroup of G fixes exactly two points.*

For the remainder of this section assume p is a counterexample to 5.3. $D = G_{\alpha\beta}$ is said to be *p-admissible* if for some $a \in z^H$, $D_\beta a$ contains a Sylow p-subgroup of D. By 4.7, p-admissible intersections exist.

For $X \leq G$ set $\theta(X) = O_\pi(X)$ where $\pi = \{2, p\}'$.

Lemma 5.4. *Let D be p-admissible. Then $\theta(D) \neq 1$.*

Proof. Let P be a Sylow p-subgroup of $O(D)$ contained in E. By 4.8, P is Sylow in $O(E)$, so as z normalizes $O(E)$ we may assume $P^z = P$. As P is Sylow in $O(D)$ we may assume $P^t = P$. Assume $\theta(D) = 1$. Then the ZJ-theorem implies $R = Z(J(P)) \trianglelefteq O(D)$. As R is characteristic in P, $R^z = R = R^t$. Thus by 5.2, $G = \langle z, t, O(D) \rangle \leq N(R)$, a contradiction.

Lemma 5.5. *Let D be p-admissible. Then $|\theta(D)| > |\theta(E)|$.*

Proof. As $O(E) \leq O(D)$, $O(D)$ is solvable, and E contains a Sylow p-subgroup of D, it follows by [9] that $\theta(E) \leq \theta(D)$. So if $|\theta(D)| \leq |\theta(E)|$ then $\theta(D) = \theta(E)$. But then as above $G \leq N(\theta(D))$.

Lemma 5.6. *Let X be a p-subgroup of H normalized by z and Y a p'-subgroup of odd order of G normalized by $\langle X, z \rangle$ with $Y \nleq H$. Set $K = \{k \in X : k^z = k^{-1}\}$. Then $C_Y(K) \nleq H$.*

Proof. Let A_1 be maximal with respect to $A_1 \trianglelefteq H \cap Y$ and $A_1 \trianglelefteq W = \langle X, Y, z \rangle$. Let B/A_1 be a minimal normal subgroup of W/A_1 contained in Y/A_1, and set $A = H \cap B$. Then $A \triangleleft B$ and z inverts $B/A = \bar{B}$. By 1.5, $[K, \bar{B}] = 1$, so $C_B(K) \nleq A = B \cap H$.

We are now in a position to derive a contradiction, thus establishing Theorem 5.3.

Let D be a p-admissible intersection with $|\theta(D)|$ minimal. Let P be a Sylow p-subgroup of $O(D)$ contained in E. We may assume $P^t = P = P^z$ as in 5.4. Set $F = G_{\beta\beta}z$. $F = O(F)C_F(z) = O(F)E$, so $O(E) \leq O(F)$. As $C_D(z) = C_E(z) = C_F(z)$,

$|E|_p = |C_D(z)|_p m_p = |C_F(z)|_p m_p |F|_p$. Then E contains a Sylow p-subgroup of F, so by [9] $\theta(E) \leq \theta(F)$. P fixes α, β^{zt}, and β^{ztz}. Thus F^t is p-admissible, so minimality of $|\theta(D)|$ implies $|\theta(D)| \leq |\theta(F^t)| = |\theta(F)|$. By 5.5, $|\theta(E)| < |\theta(D)| \leq |\theta(F)|$, so $\theta(F) \not\leq E$. That is $\theta(F) \not\leq H$. Let $K = \{k \in P: k^z = k^{-1}\}$. By 5.6, $M = C_G(K) \not\leq H$.

Set $L = \langle z^M \rangle$. Minimality of G implies $L \cap H$ is strongly embedded in L. As $L \cap M$ is a subgroup of index 2 in L, L is solvable and $O(L) = L \cap M$. Let $X \trianglelefteq L \cap H$ with $L \cap H = X(C(z) \cap L \cap H)$. $N_L(X) \not\leq H$ (e.g. 4.6 in [2]) so there exists $s \in z^{N_L(X)} - H$. Set $A = H \cap H^s$ and choose s with $|\theta(A)|$ maximal. Let $s \in H_1 = G_\gamma$. $s \in z^{N_L(X)}$, so $\gamma \in \alpha^{N_L(X)}$.

Let $B = G_{\alpha\gamma}$. $K \subseteq A \cap B$, so by 4.6, B is p-admissible. By 5.5, $|\theta(A \cap B)| < |\theta(B)| \leq |\theta(A)|$. Therefore $\theta(A) \not\leq H_1$. Then by 5.6, $C_A(K) \not\leq H_1$.

But s normalizes K and A, so s normalizes $Y = C_A(K)$. Also $[z, (L \cap H)/X] = 1$ and $X \leq Y \leq M \cap H$, so z normalizes Y. Therefore minimality of G implies z is conjugate to s in $N_G(Y)$, so $\gamma \in \alpha^{N_G(Y)}$. Thus as $Y \leq H$, we also have $Y \leq H_1$. But it was shown in the last paragraph that $Y \not\leq H_1$.

This completes the proof of 5.3.

6. The centralizer of z.

Theorem 6.1. *G^Ω is doubly transitive.*

Proof. 4.7 and 5.3.

Lemma 6.2. *Let p be an odd prime, P a Sylow p-subgroup of E with $z \in M = N_G(P)$. Set $\Delta = F(P)$. Then*

(1) *G is transitive on triples $(\gamma, \delta, \delta^s)$ such that $s \in z^G$ and s fixes γ.*

(2) *M^Δ is transitive and $t^D \cap M$ is nonempty.*

(3) *If p divides m then M^Δ is 2-transitive and P is maximal among p-subgroups of G fixing 3 or more points.*

Proof. (1) As G is 2-transitive we may take $\gamma = \alpha$ and $\delta = \beta$. Then $s \in z^G \cap H = z^D$ and the result holds.

(2) We may assume P is not Sylow in D, so a Sylow p-subgroup Q of $M_{\beta\beta^z}$ properly contains P. Thus as P is Sylow in E, $N_Q(P) = R \not\leq H$. So there exists $s \in z^R - H$. Let $\{\gamma\} = F(s)$, and $(\gamma, \alpha)^g = (\alpha, \beta)$. Then $P^g \leq D$ and $s^g \in z^G \cap H = z^D$. So we may assume $s^g = z$. Thus $P^g \leq E$, so P^g is conjugate in E to P. But 4.3 applied to M implies there exists $r \in z^M$ with $\alpha^r = \gamma$, so $t^D \cap N(P^g)$ and therefore $t^D \cap M$ is nonempty. It follows with (1) that for any $\beta \neq \alpha$ there exists $t \in z^M$ with cycle (α, β). Thus M^Δ is transitive.

(3) Let Q be a Sylow p-subgroup of $M \cap H$. By 5.3, $|\Delta| \equiv n \equiv 2 \bmod p$, so Q

is Sylow in M and we may assume $Q \leq D$. Suppose $z \in Z^*(M)$. Then we may assume $Q^z = Q$, so $Q \leq E$ and thus $P = Q$ is Sylow in M, while by 5.3, P is not Sylow in G. Thus $z \notin Z^*(M)$. Set $L = \langle z^M \rangle$. As $z \notin Z^*(M)$, minimality of G implies L contains a 4-group A with $A^{\#} \subseteq z^G$. So $X = O(L) = \Pi_{A^{\#}} C_X(a) \leq H$, and thus as M^{Δ} is transitive, $X \leq E$. Therefore $P \cap X$ is Sylow in X. This with minimality of G and 2.9 implies any p-subgroup R of $M \cap H$ fixing 3 or more points and containing P is normalized by an element of $z^M \cap H$. So (1) implies $R \leq P$. Thus P is maximal as claimed. Thus by 5.3, Q fixes exactly two points. Thus 4.7 implies M^{Δ} is 2-transitive.

Lemma 6.3. *Let $X \trianglelefteq D^*$ and Q a Sylow p-subgroup of $X \cap E$. Then $t^D \cap N(Q)$ is nonempty.*

Proof. Let $Q \leq P$ be Sylow in E. By 6.2 we may assume $P^t = P$. Thus t normalizes $P \cap X = Q$.

Theorem 6.4. $E = C_D(z)$.

For the remainder of this section assume 6.4 is false and let p be a prime divisor of $|E : C_E(z)|$. Let P be a z-invariant Sylow p-subgroup of $O(E)$ and $M = N_G(P)$. With 4.8 and 6.3 we may assume $t \in M$. We will be interested in the following hypothesis:

Hypothesis 3. $X \leq H$, $z \in Y = N_G(X) \not\leq H$, $m(\langle z^Y \rangle) > 1$, *and z does not centralize a Sylow p-subgroup of $H \cap H^y \cap Y$, for $y \notin H$.*

Notice that if Hypothesis 3 is satisfied then minimality of G implies $\langle z^Y \rangle / O(\langle z^Y \rangle)$ is the extension of a Bender group.

Lemma 6.5. *Hypothesis 3 is satisfied with $X = P$. If X satisfies Hypothesis 3, $[X, z] \neq 1$, q is an odd prime, and $Q \in \text{Syl}_q(C_D(X))$, then $z^H \cap N(XQ)$ is nonempty.*

Proof. Let A be a z-invariant Sylow p-subgroup of E containing P. By 6.2 and 5.3 there exists a p-element $x \in O(D) \cap N(A) - A$. By 4.8, $O(E) \leq O(D)$, so $x \in N(P)$. By 6.2 and 5.3, $N(A)^{F(A)}$ is an extension of a Bender group, so zz^x has even order. Thus $m(\langle z^M \rangle) > 1$, and P has Hypothesis 3 in the role of X.

Now take X and Q as hypothesized. Let $L = \langle z^Y \rangle Q$, and let $Q \leq R \in \text{Syl}_q(QO(L))$. If R fixes 3 or more points of a^Y then by 2.9 we may take $z \in N(R)$. Then z normalizes $C_R(X) = Q$. So assume Q fixes exactly two points. Then Q is Sylow in $C_{(L \cap H)}(X) \trianglelefteq H \cap L$. So a Frattini argument implies $N(Q) \cap H \cap L$ has even order and thus contains an element of z^H.

Lemma 6.6. $\theta(E) \leq \theta(D)$.

Proof. By 4.8, $O(E) \leq O(D)$. Let x be a p-element of $O(D)$ centralizing P, and let $x \in Q \in \mathrm{Syl}_p(C_D(P))$. By 6.5 there is $z^h = s \in N(PQ)$, so $QP \leq D_\beta s$. Hence $\langle x \rangle P \leq O(D)_\beta s$. So by 6.2, $x \in P$. Thus P contains all p-elements of $O(D)$ centralizing P, so a result of Thompson [9] implies any p'-subgroup of $O(D)$ normalized by P is in $O_{p'}(O(D)) = \theta(D)$. Thus $\theta(E) \leq \theta(D)$.

Lemma 6.7. *Assume Hypothesis 3 with $\beta \in \alpha^Y$ and Q a Sylow p-subgroup of $Y \cap O(D)$. Then $\theta(Y \cap D) \leq E$ and $Z(J(Q))$ is normalized by an element of z^E.*

Proof. Set $B = \langle z^{(H \cap Y)}, Y \cap O(D) \rangle$. Minimality of G implies B is solvable, and $O(B) \leq E$. z normalizes but does not centralize P, so $W = \theta(B) = O_{p'}(B)$. The ZJ-theorem implies $WR \trianglelefteq B$, where $R = Z(J(Q))$. Thus R is normalized by an element of $z^W \subseteq z^E$. Set $\bar{A} = A/W = O_p(B/W)$. As B is solvable, $C_B(\bar{A}) \leq A$. But $\theta(Y \cap D)$ centralizes A/W as $A \leq Y \cap D$. So $\theta(Y \cap D) \leq \theta(B) \leq E$.

Lemma 6.8. $\theta(D) > \theta(E)$.

Proof. By 6.2, a Sylow p-subgroup of E satisfies the role of X in Hypothesis 3. Choose X satisfying Hypothesis 3 with $|Y \cap O(D)|_p$ maximal. Let Q be a Sylow p-subgroup of $Y \cap O(D)$. 6.7 implies $R = Z(J(Q))$ satisfies Hypothesis 3, so maximality of $|Y \cap O(D)|_p$ implies Q is Sylow in $N(R) \cap O(D)$. So as R is characteristic in Q, Q is Sylow in $O(D)$. Assume $\theta(D) = 1$. Then the ZJ-theorem implies $R \trianglelefteq O(D)$. Thus by 5.2 $G = \langle t, z, O(D) \rangle$ normalizes R, a contradiction. Similarly if $\theta(E) = \theta(D)$, then $G \leq N(\theta(D))$. Thus with 6.6, the conclusion holds.

Lemma 6.9. *$\theta(E)$ is a Hall subgroup of $\theta(D)$.*

Proof. Assume not and let Q be a Sylow q-subgroup of $\theta(E)$ with Q not Sylow in $\theta(D)$. By 6.3 and 6.6 we may assume $z, t \in Y = N_G(Q)$. Choose $P \leq Y$. By 4.3 we may assume q divides m. Hence we may argue as in 6.5 to show Q satisfies Hypothesis 3 in the role of X. Thus 6.6 and 6.7 yield a contradiction.

We now derive a contradiction and establish 6.4. Let q be a prime divisor of $|\theta(D):\theta(E)|$, let $X = [P, z]$, and let R be a $X\langle z \rangle$-invariant Sylow q-subgroup of $\theta(G_{\beta\beta}z)$. By 6.9, q is not a prime divisor of $|\theta(E)|$, so $R \cap E = 1$. Thus $C_R(z) = 1$ and by 2.1, $[X, R] = 1$. R moves α so $Y = N(X) \not\leq H$. Let $L = \langle z^M \rangle$ and $z \in S \in \mathrm{Syl}_2(L)$. Then $z \in Z(S)$ so S acts on $X = [P, z]$. Thus $m(\langle z^Y \rangle) > 1$. So X satisfies Hypothesis 3. Let γ be a point of α^Y distinct from α. By 4.3 there is a conjugate s of z under Y with cycle (α, γ). Let Q be a $\langle s \rangle X$-invariant Sylow q-subgroup of $\theta(G_{\alpha\gamma})$. With 6.2 we may argue as above to show $[X, Q] = 1$. Now by 6.5 we may assume z normalizes XA, where $Q \leq A \in \mathrm{Syl}_q(C(X)_{\alpha\gamma})$. So $Q \leq \theta(G_{\alpha\gamma})_\gamma z \leq \theta(G_{\alpha\gamma\gamma}z)$. But now 6.2 and 6.9 yield a contradiction.

This completes the proof of Theorem 6.4.

7. The group $\langle [O(D), t], z, t \rangle$.

Lemma 7.1. *Let* $Y < G$ *with* $z \in H \cap Y < Y$. *Set* $L = \langle z^Y \rangle$. *Then either*

(1) $z \in Z^*(Y)$ *and* $\{z\} = z^H \cap Y$, *or*

(2) $[O(Y), L] = 1$ *and* $L/O(L) \cong L_2(q)$, $Sz(q)$, *or* $U_3(q)$, $q > 2$ *even*.

Proof. Minimality of G implies $H \cap L$ is strongly embedded in L. If $m(L) \geq 2$ let A be a 4-group in $L \cap H$ and $X = O(Y)$. Then $X = \prod_{A^\#} C_X(a) \leq H$, so X fixes a^L of order at least 3. Therefore by 6.4, z, and therefore L, centralizes X. As $H \cap L$ is strongly embedded in L, $L/O(L) \cong L_2(q)$, $Sz(q)$, or $U_3(q)$, $q > 2$ even. So assume $m(L) = 1$. Then $z \in Z^*(Y)$. 4.6 in [2] says $H \cap L = WC_H(z)$ where $W \trianglelefteq H \cap L$ and $N_L(W) \not\leq H$. As $N_L(W) \not\leq H$, W fixes at least three points, so by 6.4, $W \leq C(z)$. Thus $H \cap L \leq C(z)$, so $\{z\} = z^H \cap L = z^H \cap Y$.

Theorem 7.2. $G = \langle t, z, [t, O(D)] \rangle$.

Set $X = [t, O(D)]$ and $K = \langle t, z, X \rangle$. For the remainder of this section assume $K \neq G$. Then by 5.2, $\langle z^H \rangle$ is abelian. Set $Q = \langle z^H \rangle$.

Let u be an involution in D. Set $q = |C_Q(u)|$. u acts on K, so with 7.1, either u centralizes Q or $K \cong L_2(q^2)$. By the Z^*-theorem $m(K) > 1$. If $K \cong L_2(4)$ and $q = 2$, then $|H : C(Q)| = 2$, and by 2.3 $u \notin O^2(G)$, a contradiction. So $q > 2$.

Now with 7.1, $C_H(u)$ is transitive on $C_Q(u)^\#$, and therefore on $\Delta - \{u\}$ where $\Delta = C_Q(u)u$. As this holds for each $v \in \Delta$, and $q > 2$, it follows that $N(\Delta)$ is doubly transitive on Δ. In particular $\Delta \subseteq u^G$.

Given an involution w define $a(w)$ to be the number of pairs (v, s) with $v \in u^G$, $s \in z^G$ and $w \in \langle vs \rangle$. Given such a pair, we see that $\langle v, s \rangle$ has a subgroup $\langle r, s \rangle$ of index 2 with $r \in z^G$. As Q is abelian either rs has odd order or $w = rs$. In the former case $wv \in z^G \cap C(v)$, so by the last paragraph $w \in u^G$. Also swv has odd order. Therefore $a(u)$ is the number of pairs (r, s) such that $r, s \in z^G \cap C(w)$ and rs has odd order. Therefore

$$a(u) = (q^i + 1)(q - 1)[q^i(q - 1) + 1]$$

where $1 \leq i \leq 3$ depending on whether $\langle z^{C(u)} \rangle$ is isomorphic to $L_2(q)$, $Sz(q)$, or $U_3(q)$.

If $w = rs$ then we may assume $r, s \in H$, so $w \in Q$. Notice $[Q, u] \neq 1$. Thus $w \in z^G$. $|C(w) \cap u^G| = |u^H|/(q + 1)$. Further given $v \in C(w) \cap u^G$ we may assume v normalizes K, and thus in $\langle K, v \rangle \cong 2L_2(q^2)$ there are exactly q elements $s \in z^G$ with $w \in \langle vs \rangle$. So

$$a(z) = |u^H|q/(q + 1) = |H|(q^i + 1)q/|C(u)|(q + 1).$$

Notice that $a(w) = 0$ if $w \notin u^G \cup z^G$. But by the Thompson order formula

$$|G| = \sum_j a(w_j)|C(u)||C(z)|/|C(w_j)|$$

where $\{w_j\}$ is a set of representatives for the collection of conjugacy classes of involutions of G. It follows that

Lemma 7.3. *Let u be an involution in D. Then $|F(u)| = q^i + 1$ for $q > 2$ even and either*

(1) $u \in C(Q)$ and $n = (q^i + 1)[q^i(q - 1) + 1]$, or

(2) $u \notin C(Q)$ and $n = (q^i + 1)[q^i(q - 1) + q + 1]/(q + 1)$.

Let $f(i, q)$ and $g(i, q)$ be the expressions for n in (1) and (2) respectively. Then $f(i, q_1) \neq g(j, q_2)$ for any i, j, q_1, and q_2. Also f and g are one to one. Therefore all involutions in D have the same number $q^i + 1$ of fixed points and $C_D(Q)$ contains all involutions in D if it has even order.

Notice also that as $ut \in u^G$, all involutions in D^* and therefore in G, are conjugate either to t or to an involution in D.

Lemma 7.4. *X acts semiregularly on $\Omega - \{\alpha, \beta\}$.*

Proof. Let y be an element of order p in D where p is a prime divisor of the order of X. X is cyclic by 5.2 and by 5.3 a Sylow p-subgroup of D fixes only α and β. So if $y \in X$ then a Sylow p-subgroup of $C_D(y)$ fixes exactly two points. If $y \notin X$ then let x be an element of order p in X. Then for some $a \in \langle x, y \rangle^\#$, $C_Q(a) \neq 1$, so with 7.1, considering $C(a)$, $\langle x, y \rangle$ fixes only α, β. Thus for any element y of order p in D, a Sylow p-subgroup of $C_D(y)$ fixes only α and β. It follows that $C(x)^{F(x)}$ is 2-transitive if $|F(x)| > 2$. But t inverts x, so by 6.2 and 6.4, $|F(x)|$ is even. But $t \in Z^*(N(\langle x \rangle))$, so as $C(x)^{F(x)}$ is 2-transitive of degree greater than 2, $O(C(x))^{F(x)} \neq 1$ and therefore $F(x)$ has odd prime power order, a contradiction.

Lemma 7.5. *u centralizes Q.*

Proof. Assume not. Then we are in case (2) of 7.3. Notice $g(2, q)$ is not an integer. Thus $i \neq 2$. If $i = 1$ then $n = q^2 + 1$. Thus $z^G \subseteq K$, a contradiction. So $i = 3$. Now X has order $q^2 - 1$ and by 7.4 acts semiregularly on $\Omega - \{\alpha, \beta\}$. But $n - 2 = q^6 - 2q^5 + 2q^4 - 1 \equiv -2(q - 1) \bmod(q^2 - 1)$, a contradiction.

Lemma 7.6. *$i \neq 3$.*

Proof. Assume $i = 3$. Let $K_u = \langle z^{C(u)} \rangle$. We may assume $K \leq K_u$. Now K_u contains a cyclic subgroup $A \neq 1$ with $C_{K_u}(A) = K \times A$. Further A centralizes

Δ so A induces an automorphism on K_ν centralizing Q for each $\nu \in \Delta$. It follows that A centralizes $q + 1$ conjugates of Q in each K_ν. Thus A centralizes at least $q^2 + 1$ conjugates of Q in total. But $L = \langle z^{C(A)} \rangle$ contains $q^j + 1$ conjugates, $1 \leq j \leq 3$. So $j = 2$ or 3. As $K \leq L$, $j = 3$.

Let B be a Sylow 2-subgroup of $C(K_u)$. B acts on L with $\langle C(B) \cap z^L \rangle = K$, so $B = \langle u \rangle C_B(L)$. But $G = \langle K_u, L \rangle$ centralizes $C_B(L)$, so $B = \langle u \rangle$. Let V be a u invariant Sylow 2-subgroup of $H \cap L$ and set $U = N_V(\Delta)$. Let T be Sylow in $H \cap K_u$. Then $T = [G_\Delta, A]$ so U normalizes T. Also A acts irreducibly on T/Q, so $Q = \Phi(S)$, where $S = TU\langle u \rangle$. We may choose u to be in the center of a Sylow 2-group P of D normalizing S. By 7.3, $PS \in \mathrm{Syl}_2(G)$. $Q = \Phi(S)$ and P normalizes $U\langle u \rangle = C_S(A)$, so $U\langle u \rangle \unlhd PS$. Also $U\langle u \rangle \unlhd V\langle u \rangle$. But V fixes no conjugate of Δ in $U\langle u \rangle$, while a Sylow 2-group PS of $N(U\langle u \rangle)$ fixes Δ, a contradiction.

Lemma 7.7. *Let* $J = C(K)$ *and* $\Gamma = \Omega - F(u)$. *Then* K^Γ *is regular and* J *is isomorphic to a subgroup of* K.

Proof. Suppose $k \in K^\#$ fixes a point $\gamma \in \Gamma$. We may assume k has prime order p. As every involution of K is in z^G, $p > 2$. If p does not divide $q - 1$ then k centralizes some $s \in z^G \cap G_\gamma$. But k is inverted by some t in $Z^G \cap K$, so t is not conjugate to s in $N(\langle k \rangle)$, a contradiction as ts has odd order. So p divides $q - 1$ and we may assume $k \in X$. But now 7.4 yields a contradiction. So K acts semiregularly on Γ. Thus as $|K| = |\Gamma|$, K^Γ is regular. J acts faithfully on Γ as J fixes $\Omega - \Gamma$ pointwise. Therefore J is isomorphic to a subgroup of $N_K(K_\alpha)/K_\alpha \cong K$ (e.g. Theorem 1.13 of [8]).

Lemma 7.8. $N_H(K) = DT$ *where* T *is the Sylow 2-subgroup of* $K \cap H$.

Proof. By 6.3 we may choose t to centralize E. Thus $D = XE$ normalizes $K = \langle t, z, X \rangle$. So $N_H(K) = DT$.

Lemma 7.9. $i = 1$.

Proof. Assume $K \cong Sz(q)$. Then $n - 1 = q^3(q^2 - q + 1)$. Let p be a prime divisor of $q^2 - q + 1$. Then p is relatively prime to $|K|$ and thus to $|JK|$. Suppose $1 \neq P$ is a Sylow p-subgroup of D. Then p does not divide $q - 1$, so $C_Q(P) \neq 1$. If $|C_Q(P)| > 2$ then by 7.1, $N_H(P) = C_Q(P)N_D(P)$, so P is Sylow in $N_H(P)$ and therefore also in H, contradicting the choice of p. So $q = 2^{p^e}$ and P is cyclic. Further $q \equiv 2 \bmod p$, so $0 \equiv q^2 - q + 1 \equiv 3 \bmod p$, and thus $p = 3$. Let w be an element of order p in P. As P is cyclic, $C_H(w)$ contains a Sylow group of $N_H(P)$. But if $q \neq 8$ then $|C_Q(w)| > 2$, so $C_H(w) = C_Q(w)C_D(w)$, and thus P is Sylow in $C_H(w)$. So $q = 8$.

Next let r be a prime divisor of $q^2 - q + 1$ not dividing $|D|$. Let $R \in \mathrm{Syl}_r(H)$. Claim $R \leq C(Q) = C$. Assume not. Let $u \in S \in \mathrm{Syl}_2(C)$. If $\Delta \cap S = \Delta^C \cap S$ then a Frattini argument implies r divides $|N(\Delta)| = q|TD|$, a contradiction. So Δ is not weakly closed in S and hence as X is transitive on $\Delta - u$, $N_S(\Delta)^\Delta$ is transitive. Then with 7.3, $N_S(\Delta) \leq C$ contains a Sylow 2-group of H. So H/C is solvable. Let $F/C = \mathrm{Fit}(H/C)$. If $F \leq DC$ then as $XC/C = \mathrm{Fit}(DC/C)$, $XC = F$. Hence by a Frattini argument r divides the order of the normalizer of a Sylow m-subgroup M of F, where m divides $q - 1$. But $N(M) \leq D$ by 7.4. Thus we may assume $R \cap F \not\leq C$, and by a Frattini argument we may assume $N(R \cap F)$ is transitive on $Q^\#$. But $C_Q(R \cap F) \neq 1$, so $R \cap F \leq C$.

So $R \leq C$ and by a Frattini argument we may assume X normalizes R. Now if $x \in X^\#$ then $C_R(x) \leq D \cap R = 1$, so X acts semiregularly on $R^\#$. Thus $|R| = 1 + a(q - 1)$. But if $q = 8$ we may choose $r = 19 \not\equiv 1 \bmod 7$. So the order of D is relatively prime to $q^2 - q + 1$.

Next assume that p is a prime divisor of $q^2 - q + 1$ distinct from r and let P be Sylow in H. Then $|P| = 1 + b(q - 1)$. As p and r are odd, a and b are even, so $ab \geq 4$. But $q^2 - q + 1 \geq |R||P| > ab(q - 1)^2 + 1 \geq 4(q - 1)^2 + 1$, so $4 < q/(q - 1) < 2$, a contradiction. Thus $q^2 - q + 1$ is a power of p. But as q is an odd power of 2, $q^2 - q + 1 \equiv 3 \bmod 9$, so $q^2 - q + 1 = 3$. Thus $q = 2$, a contradiction.
Set $M = O_2(H)$.

Lemma 7.10. *If $Q < M$ then $Q < \Omega_1(M)$.*

Proof. Assume $\Omega_1(M) = Q < M$. Claim $(q - 1, |J|) = 1$. For suppose p is a prime divisor of $q - 1$ and let y be an element of order p in J. Let x be an element of order p in X. Then for some $w \in \langle x, y \rangle^\#$, $M_1/Q = C_{M/Q}(w) \neq 1$. $Q = O_2(C_H(y))$, so $w \not\in J$. Therefore $Q = [M_1, w]$, so there are involutions in $C_M(w) - Q$, a contradiction. Next claim $(q + 1, |J|) = 1$. For let p be a prime divisor of $q + 1$ and y an element of order p in J. Again $Q = O_2(C_H(y))$ so letting $X = \langle x \rangle$, $w = xy$ acts semiregularly on $(M/Q)^\#$. It follows that $|M/Q| \geq q^2$. But $n - 1 = q^3$ and as $Q = \Omega_1(M)$, $M \cap D = 1$. Thus $|M| = q^3$ and $H = MD$. Further as J is isomorphic to a subgroup of K, J is dihedral and thus as J contains all involutions in D, a Sylow 2-subgroup of D is cyclic. Now as $Q = \Omega_1(M)$, u is not in the kernal of the transfer of G to S/M where S is Sylow in G. But this contradicts 5.1.

It follows that J and therefore $C(Q)$ is a 2-group. So $Q \neq \Omega_1(M)$.

Lemma 7.11. $O_2(J) \neq 1$.

Proof. Assume $O_2(J) = 1$. Then $O_2(H) \cap D = 1$ so $Q = \Omega_1(M)$. Thus by 7.10,

$Q = M$. As J is isomorphic to a subgroup of K, J contains a self-centralizing cyclic subgroup W of odd order with $N_H(W) \cap C(Q) = \langle u \rangle W \times Q$. Thus in $\overline{C} = C(Q)/Q$, $\overline{W}$ is self-centralizing of index 2 in its normalizer. $|\overline{C} : \overline{J}|$ divides $|H : N_H(K)| = q^2$, so if $\overline{C}$ possesses a nontrivial normal subgroup which does not contain u, then $O_2(C) \neq 1$. So by a result of Suzuki [11, p. 103] $\overline{C}$ has one class of involutions. Thus $Qu = \Delta$ is normalized by a Sylow 2-subgroup S of G. So $|S : C_S(u)| = q$. But $C_S(u) \leq N_H(K)$, so $q^2 = |H : N_H(K)| = |S : C_S(u)| = q$, a contradiction.

Lemma 7.12. $M = C(Q)$.

Proof. As $O_2(J) \neq 1$ and $q^3 = |H : D|$, J contains a cyclic $2'$-Hall group W and W is $2'$-Hall in $C(Q)$. Further $W \times Q = N(W) \cap N(K) \cap C(Q) = N(W) \cap C(Q)$ is abelian so M is a normal complement for W in $C(Q)$. Let w be an element of order p in W. Then p divides $q - 1$ so there exists $x \in X$ of order p. Set $Y = \langle x, w \rangle$ and let A/Q be a minimal normal subgroup of MY/Q in M/Q. Then A/Q is centralized by some $y \in Y^\#$. If $y \in J$ then $A \leq C_M(y) = Q$, a contradiction. So $Q = [A, y]$ and $C_A(y)$ contains an involution which we may take to be u. But A/Q is in the center of M/Q, so M normalizes Δ. This yields a contradiction as in 7.11.

We now contradict the existence of G, thus establishing Theorem 7.2. Let B/Q be a minimal normal subgroup of H/Q contained in M/Q. If X does not act semiregularly on B/Q then arguing as in 7.12 we get a contradiction. Thus $|B| = q^2$ and $B \cap J = 1$.

Set $\theta = \Delta^H$. Then θ has order q. BJ fixes Δ, so as BJ is a 2-group, BJ fixes some $\Delta^h \neq \Delta$. As X normalizes BJ and is transitive on $\theta - \{\Delta\}$, BJ fixes θ pointwise. Now $JQ \cap J^hQ$ centralizes $\Delta \cup \Delta^h$ so $JQ \cap J^hQ = Q$. Also $|BJ| = q^2|J| = \Sigma|J^hQ - Q| + |B|$, so every element in $BJ - B$ centralizes a unique conjugate of Δ. Let $w \in M - BJ$. X is regular on M/BJ, of order q, so M/BJ is elementary. Thus $w^2 \in BJ$. If $w^2 \notin B$ then by the above we may assume w^2 centralizes Δ and is semiregular on $u^G - \Delta$. So as $w \in C(w^2)$, w fixes Δ, a contradiction. Thus M/B is elementary so $M/B = JB/B \times [M/B, X]$. Let $L/B = [M/B, X]$. M is transitive on θ and $|\theta| = q = |B/Q|$, so for each coset bQ in B/Q there exists $w \in M$ with $[u, w] \in bQ$. Then $u^w = ub$ is an involution so u inverts b. Thus u inverts every member of the coset bQ. As this holds for each $u \in J^\#$ it follows that $J = \langle u \rangle$.

But now $H/JL \cong D/J$ is contained in the automorphism group of K, so H/JLX is cyclic. Further u is the unique involution in D, so H/XL is cyclic of even order. So as H controls fusion in a Sylow 2-subgroup of G contained in H, G has a subgroup of index 2, contradicting 5.1.

8. The centralizer of u.

Lemma 8.1. *Let u be an involution in D with z, $t \in M = C_G(u)$ and $z^H \cap M = \Delta$ maximal. Then $M \cap D$ has 2-rank 1.*

Proof. Set $L = \langle z^M \rangle$ and $K = C_M(L)$. Let v be an involution in K. Then maximality of Δ implies $z^H \cap C(v) = \Delta$. Suppose $\langle u, v \rangle = W$ is a 4-group in K. Set $X = O(D)$. Then $X = \prod_{W^\#} C_X(w)$. Further $C_X(w) \leq N_D(\Delta)$, so $X \leq N_D(\Delta)$. Thus $G = \langle z, t, X \rangle \leq N(\Delta)$, a contradiction. Thus $m(K) = 1$. Let $W = \langle u, v \rangle$ be a 4-group in $M \cap D$. Then as $m(K) = 1$, v induces an outer automorphism on L. So $\bar{L} = L/O(L) \not\cong Sz(q)$. Further if $m(L) = 1$ or $\bar{L} \cong U_3(q)$, then $[\Delta, v] = 1$, and we get a contradiction as above. Thus $L \cong L_2(q^2)$, and $C_\Delta(v)$ has order $q - 1$. We may assume $z^H \cap C(v) \not\subseteq \Delta$, so $L_1 = \langle z^{C(v)} \rangle \cong L_2(q^2)$. Similarly either $C_\Delta(v) = z^H \cap C(uv)$ or $L_2 = \langle z^{C(uv)} \rangle \cong L_2(q^2)$.

We may assume $U = \langle W, t \rangle$ is abelian. Let p be a prime divisor of $q + 1$, P_1 a U-invariant Sylow p-subgroup of X, $P = [P_1, t]$, and $\bar{P} = P/\Phi(P)$. As $|C_{\bar{P}}(w)| \leq p$ for $w \in W^\#$, $|\bar{P}| = p^2$ or p^3. Further t inverts $\bar{P}$. Suppose $|\bar{P}| = p^2$. Then uv inverts $\bar{P}$, so $[uvt, P] = 1$, and P acts on $F(uvt)$. t inverts P so by 6.4, $\gamma \notin F(P)$ where $F(t) = \{\gamma\}$. As $\gamma \in F(uvt)$, $|F(uvt)| \geq 3$. So $L_3 = \langle t^{C(uvt)} \rangle \cong L_2(q^i)$, $i = 1$ or 2, and $t \in L_3$ inverts a noncyclic subgroup P of order p^2 in L_3, a contradiction. Thus $|\bar{P}| = p^3$. But now $|C_{\bar{P}}(ut)| = p^2$, and, arguing as above on $C_P(ut)$ and ut in place of P and uvt, we get a similar contradiction.

As an immediate consequence of 8.1 we get:

Lemma 8.2. *D has 2-rank 1.*

Let u be an involution in E. [2] implies such an involution exists. Let $z \in M = C_G(u)$ and $L = \langle z^M \rangle$. Let R be a Sylow 2-subgroup of $L \cap H$, T_1 a Sylow 2-subgroup of $M \cap H$, $T = T_1 \cap LC_M(L)$, and $U = \Omega_1(R)$. Set $\Delta = u^G \cap T$ and $N = N_G(\Delta)$.

Lemma 8.3. (1) $L/O(L) \cong L_2(q)$, $Sz(q)$, or $U_3(q)$.
(2) $\langle u \rangle U = \Omega_1(T_1)$.
(3) $uz \in u^G$ and $|\Delta| = q$.
(4) G has 2 classes of involutions, u^G and z^G.

Proof. It follows from 7.1 and 8.2 that $\langle u \rangle U = \Omega_1(T_1)$. $N_L(U)$ is transitive on $U^\#$, so T_1 contains three L-classes of involutions, $\{u\}$, z^L, and $(uz)^L$. The Z^*-theorem implies $uz \in u^G$. G is doubly transitive on Ω, so any class of involutions has a representative v with cycle (α, β). As $m(D) = 1$, we may assume $v \in T_1$. Thus $v^G = u^G$ or z^G.

Simple groups of 2-rank 2 have been classified [1], [6]; all have one class of involutions. Thus $m(G) \geq 3$. So a Sylow 2-subgroup S of G has a normal 4-group X. $|S : C_S(X)| \leq 2$, so as G has no subgroup of index 2, we may assume $u \in C_S(X)$. Thus $m(C_S(u)) \geq 3$. So $m(U) \geq 2$. Thus 7.1 implies (1).

Lemma 8.4. *Let $X \leq D$ fix 3 or more points with $t \in N(X)$. Then $[X, t] = 1$.*

Proof. Let X be a counterexample. With 6.4 it suffices to show $F(X) = \Gamma$ has odd order. So we may assume X is contained in a p-subgroup W maximal with respect to fixing 3 or more points. Then $Y = N_G(W)$ is 2-transitive on $F(W)$. Suppose $z^G \cap Y$ is empty. Then by 8.3, $m(Y) = 1$. So $Y^{F(W)}$ has a regular normal subgroup $Q^{F(W)}$ and therefore a Sylow p-subgroup of $Y \cap D$ fixes 3 or more points. Thus maximality of W implies W is Sylow in D, so $t^D \cap Y$ is nonempty. Now by 6.4, t fixes no point of Γ. Thus arguing as in 4.5, $t \in Z^*(Y)$. Thus Γ has odd order.

Lemma 8.5. *N^Δ is doubly transitive and either solvable, or permutation isomorphic to $L_2(7)$ on $q = 8$ letters.*

Proof. $N \cap L \cap D \trianglelefteq N_u$ is regular on $\Delta - \{u\}$ and is cyclic of order $q - 1$. Thus N^Δ is 2-transitive and any one of several theorems on doubly transitive groups imply N^Δ is solvable or is contained in the automorphism group of $L_2(q - 1)$. In the latter case, setting $v = uz$, N_{uv}^Δ has a cyclic subgroup of order $(q - 2)/2 = 2^{k-1} - 1$. We may assume $(q - 1) \neq 3$, for if so N^Δ is solvable. Thus there is a prime divisor p of $2^{k-1} - 1$ and an element x of order p in N_{uv}^Δ. Then $|C_U(x)| = 2$ and x induces an automorphism of $L/O(L) \cong L_2(q)$, $Sz(q)$, or $U_3(q)$, so $k = p = 2^{k-1} - 1$. Thus $q = 8$ and $N^\Delta \cong L_2(7)$.

For $x \in u^G$, let $L_x = \langle z^{C(x)} \rangle$. Set $B = N_\Delta$.

Lemma 8.6. *$B = \langle u \rangle R = T$ and $L/O(L) \not\cong U_3(q)$.*

Proof. Let $A = C(L) \cap C(L_v)$, $v = uz$, and $Y = \langle z^{C(A)} \rangle$. $\langle [t, C_D(u)], [t, C_D(ut)] \rangle = V \leq Y \cap D$. But $[t, D] = V$, so $G = \langle t, z, [t, D] \rangle \leq C(A)$. So $A = 1$.

It follows that $X = C_B(L_v)$ is isomorphic to a subgroup of Aut(L). $|R : R \cap L_v| \leq 2$ and $[X, L_v] = 1$, so X is an elementary 2-group. As X has 2-rank 1, $X = \langle v \rangle$. Thus $B = \langle u \rangle R = T$ unless $L \cong U_3(q)$.

Suppose $L \cong U_3(q)$ and let W be a $2'$-Hall subgroup of B. Then $W \neq 1$ and $W \leq \bigcap_\Delta L_x$. We may assume $[t, W] = 1$. Set $Y = \langle z^{C(W)} \rangle$. $[t, C_D(u)] \leq Y \cap D$. $X = [t, C_D(ut)]$ is a subgroup of odd order in L_{ut} normalized by t. Now if $X \leq C(W)$ then arguing as above $G \leq Y$. So $X \not\leq C(W)$. Let $X_1 = WO(D) \cap L_{ut}$. By 8.4, $N(X_1) \leq D$. It follows that $X_1 = X$ is of order $3(q + 1)^2/(q + 1, 3)$, and $|t^X| = 3(q + 1)$. Now by 8.7,

$$n - 1 = q^3[(q^3 + 1)(q - 1)/3(q + 1) + 1] \equiv 2q^3/3 \bmod q^4.$$

But if $S \in \mathrm{Syl}_2(N(\Delta))$ then by 8.5 $|S : S \cap D| = q^4$, a contradiction.

Lemma 8.7. *Let* $q^i + 1 = |F(u)|$, $i = 1, 2$, *let* $V = \langle u, t \rangle$, *and let* $a = |C_D(u) : C_D(V)| / |C_D(ut) : C_D(V)|$. *Then* $n - 1 = q^i[(q^i + 1)a + 1]$.

Proof. Let Γ be the set of pairs (v, x) with $v \in u^G$ and x a cycle in v. Then $|u^G|(n - q^i - 1)/2 = |\Gamma| = n(n - 1)e/2$ where e is the order of the set π of elements in u^G with cycle (α, β). But $\pi = (ut)^D$ has order $|D : C_D(ut)|$. Also $|u^G| = n(n - 1)|D : C_D(u)|/q^i(q^i + 1)$. This yields the required identity.

Lemma 8.8. $|C_D(u) : C_D(V)| = q - 1$.

Proof. $|C_D(u) : C_D(V)| = |L \cap D| = q - 1$ as $O(L) = 1$ and $L \cong L_2(q)$ or $Sz(q)$.

Lemma 8.9. $|C_D(ut) : C_D(V)|$ *equals* $q + 1$ *if* $L \cong L_2(q)$ *and* $q \pm \sqrt{2q} + 1$ *if* $L \cong Sz(q)$.

Proof. If $C_D(ut) = C_D(V)$ then $[t, O(D)] \leq C(u)$, so $G = \langle z, t, [t, O(D)] \rangle \leq C(u)$, a contradiction. So let $1 \neq x \in C_D(ut)$ with $x^t = x^{-1}$. By 8.4, x acts semi-regularly on $\Omega - \{\alpha, \beta\}$ and thus also on $F(ut)$. Further letting $L_1 = \langle t^{C(ut)} \rangle$, $X = C_{L_1}(x)$ acts on $F(x) = \{\alpha, \beta\}$ so any subgroup of X of odd order is in D. It follows that $X = [X, t]$ has order $q + 1$ if $L \cong L_2(q)$ and order $q \pm \sqrt{2q} + 1$ if $L \cong Sz(q)$.

Lemma 8.10. $L \cong L_2(q)$ *and* $n - 1 = q^2$.

Proof. If $L \cong L_2(q)$ then 8.7, 8.8, and 8.9 imply $n - 1 = q^2$. So assume $L \cong Sz(q)$. Then the same lemmas imply

$$n - 1 = q^2[(q - 1)(q \pm \sqrt{2q} + 1) + 1] \equiv q^2\sqrt{2q} \bmod q^3.$$

But 8.5 implies that $|S : S \cap D| = q^3$ where S is a Sylow 2-subgroup of N, a contradiction.

Lemma 8.11. *N contains a Sylow 2-subgroup S of G.*

Proof. N contains a Sylow 2-subgroup W of D, and letting S be a Sylow group of N containing W, $|S : W| = q^2 = |H : D|$, so S is Sylow in H and thus also in G.

Lemma 8.12. N^Δ *is solvable.*

Proof. Assume $N^\Delta \cong L_2(7)$. Then $T_1 = \langle u \rangle U = T$ and as u is not a square root T/U has a normal complement Y/U in N/U. Y has one of two forms depending on whether the extension splits. Assume first $Y = XU$ with $X \cong L_2(7)$. X has one class of involutions Γ so it contains a 4-group A with $A^\# \subseteq \Gamma$. Thus 8.3

implies $\Gamma \subseteq z^G$. Set $V = S \cap Y$. It follows that all involutions in V are in z^G, so considering the transfer of G to S/V, G has a subgroup of index 2, a contradiction. So the extension does not split. Again K has 2 classes of involutions [4, p. 834]. If both classes are contained in z^G we get a contradiction as above. So involutions $v \in V - U$ are in u^G. But v centralizes an element of order 4 in V (e.g. [4, p. 854], while $C(u)$ contains no elements of order 4.

We now derive a contradiction and complete the proof of Theorem 2. As N^Δ is solvable and doubly transitive on q letters it contains a regular normal subgroup Q^Δ. By 8.6 Q is a 2-group. $Q \cap M$ contains all involutions in $M \cap S$, so Q contains all involutions in S. $U \trianglelefteq N$ and N is transitive on $U^\#$, so $U = Z(Q)$. Let $A = L \cap D$. $Q/U = \langle u \rangle U/U \times [A, Q/U]$. Let V be the preimage of $[A, Q/U]$ in Q. If $V \cap u^G$ is empty then considering the transfer of G to S/V, G has a subgroup of index 2. So let $v \in V \cap u^G$. Then $v \in V - U$. As U is elementary and in the center of Q, and A is transitive on $(V/U)^\#$, V is elementary. Let $V = U \times W$, and a and b involutions in W. If $a, b \in u^G$, then by 8.3, $ab \in z^G$. Thus W contains some $w \in z^G$. 8.3 implies $Uw \subseteq z^G$. As A is transitive on $(V/U)^\#$, $V^\# \subseteq z^G$, a contradiction.

This completes the proof of Theorem 2.

REFERENCES

1. J. Alperin, R. Brauer and D. Gorenstein, *Finite groups of 2-rank 2* (to appear).

2. H. Bender, *Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlässt*, J. Algebra 17 (1971), 527–554. MR 44 #5370.

3. D. Gorenstein and K. Harada, *On finite groups with Sylow 2-subgroups of type A_n, n = 8, 9, 10, 11*, Math. Z. 117 (1970), 207–238.

4. ———, *Finite simple groups of low 2-rank and the families $G_2(q)$, $D_4^2(q)$, q odd*, Bull. Amer. Math. Soc. 77 (1971), 829–862. MR 46 #5427.

5. ———, *Finite groups whose Sylow 2-subgroups are the direct product of two dihedral groups*, Ann. of Math. 95 (1972), 1–54.

6. ———, *Finite groups of sectional 2-rank at most four* (to appear).

7. D. Gorenstein and J. H. Walter, *Centralizers of involutions in balanced groups*, J. Algebra 20 (1972), 284–319. MR 45 #2008.

8. E. Shult, *On the fusion of an involution in its centralizer* (to appear).

9. J. G. Thompson, *Fixed points of p-groups acting on p-groups*, Math. Z. 86 (1964), 12–13. MR 29 #5911.

10. J. H. Walter, *The characterization of finite groups with abelian Sylow 2-subgroups*, Ann. of Math. (2) 89 (1969), 405–514. MR 40 #2749.

11. M. Suzuki, *Applications of group characters*, Proc. Sympos. Pure Math., vol. 6, Amer. Math. Soc., Providence, R. I., 1962, pp. 101–105. MR 24 #A3196.

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91109