SMALL MODULES FOR SMALL GROUPS

Andrew Chermak

Department of Mathematics
Kansas State University
Manhattan KS, 66502

December, 2001

Introduction. This paper concerns "small" modules for finite groups which are themselves "small" in a certain sense to be defined, and it is directed towards some specific applications. For the space of a few paragraphs, however, we can try to place things in a fairly broad context.

For any finite group Y and any prime p, one may consider the action induced by Y, via conjugation, on the largest normal p-subgroup $O_p(Y)$ of Y. As an example, let Y be a proper parabolic subgroup in a simple group X of Lie type, in characteristic p. Then $C_Y(O_p(Y)) \leq O_p(Y)$, which is to say that $Y/Z(O_p(Y))$ is faithfully represented as a group of automorphisms of $O_p(Y)$. Denote by L the subgroup of Y generated by the p-elements in Y, and assume that L properly contains $O_p(Y)$. That is, assume that Y is not a Borel subgroup of X. Then $O_p(Y) = O_p(L)$, and $L/O_p(L)$ is itself a group of Lie type in characteristic p. Further, there then exists an L-invariant section V of $O_p(L)$ having exponent p, and such that $L/O_p(L)$ acts faithfully on V. Thus V is a module for $L/O_p(L)$ over the field $\mathbb{F}_p$ of p elements, and one may then appeal to the enormous body of work concerning such representations of characteristic-p groups of Lie type, in order to obtain information about the structure of V and, indirectly, about the structure of L and even of X.

The assumption that Y be a proper parabolic subgroup of X and that Y not be a Borel subgroup implies that the Lie rank of X is at least 2. There is then a rich geometry $\Gamma(X)$ associated with X, namely the building associated with the set of all parabolic subgroups of X, and which is encoded in the Dynkin diagram associated with X. From this diagram one also reads off information about the various "residues" at the proper parabolic subgroups of X, so that the geometry $\Gamma(L)$ associated with the group $L/O_p(L)$ is given by a sub-diagram. The point is that this geometry imposes severe restrictions on the sorts of modules V which can arise in the above context. Indeed, if we choose L so that the diagram for $\Gamma(L)$ is *connected* then, as it happens, all such

Typeset by $\mathcal{AMS}$-TEX

modules V are "small", in the sense that $|L/O_p(L)|^2 > |V|$. This fact can be seen as a consequence of another one, which has more to do with the particular nature of the action of L on V. Namely, in "most" cases in which $\Gamma(L)$ is connected there exists an elementary abelian p-subgroup A of $X/O_p(X)$, $A \neq 1$, with the property that

$$|A|^2 \geq |V/C_V(A)|. \tag{0.1}$$

(The qualifying adjective "most" will be made more precise, further along in this introduction.) For the moment, we mention that the condition (0.1) implies the condition that $|L/O_p(L)|^2 > |V|$ as a consequence of [CD, Theorem 2.3].

Suppose now that we weaken the above hypotheses, so that the ambient group X is no longer assumed to be a simple group of Lie type. Suppose instead that we require only that $O_p(X) = 1$ and that for any non-identity p-subgroup Q of X, the group $Y = N_X(Q)$ has the property that $C_Y(O_p(Y)) \leq O_p(Y)$. (That is, all p-local subgroups of X are *p-constrained*.) As above, let L be the group generated by the p-elements in Y. One may ask whether there exists a suitable p-local subgroup Y of X, a non-identity elementary abelian subgroup A of $L/O_p(L)$, and an elementary abelian section V of L in $O_p(L)$, admitting faithful action by A, such that (0.1) holds.

In raising this question, we have in mind the situation where X is a simple, or nearly simple, group in which the composition factors of the various groups Y are on the list if "known" simple groups, but in which X itself is not assumed to be on such a list. That is to say, our intention is to address issues that pertain to the Classification of the Finite Simple Groups (or the CFSG, for short).

Specifically, the aim of this paper is to provide support for a project, initiated by Ulrich Meierfrankenfeld, to classify the finite simple groups X which are of "generic characteristic p type." We will not attempt here to outline this program, other than to say that the groups under consideration correspond roughly to the class of simple groups of Lie type, of Lie rank at least 2. The feature of Meierfrankenfeld's project which distinguishes it most clearly from the treatment of characteristic p-type groups in the CFSG as it currently stands, and from the treatment in the ongoing revision project of Gorenstein, Lyons, and Solomon (GLS), consists in directly targeting the groups $Y = N_X(Q)$ for analysis, rather than switching attention to a prime r different from p. This difference in approach can be summarized by saying that in the CFSG as it stands, the emphasis is on "semisimple" subgroups, while in the Meiefrankenfeld program the emphasis is on normalizers of unipotent subgroups. Actually, even in the old version of CFSG, and in the GLS revision, an important chapter - namely the classification of Quasithin Groups - is treated via a "unipotent" approach for the prime 2 (for which see [AS]). So it may be more correct to say that in the Meierfrankenfeld program, the unipotent approach takes center stage, rather than being relegated to the treatment of a difficult special case.

In the Meierfrankenfeld program one begins with a group X of characteristic p-type, with $O_p(X) = 1$, and in which a Sylow p-subgroup S of X is contained in at least two different maximal p-local subgroups of X (so that one has, from the outset, the rudiments of a geometry). The analysis then centers on a pair of p-local subgroups $\widetilde{C}$ and M of X

containing S, such that $\widetilde{C}$ contains the centralizer in X of $Z(S)$, and such that $M/O_p(M)$ acts faithfully on a subgroup V of exponent p in $O_p(M)$ (where V is taken to be as large as possible for this condition). The normal closure W of V in $\widetilde{C}$ is then either an abelian p-group, a non-abelian p-group, or (of course) a group which is not a p-group. One then finds:

(0.2) If W is an abelian p-group then there exists a conjugate A of V in $\widetilde{C}$ such that $[V, A, A] = 1$, and such that $|A/C_A(V)|^2 \geq |V/C_V(A)|$.

The case where W is not a p-group leads to a variant of (0.2), as follows.

(0.3) If W is not a p-group then there is a $\widetilde{C}$-conjugate A of a subgroup of V, such that the following hold.
(i) $[V, A, A, A] = 1$,
(ii) $[C_V(a), A, A] = 1$ for every $a \in A - C_A(V)$, and
(iii) $|A/C_A(V)|^2 \geq |V/C_V(A)|$, and if $p = 2$ then $|A/C_A(V)|^{3/2} \geq |V/C_V(A)|$.

The case in which W is a non-abelian p-group does not lend itself to the formulation of conditions as in (0.2) or (0.3). This is the reason for the qualification concerning "most" cases in the condition (0.1).

We have, so far, explained what a small module is, for our purposes. But we have not yet explained the other half of the title of this paper. A group G is a "minimal parabolic" group (for the prime p) if a Sylow p-subgroup S of G is not normal in G and is contained in a unique maximal subgroup of G. Such groups G are the "small" groups that we will consider here, and a general description of such groups may be found in 11.1, below. Our aim in this paper is to obtain information about $\mathbb{F}_pG$-modules V, where G is a minimal parabolic group and where V satisfies conditions as in (0.2) or (0.3). The reason for restricting attention to these groups has to do with the specific demands made by one portion of the Meierfrankenfeld project. But some of our results do in fact concern small modules for groups which are not necessarily minimal parabolics. We therefore begin by stating a series of hypotheses, of varying degrees of restrictiveness.

Hypothesis 1. *G is a finite group, p is a prime, S is a Sylow p-subgroup of G, and V is a faithful $\mathbb{F}_pG$-module. Further, we have $O_p(G) = 1$, and there exists a non-identity, elementary abelian subgroup A of S such that $|A|^2 \geq |V/C_V(A)|$.*

Whenever Hypothesis 1 is in effect, we put:

$$H = O^p(G).$$

That is:

$$H = \langle g \in G \ : \ |h| \quad \text{is relatively prime to } p\rangle.$$

Also, whenever Hypothesis 1 is in effect, we will use additive notation for the group operation in V (so that 0, rather than 1, denotes the identity element of V). It will be important to observe that, under Hypothesis 1, if H is quasisimple then the Fitting subgroup $F(G)$ is contained in H, and so $H = F^*(G)$.

Hypothesis 2. *In addition to Hypothesis 1, assume that $V = \langle (C_V(S \cap H))^G \rangle$, and $C_V(G) = 0$. Assume also that $G = \langle S^G \rangle$.*

Hypothesis 3. *Let G, p, S, V, and A satisfy the conditions of Hypothesis 2. We further assume that S is contained in a unique maximal subgroup of G.*

Hypothesis 4. *In addition to Hypothesis 3, we assume that A can be chosen so that A acts quadratically on V. That is, we have $[V, A, A] = 0$.*

Recall that a group X is "quasisimple" if $X/Z(X)$ is simple and $Z(X) \leq [X, X]$.

Hypothesis $4'$**.** *Assume Hypothesis 2, and assume that H is quasisimple. Assume further that there is a non-identity elementary abelian p-subgroup A of G satisfiying the following conditions.*

(a) $[V, A, A, A] = 0$.
(b) $[C_V(a), A, A] = 0$ *for every non-identity element a of A.*
(c) *If $p = 2$ then $|A|^{3/2} \geq |V/C_V(A)|$, while if p is odd then $|A|^2 \geq |V/C_V(A)|$.*

Recall that a "component" of a group X is a quasisimple subnormal subgroup of X. We assume always that the Classification of the Finite Simple Groups applies to the components (if any) of G. Thus, to state things explicitly, we have the following:

Background Hypothesis. *Whenever Hypothesis 1 holds, and K is a component of G, then $K/Z(K)$ is an alternating group, the commutator subgroup of a group of Lie type, or one of twenty-six "sporadic" groups.*

(To be scrupulously honest, it must be said that we assume also that if K is a quasisimple subgroup of $SL(4, p)$ then $K/Z(K)$ is given by the CFSG. But, presumably, this assumption is not essential.) We accept, as part of the above background hypothesis, the classification as it stands, of the Schur multipliers of the alternating groups, the groups of Lie type, and the sporadic groups, together with structural information of various kinds concerning these groups. The information that we need can be found in [GLS3] and, for the sporadic groups, in [A2]. Also, whenever the ATLAS of finite simple groups [CCNPW] asserts that a certain group occurs as a maximal subgroup of some group, we accept that information uncritically. This kind of information from the ATLAS will be used (and will indeed be used extensively) only in section 10 below, in dealing with groups of Lie type in characteristic different from p.

In order to state our results, we need first of all to establish some terminological conventions relating to specific groups and modules.

Let G be an alternating or symmetric group $Alt(n)$ or $Sym(n)$, and denote by $P(n, p)$ the permutation module for G, of dimension n over $\mathbb{F}_p$. The "natural module" for G

in characteristic p is, by definition, the module $V = [P(n,p), G]/C_{[P(n,p),G]}(G)$. When $p = 2$ we shall need also the notion of a "spin module" for G, and for this we adopt the view-point taken in [M]. Thus, set $U = [P(n,2), G]$. There is then a natural G-invariant quadratic form Q on U, and if Q is degenerate then n is divisible by 4 and the radical of Q has dimension 1. In any case, set $\overline{U} = U/Rad(Q)$, and let $\overline{Q}$ be the (non-degenerate) form on $\overline{U}$ induced by Q. There is then an induced action of G on the Clifford algebra $\mathcal{C}$ associated with $\overline{Q}$. An $\mathbb{F}_2$-module V is then said to be a **spin module** for G if V is isomorphic to an irreducible G-submodule of $\mathcal{C}$.

The class $Lie(p)$ of "groups of Lie type in characteristic p" will have the following meaning. A group X is in $Lie(p)$ if there is a simple, affine algebraic group $\overline{X}$, defined over an algebraic closure of $\mathbb{F}_p$, and a Steinberg endomorphism σ of $\overline{X}$, such that X is isomorphic to the subgroup of $\overline{X}$ generated by the elements of p-power order in $C_{\overline{X}}(\sigma)$. Having said this, we then make three exceptions. Namely, it will be convenient, for our purposes, to consider also the commutator subgroups of $Sp(4,2)$, ${}^2F_4(2)$, and of ${}^2G_2(3)$ to be groups of Lie type in the characteristics 2, 2, and 3, respectively.

By "a" natural module" for $SL(2,p^n)$ we mean any module for $SL(2,p^n)$ which is isomorphic over $\mathbb{F}_p$ to "the" natural module for $SL(2,p^n)$ (and by which we mean the vector space of dimension 2 over $\mathbb{F}_{p^n}$ on which $SL(2,p^n)$ acts by matrix multiplication). We also have the notion of a natural $\Omega_3(p^n)$- module and, for n even, a natural $\Omega_4^-(p^n)$-module for $SL(2,p^n)$, given by identifying $PSL(2,p^n)$ with one or the other of these orthogonal groups. In the same way, we have the notion of a natural module for $SU(3,p^n)$. A natural module for a Suzuki group $Sz(2^n)$ is, by definition, any irreducible module of dimension 4 over $\mathbb{F}_{2^n}$ for $Sz(2^n)$ (n odd), it being known from [St2] that all such modules are isomorphic over $\mathbb{F}_2$ to a module obtained from an embedding of $Sz(2^n)$ in $Sp(4,2^n)$ as the fixed points of a symplectic polarity. The notions of natural modules for $SL(3,p^n)$ and $Sp(4,p^n)$ should now require no further explanation. If V is a natural module for $Sp(4,2^n)$ then a "contragredient module" associated with V is, by definition, the image of V under a symplectic polarity.

We require also some terminology concerning the groups A which enter into the various hypotheses stated above. Thus, let V be a vector space over $\mathbb{F}_p$, and let G be a subgroup of $GL(V)$. A subgroup A of G is said to act **quadratically** on V (or to be a **quadratic subgroup** of G) if $A \neq 1$ and $[V, A, A] = 0$. It is an entirely elementary result that such a group A is necessarily an elementary abelian p-group (for which see lemma 1.1 in [C1], for example). Let Y be a subgroup of G. We denote by $\mathcal{Q}(Y,V)$ the set of all quadratic subgroups A of Y. Assuming that $\mathcal{Q}(Y,V) \neq \emptyset$, we then define $q(Y,V)$ to be the smallest real number q for which there exists $A \in \mathcal{Q}(Y,V)$ with $|A|^q|C_V(A)| = |V|$. We then set

$$\mathcal{Q}^*(Y,V) = \{A \in \mathcal{Q}(Y,V) \mid |A|^{q(Y,V)}|C_V(A)| = |V|\}.$$

For $i = 1$ and 2, we say that V is an $\boldsymbol{Fi}$**-module** for G if there exists a non-identity elementary abelian p-subgroup A of G such that $|A|^i \geq |V/C_V(A)|$, and that V is a **quadratic** $\boldsymbol{Fi}$**-module** if such an A can be chosen in $\mathcal{Q}(G,V)$. The group A is then said to be an $\boldsymbol{Fi}$**-offender** on V, and a **quadratic** $\boldsymbol{Fi}$**-offender** if also A acts quadratically on V. If $|A| = p$ and A is an $F2$-offender on V then any non-identity element of A is said to be a **2-transvection** on V.

We may now state our main results.

Theorem 1. *Assume Hypothesis 4. Then there exists a subgroup K of H, unique up to conjugation, such that, upon setting $U = [V, K]$, the following conditions hold.*

(a) *$H = K_1 \times \cdots \times K_r$ where $\{K_1, \cdots, K_r\} = K^S$.*

(b) *We have $[V, K_i, K_j] = 0$ whenever $i \neq j$.*

(c) *One of the following holds:*

   (i) *$K \cong O^p(SL(2, p^n))$, $n \geq 1$, and $U/C_U(K)$ is a natural $SL(2, p^n)$-module for K, or a direct sum of two natural modules for K.*

   (ii) *$K \cong O^p(O_4^{\epsilon}(p^n))$, $n \geq 1$, $\epsilon = \pm 1$, and U is a natural orthogonal module for K.*

   (iii) *$K \cong O^p(SU(3, p^n))$ and U is a natural module for K.*

   (iv) *$p = 2$, $K \cong O^2(Sz(2^n))$, and U is a natural module for K.*

   (v) *$p = 2$, $A \leq C_G(K)K$, $K \cong SL(3, 2^n)$ (resp. $O^2(Sp(4, 2^n))$) and U is the direct sum of a natural and a dual module (resp. a natural and a contragredient module) for K. Moreover, there exists $g \in N_S(K)$ such that g interchanges, by conjugation, the two maximal subgroups of K containing $S \cap K$.*

   (vi) *$p = 2$, $K \cong Alt(2^n + 1)$, $n \geq 3$, and U is a natural module for K, or a direct sum of two natural modules for K.*

   (vii) *$p = 2$, $K \cong Alt(9)$, and U is a spin module for K, of dimenson 8 over $\mathbb{F}_2$.*

Moreover, if K is not invariant under $\mathcal{Q}^*(S, V)$ then $p = 2$, $K \cong \mathbb{Z}_3$, $|U| = 4$, and $q(S, V) = 2$.

Two special cases of Theorem 1 are of importance in their own right, where $q(A, V) < 2$, and where $q(A, V) \leq 1$. Theorems 2 and 3 describe the possible outcomes in these two cases.

Theorem 2. *In Theorem 1, suppose that we have $q(A, V) < 2$. Then one of the following holds.*

(i) *$K \cong O^p(SL(2, p^n))$, $n \geq 1$, and $U/C_U(K)$ is a natural $SL(2, p^n)$-module for K.*

(ii) *$p = 2$, $KA/C_{KA}(K) \cong O_4^{\epsilon}(2^n)$, $n \geq 1$, $\epsilon = \pm 1$, and U is a natural orthogonal module for K. Moreover, we have $|A/C_A(K)| = 2^{n+1}$, and if $n = 1$ then $\epsilon = -1$.*

(iii) *$p = 2$, $A \leq C_G(K)K$, $K \cong SL(3, 2^n)$ and U is the direct sum of a natural and a dual module for K. Moreover, there exists $g \in N_S(K)$ such that g interchanges, by conjugation, the two maximal subgroups of K containing $S \cap K$.*

(iv) *$p = 2$, $K \cong Alt(2^n + 1)$, $n \geq 3$, and U is isomorphic to the natural module for K.*

Theorem 3. *In Theorem 1, suppose that we have $q(S, V) \leq 1$. Denote by $\mathcal{A}(S, V)$ the set of all subgroups A of S such that $|A| \geq |V/C_V(A)|$ and such that $[V, A, A] = 0$. Then*

$q(S,V)=1$ and $H \leq \langle \mathcal{A}(S,V)^G \rangle = E_1 \cdots E_r$ where E_i is a subnormal subgroup of G and where one of the following holds.

(i) *$E_i \cong SL(2,p^n)$, $n \geq 1$, and $[V,E_i]$ is a natural $SL(2,p^n)$-module for E_i.*

(ii) *$p=2$, $E_i \cong Sym(2^n+1)$, $n \geq 2$, and $V = C_V(E_i) \oplus [V,E_i]$, where $[V,E_i]$ is isomorphic to the natural module for E_i.*

In Theorems 4,5, and 6 we drop the assumption that A acts quadratically.

Theorem 4. *Assume Hypothesis 3, and assume that H is a quasisimple group of Lie type in characteristic p. Let A be an $F2$-offender on V. Then one of the following holds.*

(a) *$H \cong SL(2,p^n)$ and one of the following holds.*

  (i) *V is a natural $SL(2,p^n)$-module for H.*

  (ii) *V has an H- submodule U such that both U and V/U are natural $SL(2,p^n)$-modules for H.*

  (iii) *p is odd, $H \cong L_2(p^n)$, and V is a natural $\Omega_3(p^n)$-module for H.*

  (iv) *n is even and V is a natural $\Omega_4^-(p^{n/2})$-module for H.*

(b) *$H \cong SU(3,p^n)$ and V is a natural module for H.*

(c) *$p=2$, $H \cong Sz(2^n)$, and V is a natural module for H.*

(d) *$p=2$, $H \cong SL(3,2^n)$ (resp. $O^2(Sp(4,2^n))$) and V is the direct sum of a natural and a dual module (resp. a natural and a contragredient module) for H. Moreover, there exists $g \in N_S(K)$ such that g interchanges, by conjugation, the two maximal subgroups of H containing $S \cap H$. If A is a quadratic $F2$-offender then $A \leq H$, and if also $H \cong Sp(4,2^n)$ then A is conjugate to $Z(S)$.*

Theorem 5. *Assume Hypothesis 4′, and assume that $H/Z(H)$ is isomorphic to $Alt(n)$, $n \geq 5$. Assume also that $H/Z(H)$ is not of Lie type in characteristic p, and if $p=2$ assume that n is odd. Then one of the following holds.*

(i) *$p=2$, $H \cong Alt(n)$, $n \geq 5$, and V is a natural module for H.*

(ii) *$p=2$, $H \cong Alt(n)$, $n=5,7$, or 9, and V is a spin module for H (of dimension 4, 4, or 8, respectively). Moreover, if $n=9$ then A is the direct product of two quadratic fours groups in H.*

(iii) *$|A|=p=3$, $G \cong Alt(n)$, $n \neq 6$, and V is a natural module for G. Moreover, A is generated by a 3-cycle.*

(iv) *$|A|=p=3$, $H \cong SL(2,5)$, and V is isomorphic to the natural $SL(2,9)$-module for H.*

(v) *$p=3$, $H \cong Alt(9)$, $|A|=27$, and V is a spin module for H (of dimension 8 over $\mathbb{F}_3$). Moreover, we have $|A|^2 = |V/C_V(A)|$.*

Theorem 6. *Assume Hypothesis 4′, and assume that S is contained in a unique maximal subgroup of G. Assume also that $H/Z(H)$ is a quasisimple group of Lie type in characteristic different from p, or a sporadic group, and that there exists no isomorphism of $H/Z(H)$ with a group of Lie type in characteristic p. Then $p=3$, $G/Z(H) \cong Sp(6,2)$, $|A|^2 = |V/C_V(A)|$, and one of the following holds.*

(i) *$|A|=3$, $Z(H)=1$, and V has dimension 7 over $\mathbb{F}_3$.*

(ii) *$|A| = 27$, $|Z(H)| = 2$, and V has dimension 8 over $\mathbb{F}_3$.*

We mention that the case where G is solvable is hidden in Theorem 1. Section 4, below, contains many results concerning the case where $F^*(G)$ is solvable, and which are not revealed in the statements of Theorems 1 through 6. Of these results, 4.6 is the most important, and figures strongly in the proof of 11.1. There is a certain sense in which this case forms the core of this paper, and we therefore invite the reader to glance through section 4 before undertaking a thorough reading of the whole.

We attempt to list our notational conventions, many of which stem from the ATLAS), and to list also those cases where we are torn between competing conventions. We denote by 2^{1+2n}_ϵ an extraspecial 2-group T whose corresponding orthogonal space $T/Z(T)$ has "defect" ϵ, where $\epsilon = 1$ or -1. But we also write Q_8 and D_8 for the quaternion and dihedral groups, respectively, of order 8, and we write $X \circ Y$ for the "central product" of the groups X and Y, this being the direct product, modulo the relations which identify the centers of X and Y, and which is defined only only if those centers are isomorphic. An alternative notation for the groups 2^{1+2n}_ϵ is given by the iterated central products $D_8^{(n)}$ and $Q_8^{(n)}$.

The symbol $[n]$ indicates a group of order n, and if p is a prime then p^n is often used to denote an elementary abelian group of order p^n. If X and Y are groups then $X.Y$ or $(X).Y$ or sometimes just XY is said to be the "shape" of a group G provided that G has a normal subgroup $X*$ isomorphic to X, with $G/X*$ isomorphic to Y, and with G not isomorphic to the direct product of X and Y. Conventional notation for the groups of Lie type will always be taken to give the corresponding adjoint version. So, the center of the group ${}^2A_n(q)$, for example, is trivial. We often write $L_n(q)$ for $PSL(n, q)$, and $U_n(q)$ for $PSU(n, q)$. In general we write $[X, X]$ for the commutator subgroup of a group X, but in the case where X is a group of Lie type or, more specifically, a classical group, we feel free to use the "apostrophic" notation to indicate derived groups. Thus, $Sp(4, 2^n)'$, or $U_3(2)'$, or ${}^2F_4(2)'$, for example. Our hope is that other notation, which we have not had the foresight to introduce at this point, will be self- explanatory.

Section 1: Decomposability questions

1.1 Lemma. *Let G be a group acting faithfully on a vector space V over $\mathbb{F}_p$. Let T be a Sylow p-subgroup of $O^p(G)$, and assume that $V = \langle C_V(T)^G \rangle$. Then $V = [V, O^p(G)] + C_V(O^p(G))$.*

Proof. Set $H = O_p(G)$, let $\{h_1, \cdots, h_r\}$ be a right transversal for T in H, let u be a non-zero element of $C_V(T)$, and set $v = u^{h_1} + \cdots + u^{h_r}$. Each $g \in H$ defines a permutation in $Sym(r)$ by means of the formula $h_i g \in T h_{ig}$, and then

$$v^g = u^{h_1 g} + \cdots + u^{h_r g} = u^{h_{1g}} + \cdots + u^{h_{rg}} = v.$$

If $u \notin [V, H]$ then $v = ru + w$ for some $w \in [V, H]$, and so $ru \in [V, H] + C_V(H)$. As p

does not divide r, we conclude that $C_V(T) \leq [V,H] + C_V(H)$. As $V = \langle C_V(T)^G \rangle$, we then have the lemma. $\square$

1.2 Corollary. *Assume Hypothesis 2, and suppose that there is a unique non-trivial irreducible constituent for G in V. Then V is irreducible.*

Proof. Immediate from 1.1. $\square$

1.3 Lemma. *Let (L,U) be a pair consisting of a group L and an irreducible $\mathbb{F}_2[L]$-module U. Assume that (L,U) is given by one of the following:*

(1) *$L \cong SL(2,2^n)$, U the natural module.*
(2) *$L \cong \Omega_4^\epsilon(2^n)$, $\epsilon = \pm 1$, U the natural orthogonal module.*
(3) *$L \cong SL(3,2^n)$, U the natural module.*
(4) *$L \cong Sp(4,2^n)'$, U the natural module for $Sp(4,2^n)$.*
(5) *$L \cong Alt(n)$, U the natural module.*

Then one of the following holds.

(i) *$H^1(L,U) = 0$.*
(ii) *$L \cong SL(2,2^n)$ and $H^1(L,U) \cong \mathbb{F}_{2^n}$.*
(iii) *$L \cong SL(3,2)$ and $H^1(L,U) \cong \mathbb{F}_2$.*
(iv) *$L \cong Sp(4,2^n)'$ and $H^1(L,U) \cong \mathbb{F}_{2^n}$.*
(v) *$L \cong Alt(n)$, n even, and $H^1(L,U) \cong \mathbb{F}_2$.*

Proof. In each of the cases to be considered, let W denote an L-module containing U, with $[W,L] = U$ and with $C_W(L) = 0$. Suppose first that $L \cong SL(2,2^n)$ and that U is the natural module for L. For any involution t in L we have $[W,t] \leq C_U(t)$, and hence $|W/C_W(t)| \leq 2^n$. Since three involutions suffice to generate L, it follows that $|W| \leq 2^{3n}$. On the other hand, one may produce an example where $|W| = 2^{3n}$, in the following way. Put $L^* = SL(2,2^{2n})$ and regard L as a subgroup of L^*. Identify L^* with $\Omega_4^-(2^n)$ and let V be the natural orthogonal module for L^*. Then L centralizes a 1-dimensional singular subspace V_0 of V, and by taking $W = V/V_0$ we obtain the desired example. Thus $|H^1(L,U)| = 2^n$.

Next, take $L = \Omega_4^-(2^n)$, U the natural orthogonal module. Assume that $|W/U| = 2$. Put $q = 2^n$ and let D be a subgroup of L of order $q+1$. Then $|C_W(D)| = 2q^2$. For any involution t of L one then has $C_W(\langle D,t \rangle) \neq 0$. But an elementary counting argument shows that one may choose t so that $\langle D,t \rangle$ is not an $SL(2,2^n)$-subgroup of L, and is not a dihedral group of order $2(q+1)$. Then $\langle D,t \rangle = L$, by appeal to Dickson's list of subgroups of L. That is, $C_W(L) \neq 0$, so W is decomposable after all, and $H^1(L,U) = 0$.

Assume next that $L = \Omega_4^+(2^n)$, U the natural module, and form the semi-direct product $H = U : L$. Let $K = K_1 \times K_2$ be a complement to U in H, $K_i \cong SL(2,2^n)$. After a suitable conjugation, we may assume that $K \cap L$ contains a subgroup $X = X_1 \times X_2$, where $X_i = X \cap K_i$ is of order $2^n + 1$. But $C_U(X_i) = 0$, so $C_H(X_i) = X_i K_{3-i}$. This shows that $K = L$, and so there is only one conjugacy class of complements to U in H. That is, $H^1(L,U) = 0$.

We next consider the case where $L = SL(3, 2^n)$ or $Sp(4, 2^n)'$. Let P_1 and P_2 be the two maximal subgroups of L containing a fixed Sylow 2-subgroup S of L. Put $L_i = [P_i, P_i]$, $Q_i = O_2(P_i)$, and $Z_i = C_{Q_i}(L_i)$, and let the indexing be chosen so that $C_U(L_1) \neq 0$.

Assume now that $L \cong SL(3, 2^n)$, $n > 1$. Assume that $|W/U| = 2$, and let K be a complement to Q_2 in L_2. Then both Q_2 and $C_U(Q_2)$ are natural $SL(2, 2^n)$-modules for K, so we have $|Hom_K(Q_2, C_U(Q_2))| = 2^n$. Then $[W, L_2] \leq C_U(Q_2)$, and so $W = U + C_W(Q_2)$. Then $[W, Q_1 \cap Q_2] \leq [U, Q_1] = C_U(L_1)$, and then also $[W, Q_1] = [W, \langle (Q_1 \cap Q_2)^{L_1} \rangle] \leq C_U(L_1)$. This yields $|C_W(Q_1)| = |C_W(L_1)| = 2^{n+1}$. But also, for any involution $t \in L$ we have $|W/C_W(t)| = 2^n$. Choosing $t \in L - L_1$, we get $L = \langle L_1, t \rangle$, and so $C_W(L) \neq 0$. Thus $H^1(L, U) = 0$.

One may produce an indecomposable module for $L = L_3(2)$ by considering the action of $Alt(7)$ on the natural $L_4(2)$-module, and observing that $Alt(7)$ contains two classes of $L_3(2)$-subgroups. Thus $|H^1(L, U)| \geq 2$ in this case. Let W be an L-module of order 32, with $U = [W, L]$. For any $y \in L$ with $|y| = 3$ one has $|[W, y]| = 4$, and since two conjugates of y suffice to generate L we then have $C_W(L) \neq 0$. This shows that $|H^1(L, U)| = 2$ if $L \cong L_3(2)$.

Next, suppose that $L \cong Sp(4, 2^n)$, $n > 1$, and assume that $|W/U| > 2^n$. We have $|U/C_U(Z_1)| = |[U, Z_1]| = 2^n$, and $[W, L_1] \leq C_U(Z_1)$. The Three Subgroups Lemma yields $[W, Z_1, L_1] = 0$, and so $[W, Z_1] = [U, Z_1]$. Let K_1 be a complement to Q_1 in L_1 such that K_1 is generated by two conjugates of Z_1. Then $|[W, K_1]|| \leq 2^{2n}$, and $[W, K_1]$ is a natural $SL(2, 2^n)$-module for K_1. By what has already been proved, we have $|H^1(K_1, [W, K_1])| = 2^n$, and so there exists $w \in W - U$ with $[w, K_1] = 0$. Then also there exists $v \in W - U$ with $[v, Z_1] = 0$. Set $W_0 = \langle v \rangle + U$. As four conjugates of Z_1 suffice to generate L we then have $C_{W_0}(L) \neq 0$, contrary to assumption. This shows that $|H^1(L, U)| \leq 2^n$. To see that equality holds, it is enough to observe that in $Sp(6, 2^n)$ there is a maximal parabolic subgroup P with $O^{2'}(P/O_2(P)) \cong L$ and with $O_2(P)$ an indecomposable module for $O^{2'}(P)$, such that $C_{O_2(P)}(O^{2'}(P))$ is of order 2^n and such that $O_2(P)/C_{O_2(P)}(O^{2'}(P))$ is a natural $SL(2, 2^n)$-module for $O^{2'}(P/O_2(P))$. (This is entirely well known, but one can find this worked out in detail in lemma 5.4 of [C2].)

Suppose next that $L = (Sp(4, 2))'$. The natural permutation module for $Alt(6)$ provides an example which shows that $|H^1(L, U)| \geq 2$. Let W be an L-module of order 64 with $U = [W, L]$, and let L_0 be a subgroup of L, $L_0 \cong Alt(5)$, such that U is the natural $\Omega_4^-(2)$-module for L_0. By what has already been shown, we have $H^1(L_0, U) = 0$, and so $W = U \oplus C_W(L_0)$. Let S be a Sylow 2-subgroup of L such that $|S \cap L_0| = 4$, and let t be an involution in $S - L_0$. Here $|C_U(S \cap L_0)| = 2$, and so $C_W(L_0) \cap C_W(t) \neq 0$. As $\langle L_0, t \rangle = L$ we then have $C_W(L) \neq 0$, and this shows that $|H^1(L, U)| = 2$.

Finally, let $L = Alt(n)$, with U the natural module. Suppose that $n = 2m + 1$ is odd. Then L is generated by m 3-cycles, each of which centralizes a subspace of codimension 2 in W. Then $dim(W) \leq 2m = dim(U)$. Thus $W = U$, and $H^1(L, U) = 0$ in this case. Now suppose that $n = 2m$ is even. Then $m - 1$ 3-cycles suffice to generate the subgroup K_i of L which fixes the point i in the natural action of L on n points. Here $C_U(K_i) = 0$, and $dim(U) = 2m-2$, so we have $W = U + C_W(K_i)$. Set $X = K_1 \cap K_2$, and observe that $dim(C_U(X)) = 1$. Thus $C_W(K_i)$ is a hyperplane of $C_W(X)$, for $i = 1$ and

2. As $\langle K_1, K_2 \rangle = G$ we have $C_W(K_1) \cap C_W(K_2) = 0$, and we conclude that $|W/U| \leq 2$. On the other hand, the natural permutation module for L, modulo its fixed-points for L, provides an example of an indecomposable module W in which $|W/U| = 2$. Thus $|H^1(L, U)| = 2$ in this case, and the lemma is proved. $\square$

1.4 Lemma. *Let L be the group $L_2(q)$, q a power of p, p odd, and let V be a module for L over $\mathbb{F}_p$, such that $[V/C_V(L), L]$ is isomorphic to the natural $\Omega_3(q)$-module for L. Then $V = [V, L] \oplus C_V(L)$.*

Proof. Let T be a Sylow p-subgroup of L, let D be a complement to T in $N_L(T)$, let U be the natural $\Omega_3(q)$-module for L, and form the semi-direct product $U : L$. We will show that there is a unique conjugacy class of D-invariant complements to U in UT, and the lemma will follow from a standard result on 1-cohomology. (See 17.7 in [A3].)

Let T_1 be a D-invariant complement to U in UT, and set $X = \langle T^U \rangle$. Then $X = [U, T]T$, where $[U, T]$ is a 2-dimensional $\mathbb{F}_q$- subspace of U. Every element of order p in UT lies in X, so we have $T_1 \leq X$. Notice that D acts trivially on the 1-dimensional space $[U, T]/C_U(T)$, and so the q distinct conjugates of T under $[U, T]$ are all D-invariant. These conjugates, together with $C_U(T)$, provide a partition of $(C_U(T)T)^\#$ into D-invariant sets, so if $T_1 \leq C_U(T)T$ then T_1 is conjugate to T. Suppose now that $q > 3$, so that $D \neq 1$. Then $[X, D] = C_U(T)T$, and so $T_1 \leq C_U(T)T$ in this case. Thus, we are reduced to the case $p = 3$. Here there are exactly 9 conjugates of T under U, and there are exactly $13 = (3^3 - 1)/(3 - 1)$ subgroups of X of order 3, four of which lie in U. Thus T_1 is conjugate to T in this case as well, and the lemma is proved. $\square$

1.5 Lemma. *Let $L = L_3(2)$ and let V be an $\mathbb{F}_2L$-module such that $C_V(L) \leq [V, L]$, and such that $[V/C_V(L), L]$ is a natural $L_3(2)$-module for L. Then either $V = [V, L]$ or $C_V(L) = 0$.*

Proof. Suppose false. Then 1.1 implies that $|V/[V, L]| = |C_V(L)| = 2$, and so $|V| = 32$. Let t be an involution in L. Then two conjugates of t generate a Sylow 2-subgroup of L, and then three conjugates of t suffice to generate L. If t induces a transvection on $[V, L]$ we then obtain $C_{[V,L]}(L) \neq 0$, while if t induces a transvection on $V/C_V(L)$ then L has a non-trivial fixed-point on $V/C_V(L)$. These results are contrary to the case, so we conclude that t induces a 2- transvection on both $[V, L]$ and $V/C_V(L)$. Then $C_V(t) \leq [V, L]$, and $|V/C_V(t)| \geq 8$. But $|V/C_V(t)| \leq 4$ as $|V| = 32$. This contradiction proves the lemma. $\square$

1.6 Lemma. *Let $L = SL(2, p^n)$ and let U be a module for L over $\mathbb{F}_p$. Suppose that every irreducible constituent for L in U is a natural module for L. If $p = 3$ assume further that a Sylow p-subgroup of L acts quadratically on U. Then U is completely reducible.*

Proof. This is an old result of Richard Niles (Theorem 3.2 in [N]). To be precise, Niles' theorem states that if the Sylow p-subgroup S of L does *not* act quadratically on V, and V is indecomposable, then $p = 3$. But in fact, Niles' proof makes no use of the assumption that S acts non-quadratically, and what is really proved is that if V is indecomposable then $p = 3$ and S acts non-quadratically. The lemma follows from this result. $\square$

1.7 Lemma. *Let $L = SL(2, p^n)$, and let $V = [V, L]$ be a non-zero module for L over $\mathbb{F}_p$. Suppose that a Sylow p-subgroup of L acts quadratically on V, and if $p = 2$ assume that $C_V(X) = 0$ for some Cartan subgroup X of L. Then V is a direct sum of natural modules for L.*

Proof. If p is odd then $C_U(Z(L)) = C_U(L)$, and we may assume that $C_U(Z(L)) = 0$ in this case. Let U be an irreducible L-invariant section of V. Then U is a non-trivial L-module, since $C_U(X) = 0$ if $p = 2$. Let S be a Sylow p-subgroup of L, and set $F = End_L(U)$. As is well known (see Corollary (a) to Theorem 46 in [St2]), F is a subfield of $\mathbb{F}_{p^n}$ and $dim_F(C_U(S)) = 1$. As S acts quadratically on V, by hypothesis, and as two conjugates of S generate L, it follows that $dim_F(U) = 2$, and then $F = \mathbb{F}_{p^n}$ and U is a natural module for L. Thus, we are reduced to the situation in which V has a submodule U such that both U and V/U are natural modules for L. Now apply 1.6. □

1.8 Lemma. *Let $L = Alt(n)$, n odd, and let V be an $\mathbb{F}_2L$-module such that the only non-trivial irreducible constituents for L in V are natural modules. Then V is completely reducible.*

Proof. In view of 1.3, we may assume that $C_V(L) = 0$, and then that V has a submodule U such that both U and V/U are natural modules for $O^2(L)$. Let K be the stabilizer of a point for the natural action of L on n points. As n is odd, U is isomorphic, as a K-module, to the natural permutation module for K. As $n - 1$ is even we then have $U \neq [U, K] \geq C_U(K) \neq 0$, and the same is true with V/U in place of U. As $H^1(K, [U, K]/C_U(K)) \cong \mathbb{F}_2$, by 1.3, it follows that $C_{V/U}(K) = (U + C_V(K))/U \neq 0$. Let $w \in C_V(K) - U$ and set $W = \langle w^{O_2(L)} \rangle$. Then $dim(W) \leq |O^2(L) : K| = n$, and so W is an $O^2(L)$-invariant complement to U in V. □

Section 2: Cyclic Sylow p-subgroups

In this section we treat Hypothesis 4′, in "miniature".

2.1 Lemma. *Let V be a 4-dimensional vector space over $\mathbb{F}_p$, p an odd prime, and set $G = SL(V)$. Let X be a quasisimple subgroup of G, and assume that X satisfies the following conditions.*

(a) *$Z(X) \leq Z(G)$.*
(b) *X has cyclic Sylow p-subgroups.*
(c) *For any element a of X of order p, we have $[V, a, a, a] = 0$ and $[V, a, a] \neq 0$.*

Assume further that $X/Z(X)$ is an alternating group, a group of Lie type, or one of the twenty-six sporadic groups. Then one of the following holds.

(i) *$p \geq 5$, $X \cong L_2(p)$, $V = [V, X] \oplus C_V(X)$, and $[V, X]$ is a natural $\Omega_3(p)$-module for X (of dimension 3).*
(ii) *$p = 3$ and $X \cong Alt(5)$.*

Proof. The 2-rank of $SL(4,p)$ is equal to 3, so we obtain the following information at the outset.

(1) The 2-rank of X is at most 3, and if equal to 3 then $Z(X)$ is of even order.

Suppose first that $X \in Lie(p)$. Condition (b) then implies that $X \cong L_2(p)$ or $SL(2,p)$, and then since X is assumed to be quasisimple, we have $p \neq 3$. Denote by M_i the space (of dimension $i+1$) of homogeneous polynomials of degree i in the two variables x and y. Then M_i admits a natural action by $SL(2,p)$, and $\{M_i\}_{0\leq i\leq p-1}$ forms a complete set of representatives for the isomorphism classes of the irreducible modules for $SL(2,p)$ over $\mathbb{F}_p$. (See [St 1] or section 13 in [St 2].) Let S be a Sylow p-subgroup of $SL(2,p)$. One checks easily that $[M_i,S,S,S] \neq 0$ for $i>2$, and so condition (c) implies that any irreducible constituent U for X in V is isomorphic to one of the modules M_i, $0\leq i\leq 2$. That is, U is either a trivial module, a natural $SL(2,p)$-module, or a natural $\Omega_3(p)$-module for X. If there exists a constituent U such that U is a natural $SL(2,p)$-module then $1 \neq Z(X) \leq Z(G)$, by condition (a), so all irreducible constituents of X in V are natural $SL(2,p)$- modules, and then V is completely reducible for X, by 1.6. But then a acts quadratically on V, contrary to (c), so we conclude that no such constituent U exists. Thus, X has a unique non-trivial irreducible constituent U in V, and U is a natural $\Omega_3(p)$-module. Now 1.2 implies that V is completely reducible, and so (i) holds.

Suppose next that X is of Lie type in characteristic different from p. We appeal to Table I in [SZ] for the list of minimal degrees of cross-characteristic projective representations of groups of Lie type, where we find that only the groups $L_2(4)$, $L_2(9)$, $L_3(2)$, $L_3(4)$, and $U_4(2)$ have such representations of degree at most 4. Suppose that $X/Z(X) \cong L_2(4)$. Then $p=3$ (as $L_2(4) \in Lie(5)$). If $Z(X) \neq 1$ then there is an element f of order 4 in X such that f inverts a, with $\langle f^2\rangle = Z(X)$, and since $|[V,a,a]| = 3$ it follows that $Z(X)$ centralizes $[V,a,a]$. But $C_V(Z(X)) = 0$, so in fact $Z(X)=1$, and (ii) holds. Suppose that $X/Z(X) \cong L_3(2)$. Then $p=3$ as $L_3(2) \in Lie(7)$. As 7 does not divide the order of G, we have a contradiction in this case. We note that any central extension of $L_3(4)$ has 2-rank at least 4, so (1) implies that $X/Z(X)$ is not isomorphic to $L_3(4)$. Suppose that $X/Z(X) \cong U_4(2)$. The 2-rank of $U_4(2)$ is greater than 3, $U_4(2) \cong PSp(4,3)$, and $Sp(4,3)$ is the universal perfect central extension of $U_4(2)$, so we have $X \cong Sp(4,3)$ and $p=5$. But 27 does not divide the order of $SL(4,5)$, so we have a contradiction. Now suppose that $X/Z(X) \cong L_2(9)$. Then $X/Z(X) \in Lie(2) \cup Lie(3)$, and so $p=5$. There are then non-conjugate subgroups K_1 and K_2 of X, with $K_i/Z(X) \cong L_2(5)$, and with $a \in K_1 \cap K_2$. The argument in the preceding paragraph then shows that for each i we have $K_i \cong L_2(5)$, V is completely reducible for K_i, and $[V,K_i]$ is a natural $\Omega_3(5)$-module for K_i. Let x_i be an element of order 3 in K_i. It now follows that $dim(C_V(x_i)) = 2$. On the other hand, a Sylow 3-subgroup of X is one of G, and evidently G contains an element x of order 3 such that $C_V(x) = 0$. As x_1 and x_2 represent the two conjugacy classes of elements of order 3 in X, we have a contradiction.

Suppose next that $X/Z(X)$ is an alternating group $Alt(n)$. The 2-rank of any central extension of $Alt(8)$ is at least 4, so (1) implies that $n \leq 7$. As $Alt(5)$ and $Alt(6)$ are of Lie type, we then have $n = 7$. By condition (b), $p \neq 3$, and since $Alt(7)$ contains $L_2(9)$ we have $p \neq 5$. Then $p = 7$, and since $Alt(7)$ contains $L_2(7)$ we have $Z(X) = 1$. The minimal degree of a non-trivial complex irreducible representation of $Alt(6)$ is greater than 4, and since $|Alt(6)|$ is not divisible by 7 the same is true of the irreducible representations of $Alt(6)$ over $\mathbb{F}_7$. Thus, $Alt(7)$ is not a subgroup of G.

Suppose finally that $X/Z(X)$ is a sporadic group. Then (1) implies that $X \cong M_{11}$ or $2^{\cdot M_{12}}$. Then $p \neq 3$, by (b), and since M_{11} is a subgroup of $2^{\cdot}M_{12}$ it will now suffice to derive a contradiction in the case that $X \cong M_{11}$. In this case we have $p = 5$ or 11, and since M_{11} contains $L_2(9)$ we conclude that $p = 11$. Let B be a Sylow 3-subgroup of X. Then all subgroups of order 3 in B are fused in X. But also B is a Sylow subgroup of G, and evidently there are two different classes of elements of subgroups of order 3 in G. This contradiction proves the lemma. □

2.2 Corollary. *Assume Hypothesis 3, with H quasisimple, and assume that S is of order p. Suppose further that p is odd, that $[V, A, A, A] = 0$, and that A is not quadratic on V. Then $G \cong L_2(p)$ or $Alt(5)$.*

Proof. By Hypothesis 3 there is a unique maximal subgroup M of G containing A. As H is quasisimple, there exists $g \in G$ with $A^g \not\leq M$. Then $\langle A, A^g \rangle = G$, and so $G \cong L_2(p)$ or $Alt(5)$ by 2.1. □

2.3 Theorem. *Assume Hypothesis $4'$, and assume that $H/Z(H)$ is one of the twenty-six sporadic groups. Then S is contained in more than one maximal subgroup of G.*

Proof. By 2.2, $|S| > p$, and then a survey of the sporadic groups shows that S is non-cyclic. In [A3] it is shown that if X is a group with $F^*(X)$ sporadic, and T is a non-cyclic Sylow p-subgroup of X, then either T is contained in two distinct maximal subgroups of X, or else $X \cong J_4$ and $p = 11$. Moreover, it is shown that if J_4 has a faithful 112-dimensional module over $\mathbb{F}_2$ then also for $p = 11$ there are at least two maximal overgroups of T in J_4. The existence of such a module for J_4 is now known from various sources. (?) □

Section 3: Measuring lemmas

3.1 Lemma. *Let G be a group, and let V be a faithful $\mathbb{F}_pG$-module. Suppose G has a cyclic subgroup of order $p^k + 1$. Then $dim(V) \geq 2k$.*

Proof. Suppose first that $p^{2k} = 2^6$. Then $p^k + 1 = 9$, and since $L_5(2)$ has elementary abelian Sylow 3-subgroups we are done in this case. Also, the result evidently obtains if $k = 1$. Thus, we may assume that $p^{2k} \neq 2^6$ and that $k > 1$. The main result of [Z] then says that $p^{2k} - 1$ is divisible by a prime r such that r does not divide $p^i - 1$ for any i with $1 \leq i < 2k$. Then r does not divide $|GL(V)|$ if $dim(V) < 2k$. □

[For sure there is a proof of 3.1 that does not use [Z].]

The next result is extracted from [CD].

3.2 Lemma. *Let X be a finite group, Y a normal subgroup of X, p a prime, and V a faithful $\mathbb{F}_pX$-module. Let r be a positive real number, and let E be an elementary abelian p-subgroup of Y, chosen so that*

$$(*) \qquad |E|^r|C_V(E)| \quad \textit{is as large as possible.}$$

Then For any $x \in X$ we have $|EE^x|^r|C_V(EE^x)| \geq |E|^r|V/C_V(E)|$. In particular, If E is chosen to be as large as possible, subject to (*), then E is weakly closed in $C_X(E)$ with respect to X.

Proof. . Set $F = E^x$, and suppose that $|E|^r|C_V(E)| > |EF|^r|C_V(EF)|$. We then have

$$\frac{|F|^r}{|E \cap F|^r} = \frac{|EF|^r}{|E|^r} < \frac{|C_V(E)|}{|C_V(EF)|} = \frac{|C_V(E) + C_V(F)|}{|C_V(F)|} \leq \frac{|C_V(E \cap F)|}{|C_V(F)|},$$

and hence

$$(**) \qquad |F|^r|C_V(F)| < |E \cap F|^r|C_V(E \cap F)|.$$

But $|F|^r|C_V(F)| = |E|^r|C_V(E)|$, and the maximality of this number, among elementary abelian subgroups of X, contradicts (**). Thus $|E|^r|C_V(E)| \leq |EF|^r|C_V(EF)|$. □

3.3 Lemma. *Let X be a finite group, p a prime, and V a faithful $\mathbb{F}_pX$-module. Let A be a subgroup of X, and let r be a real number such that $|A|^r \geq |V/C_V(A)|$. Then let B be a normal subgroup of A, set $W = C_V(B)$, and suppose that $|A/B|^r \leq |W/C_W(A)|$. Then $|B|^r \geq |V/C_V(B)|$.*

Proof. As $|A|^r \geq |V/C_V(A)|$ and $|A/B|^r \leq |W/C_W(A)|$, we have

$$|B|^r|C_V(A)||W|/|C_W(A)| \geq |V|.$$

But $C_W(A) = C_V(A)$, so we obtain $|B|^r \geq |V/W| = |V/C_V(B)|$, as required. □

We end this section with a result which will effectively reduce the proof of Theorem 1 to the consideration of the case where $F^*(G)$ is quasisimple or where $F^*(G)$ is a q-group for some prime q, $q \neq p$.

3.4 Lemma. *Assume Hypothesis 1, and let $A \in \mathcal{Q}(S, V)$ with $A \in \mathcal{Q}^*(A, V)$. Let X be a non-identity subgroup of G with $X = [A, X]$, and such that $X/\Phi(X)$ is a minimal normal subgroup of $AX/\Phi(X)$. Let A_0 be a complement in A to $C_A(X)$. Then the following hold:*

(a) $[V, X, C_A(X)] = 0$.

(b) *For any AX-invariant section W of $[V, X]$ on which X acts non-trivially, we have $C_{A_0}(W) = 1$, and:*

$$q(A_0, W) \leq q(A_0, [V, X]) \leq q(A, V)$$

(c) $A_0 \in \mathcal{Q}^*(A_0, [V, X])$.

Proof. We have $X \leq \langle A^X \rangle$, so $[V, X, C_A(X)] = 1$ since A acts quadratically on V. Put $U = [V, X]$, and let $U_1 \leq U_0$ be AX-invariant subspaces of U with $[U_0, X] \not\leq U_1$. Put $W = U_0/U_1$ and set $Y = C_X(W)$. Then $Y \leq \Phi(X)$ and so $[X, C_{A_0}(W)] \leq \Phi(X)$. Thus, we get $C_{A_0}(W) \leq A_0 \cap C_A(X)$, and so $C_{A_0}(W) = 1$.

Put $U^* = C_V(C_A(X))$ and put $q = q(A, V)$. Suppose next that $|A_0|^q < |U^*/C_{U^*}(A_0)|$. Since $C_{U^*}(A_0) = C_V(A)$ we then have:

$$|V| = |A|^q |C_V(A)| < |C_A(X)|^q |U^*|$$

and thus $q(C_A(X), V) < q(A, V)$. But this is contrary to $A \in \mathcal{Q}_*(S, V)$, so we now conclude that $|A_0|^q \geq |U^*/C_{U^*}(A_0)|$. Then also $|A_0|^q \geq |U/C_U(A_0)|$, and so $q(A_0, U) \leq q(A, V)$.

Next, put $r = q(A_0, U)$. We have:

$$|A_0|^r = |U/C_U(A_0)| \geq |U_0/C_{U_0}(A_0)|$$

and also:

$$|C_W(A_0)| \geq |C_{U_0}(A_0)U_1/U_1| = |C_{U_0}(A_0)/C_{U_1}(A_0)|$$

and thus:

$$|A_0|^r |C_W(A_0)| \geq |U_0/C_{U_1}(A_0)| \geq |W|.$$

This shows that $q(A_0, W) \leq r$, and completes the proof of (b).

Next, let $B \leq A_0$ and put $A_1 = C_A(X)B$. Since $A \in \mathcal{Q}_*(S, V)$ we have $q \leq q(A_1, V)$, and so:

$$|A_0/B|^q = |A/A_1|^q \geq |C_V(A_1)/C_V(A)| \geq |C_U(A_1)/C_U(A)|$$

which shows that $|A_0|^q |C_U(A_0)| \geq |B|^q |C_U(B)|$. This proves (c). □

Section 4: Solvable Groups

In this section we assume Hypothesis 1. Recall that for any subgroup X of G, $\mathcal{Q}(X, V)$ is the set of quadratic subgroups of X, and that if $\mathcal{Q}(X, V)$ is non-empty then $q(S, V)$ is the minimum, over all $A \in \mathcal{Q}(X, V)$, of the numbers q for which $|A|^q = |V/C_V(A)|$. Denote by $\mathcal{Q}^*(X, V)$ the set of all $A \in \mathcal{Q}(X, V)$ such that $|A|^{q(X,V)} = |V/C_V(A)|$.

4.1 Lemma. *Assume Hypothesis 1, with p odd. Let a be an element of order p in G, such that a acts quadratically on V, and let R be an a-invariant p'-subgroup of G. If $p = 3$ assume also that R is abelian or that $|R|$ is odd. Then $[R, a] = 1$.*

Proof. This is [C2, Lemma 1.2].

4.2 Lemma. *Let S be a 2-group, and let a be an automorphism of S of order 3. Assume that $S = [S, a]$, and that the following condition holds.*

(*) *Every a-invariant abelian subgroup of S is centralized by a.*

Then $\Phi(S) = [S, S] = Z(S) = \Omega_1(S) = C_S(a)$.

Proof. It will be convenient to form the semi-direct product $G = S\langle a\rangle$. Let $\mathcal{R}$ denote the set of all proper subgroups R of S such that $R = [R, a]$. We assume that S provides a minimal counter-example to the lemma. So:

(1) For any $R \in \mathcal{R}$ we have $\Phi(R) = [R, R] = Z(R) = \Omega_1(R) = C_R(a)$.

Put $X = \langle C_S(a)^G\rangle$. Then $X \subseteq \Phi(S)$ since $S = [S, a]$. Here $\Phi(S) = \langle s^2 : s \in S\rangle$ since S is a 2-group. Suppose that $X \neq \Phi(S)$ and let $g \in S$ with $g^2 \notin X$. Put $T = \langle g, g^a\rangle\Phi(S)$, and put $R = [T, a]$. Then $T = RX$. Now $R/(R \cap X) \cong T/X$, and so $R/(R \cap X)$ is not elementary abelian. If now $T \neq S$, then $R \in \mathcal{R}$ and (1) then implies that $R/C_R(a)$ is elementary abelian, for a contradiction. We have thus shown:

(2) Either $X = \Phi(S)$ or $|S/\Phi(S)| = 4$.

Notice that $Z(S) \subseteq X$,by (*). Now let Y be a normal 2-subgroup of G properly containing $Z(S)$, and with Y minimal for this property. Moreover, if possible, choose $Y \subseteq X$. If $[Y, a] = 1$ then $[Y, S] \subseteq [Y, \langle a^S\rangle] = 1$, contrary to the choice of Y. Thus $|Y : Z(S)| = 4$. Setting $H = [Y, a]$, it then follows from (*) that H is a quaternion group, of order 8. Notice that H is invariant under $C_S(a)$, and then $[H, C_S(a)] = 1$. But then $1 = [Z(S)H, C_S(a)] = [Y, C_S(a)]$, and so $[Y, X] = 1$. In particular, we have $[H, X] = 1$, and so $H \nsubseteq X$. By our choice of Y, it then follows that $[X, a] = 1$, whence $[X, \langle a^S\rangle] = 1$. Thus:

(3) We have $X = C_S(a) = Z(S)$.

Suppose next that $X = \Phi(S)$. In particular, (3) then says that the nilpotence class of S is 2. Let $\mathcal{Q}$ denote the set of all subgroups Q of S such that $Q = [Q, a]$ is a quaternion group, and put $Z = \langle [Q, Q] : Q \in \mathcal{Q}\rangle$. Then $Z \subseteq \Omega_1(Z(S))$. Let t be an arbitrary element of S and put $D = \langle t, t^a, t^{a^2}\rangle$ and $R = [D, a]$. Then either $R \in \mathcal{Q}$ or $R = 1$, and in either case we have $D = C_D(a)R = (D \cap X)R$. Write $t = xr$ with $r \in R$ and $x \in X$. Then $t^2 = x^2r^2 \in \Phi(X)Z$. But then $X = \Phi(S) = \Phi(X)Z$, and so $X = Z$. In particular, we now have $\Phi(S) = \Omega_1(Z(S)) = [S, S]$. Moreover, if t is an involution then $1 = x^2r^2 = r^2$, and so $r \in Z(R) \subseteq X$, and $t \in X$. This shows that $\Omega_1(S) = X$, and thus the proposition is proved in the case that $X = \Phi(S)$. In view of (2) we then have:

(4) $|S/\Phi(S)| = 4$, and X is a proper subgroup of $\Phi(S)$.

Here $\Phi(S) = [\Phi(S), a]X$, so it follows from (1) that $\Phi(S)/X$ is elementary abelian. Suppose that $|\Phi(S)/X| > 4$. We may then choose a normal subgroup M of G with $X \subseteq M \subset \Phi(S)$, and with $|\Phi(S)/M| = 16$. Put $V = \Phi(S)/M$. Then $G/\Phi(S)$ operates faithfully on V, as otherwise $|S/\Phi(S)| > 4$. Here $G/\Phi(S) \cong Alt(4)$, and a is fixed-point-free on V. One may then verify that for every g in $S - \Phi(S)$ we have $C_V(g) = [V, g] = C_V(S) = [V, S]$, a subgroup of V of order 4. But then g^2 lies in $[S, \Phi(S)]$ for all $g \in S$, whereas $\Phi(S) = \langle g^2 : g \in S \rangle$. Thus we have a contradiction, proving that $|\Phi(S)/X| = 4$. This immediately implies:

(5) $S/X \cong \mathbb{Z}_4 \times \mathbb{Z}_4$.

Recall from the proof of (3) that we have a quaternion group $H = [H, a]$ with $H \not\leq X$. It now follows from (5) that $\Phi(S) = HX$. Suppose that $\Omega_1(X) \neq Z(H)$, and let Z be a subgroup of X of order 2 with $Z \neq Z(H)$. Then observe that S/Z satisfies the condition (*), in place of S. (Indeed, if $g \in S - C_S(a)$ then $\langle a, a^g \rangle = H\langle a \rangle$ or G.) By minimality of the counter-example, we then have $[\Phi(S/Z), a] = 1$, which is contrary to (5). Thus, we conclude that $\Omega_1(X) = Z(H)$, and hence X is cyclic. Then H is the unique quaternion subgroup of HX, and so H is a normal subgroup of G. Then $S = C_S(H)H$, a central product. This violates $|S/\Phi(S)| = 4$, and the proposition is thereby proved. □

4.3 Lemma. *Assume Hypothesis 1 with $G = QA$, Q a normal p'- subgroup of G, and with $|A| = p$. Assume further that $Q = [Q, A]$, $V = [V, Q]$, and $|V : C_V(A)| \leq p^2$. Finally, assume that A acts quadratically on V. Then one of the following holds.*

(i) *$G \cong SL(2, 2)$ and V is either a natural $SL(2, 2)$-module or a direct sum of two natural $SL(2, 2)$-modules for G.*

(ii) *$G \cong (3 \times 3) : 2$, $|V| = 16$, and V is the direct sum of two G-invariant subspaces of dimension 2.*

(iii) *$G \cong (SU(3, 2))'$, and V is a natural $SU(3, 2)$-module for G, of order 64.*

(iv) *$G \cong Dih(10)$ and $|V| = 16$.*

(v) *$G \cong SL(2, 3)$, V is either a natural $SL(2, 3)$-module or a direct sum of two natural $SL(2, 3)$-modules for G.*

(vi) *$G \cong (Q_8 \times Q_8) : 3$, $|V| = 81$, and V is the direct sum of two G-invariant subspaces of dimension 2.*

Proof. Let (G, V) be a counter-example with $|G| + |V|$ as small as possible. Write $A = \langle a \rangle$.

Suppose first that p is odd. As Q is generated by its A-invariant Sylow subgroups, 4.1 implies that $p = 3$ and that $C_Q(A)$ has index a power of 2 in Q. Let T be an A-invariant Sylow 2-subgroup of Q, and put $X = [T, A]$. Then $G = C_G(A)X$ and we have $\langle Z(X)^G \rangle = \langle Z(X)^{C_G(A)} \rangle \leq C_G(A)$, and so $\langle Z(X)^G \rangle$ centralizes $\langle A^G \rangle = G$. That is, we have $Z(X) \leq Z(G)$.

Suppose now that $X \neq Q$. The minimality of $|G| + |V|$ then implies that outcome (v) or (vi) of the lemma holds, with $(XA, [V, X])$ in place of (G, V). Then $[V, X] = [V, Z(X)]$ and $C_V(X) = C_V(Z(X))$. Thus $[V, X]$ and $C_V(X)$ are G-invariant. As $Q = [Q, A] = \langle X^Q \rangle$, we conclude that $[C_V(X), Q] = 0$, so $C_V(X) = 0$, and $|V| = 9$ or 81. Observe that in $SL(4, 3)$ the centralizer of any element of order 3 is a $\{2, 3\}$-group. Thus $C_Q(A) \leq T$, and thus $Q = T = X$. Thus, we have shown that $Q = X$ after all.

Now 4.2 yields $\Phi(Q) = [Q, Q] = Z(Q) = \Omega_1(Q) = C_Q(A)$. Suppose that $|Z(Q)| = 2$. Then Q is a quaternion group of order 8 and G is generated by two conjugates of A. As $|V/C_V(A)| \leq 9$ we then have $|V| \leq 81$, and then 2.3 implies that V is a direct sum of two natural $SL(2,3)$-modules for G. That is, (v) holds, and (G,V) is not a counter-example. We therefore conclude that $|Z(Q)|>2$. Let $\langle s,t\rangle$ be a fours group in $Z(Q)$, with the generators s and t chosen so that both $C_V(s)$ and $C_V(t)$ are non-trivial. As $G=\langle A^G\rangle$, A acts non-trivially on both $[V,s]$ and on $C_V(s)$, and so A induces a transvection on each of these subspaces. By induction, both $[V,s]$ and $C_V(s)$ are of order 9, and then $C_V(s)=[V,t]$, and $V=[V,s]+[V,t]$. Set $Q_1=C_Q([V,s])$ and $Q_2=C_Q([V,t])$. Then $Q_1\cap Q_2=1$, and Q/Q_i is a quaternion group for $i=1,2$. As $\Phi(Q)$ is non-cyclic, the 2-rank m of $Q/\Phi(Q)$ is greater than 2, and since $Q=[Q,A]$ we have $m=4$. It follows that each Q_i is a quaternion group, and $Q=Q_1\times Q_2$. Thus, (vi) holds, and so the lemma holds if p is odd.

We now take $p=2$. Let $\mathcal{R}$ be the set of all proper subgroups R of Q with $R=[R,A]$ and with $|R|>3$. For any $R\in\mathcal{R}$, the pair $(RA,[V,R])$ is then given by one of the outcomes (ii) through (iv) in the statement of the lemma. We note also the following consequence of our hypothesis that $V=[V,Q]$.

(1) No proper Q-invariant subspace of V contains $[V,A]$.

From this it follows that:

(2) If $R\in\mathcal{R}$ and R is a normal subgroup of Q, then $V=[V,R]$.

Let $1\neq x\in Q$ with $x^a=x^{-1}$. Then $|V/C_V(x)|\leq 16$, and then $\langle a,x\rangle$ is dihedral of order 6 or 10. Suppose $|x|=5$, and then suppose that there exists $y\in Q-\langle x\rangle$ with $y^a=y^{-1}$. Examining outcomes (i) through (iv) of the Lemma, we see that $\langle x,y\rangle\notin\mathcal{R}$, and hence $\langle x,y\rangle=Q$. Here $[V,A]\leq[V,x]$, so $|V|\leq|[V,x]+[V,y]|\leq 2^6$, and G may be identified with a subgroup of $L_6(2)$. One may readily verify that no subgroup of $L_6(2)$ of odd order admits faithful action by a dihedral group of order 10. Therefore x lies in $Z(Q)$, and then (2) yields that $V=[V,x]$ is of order 16. Then Q is cyclic, and since $SL(4,2)$ contains no dihedral group of order 30 it follows that G is dihedral of order 10. Thus, no element y exists as chosen above, and so (iv) holds in this case.

We now conclude that $x^3=1$ for all x in Q with $x^a=x^{-1}$. Then $Q=C_Q(A)T$ where T is an A-invariant Sylow 3-subgroup of Q. Then $[Q,A]\leq T$, so since $Q=[Q,A]$ by hypothesis we obtain $[Q,A]=T$, and Q is a 3-group. Put $\overline{Q}=Q/\Phi(Q)$, and suppose first that $|\overline{Q}|>9$. Then any maximal subgroup of $\overline{Q}$ is the image of some element of $\mathcal{R}$, and so $|\overline{Q}|=27$. Notice that for any $R\in\mathcal{R}$ we have $C_R(A)=\Phi(R)$ and $R/C_R(A)=9$. It follows $R\cap\Phi(Q)\leq C_R(a)$, and then $[\Phi(Q),A]=1$ and $\Phi(Q)\leq Z(G)$. Suppose that there exists $R\in\mathcal{R}$ with R non-abelian. Then $(RA,[V,R])$ is described by outcome (iii) of the lemma, so $[V,R]=[V,Z(R)]$, and thus $[V,R]$ is G-invariant. Then $V=[V,R]$, by (2). Then $|V|=64$,, and since $R\neq Q$, Q is isomorphic to a Sylow 3-subgroup of $L_6(2)$, of order 3^4. Then Q is a wreath product, contrary to $|\overline{Q}|=9$. We conclude that every $R\in\mathcal{R}$ is abelian. As $|\overline{Q}|=27$ it follows that Q has a generating set consisting of elements which commute pair-wise, and so Q is abelian. But with $|V/C_V(A)|\leq 4$ we then have $|Q|=9$.

We conclude that $|\overline{Q}\leq 9$. If $|\overline{Q}|=3$ then Q is cyclic, and (i) holds, so in fact $|\overline{Q}|=9$.

Then three conjugates of a suffice to generate G, and so:

(3) $|V| \leq 64$.

Suppose next that $\Phi(Q) \leq Z(G)$. Then $\Phi(Q)$ is cyclic, of exponent at most 3, and so Q is either elementary abelian of order 9 or extraspecial of order 27. Suppose that Q is elementary abelian, and let $x \in Q^{\#}$ with $[V,x]$ as large as possible. As $x^a = x^{-1}$ we then have $|[V,x]| = 16$ and $[V,a] \leq [V,x]$. Here $[V,x]$ is G-invariant, so $[V,x] = V$ and (ii) holds. On the other hand, suppose that Q is extraspecial. No member of $\mathcal{R}$ is cyclic of order 9, so the exponent of Q is 3, and then G is isomorphic to the commutator subgroup of $SU(3,2)$. Then $|V| > 32$, and (3) then yields $|V| = 64$. There is, up to isomorphism, a unique faithful representation of Q of degree 3 over $\mathbb{F}_4$ (by ordinary character theory), and so we obtain (iii) in this case. We therefore conclude that $\Phi(Q) \not\leq Z(G)$.

Now $[\Phi(Q), a] \neq 1$, and we may choose $y \in \Phi(Q)$ with $y^a = y^{-1}$. Choose a generating set $\{x_1, x_2\}$ for Q with $(x_i)^a = (x_i)^{-1}$ for $i = 1$ and 2, and set $R_i = \langle x_i, y\rangle$. Then $R_i \in \mathcal{R}$ and $Q = \langle R_1, R_2\rangle$. Suppose $y \in Z(Q)$. Then each R_i is abelian, and so $|[V,R_i]| = 16$, and $[V,R_1] \neq [V,R_2]$. Then $[V,y] \neq [V,R_i]$ for some i, and so $|[V,y]| = 4$. But then $Q = C_Q([V,y]) \times \langle y\rangle$, contrary to $y \in \Phi(Q)$. Thus $y \notin Z(Q)$, and we may assume that R_1 is non-abelian. Then $R_1A \cong SU(3,2)'$ and $|[V,R_1]| = |[V,y]| = 64$. Then also R_2 is non-abelian, and (3) yields $[V,R_1] = [V,R_2] = V$. We conclude that Q is isomorphic to a Sylow 3-subgroup of $GL(V)$, of order 81. Then Q has an elementary abelian subgroup E of order 27, and every element of order 3 in Q is contained in $E \cup R_1$. Then $R_2 = (R_1 \cap R_2) \cup (E \cap R_2)$, and so $R_2 \leq E$. As R_2 is non-abelian, we have a contradiction at this point, proving the lemma. □

4.4 Proposition. *Assume Hypothesis 1, and assume that $G = QA$, where $Q = [Q,A]$ is a p'-subgroup of G and where A is a subgroup of G which satisfies the following conditions.*

(a) *A acts quadratically on V.*

(b) $|A|^2 \geq |V/C_V(A)|$.

(c) *For any non-identity subgroup B of A, we have $|A|^2|C_V(A)| \geq |B|^2|C_V(B)|$.*

Denote by $\mathcal{Y}$ the set of subgroups Y of Q for which there exists a hyperplane B of A such that $Y = [C_Q(B), A]$, and such that $Y \neq 1$. Then Q is the direct product $\prod\{[V,Y]\}_{Y\in\mathcal{Y}}$, and $[V,Q]$ is the direct sum $\bigoplus\{[V,Y]\}_{Y\in\mathcal{Y}}$. Further, for any $Y \in \mathcal{Y}$ and any $a \in A - C_A(Y)$, the pair $(Y\langle a\rangle, [V,Y])$ is given by one of the outcomes in 4.3, with $Y\langle a\rangle$ in place of G and $[V,Y]$ in place of V.

Proof. Put $Q_0 = C_Q(C_V(A))$. The quadratic action of A yields $[V,A,Q_0] = 0$, while also $[V,Q_0,A] \leq [V,A] \leq C_V(Q_0)$. The Three Subgoups Lemma then yields $[V,[Q_0,A]] \leq C_V(Q_0)$, and then $[Q_0,A] = 1$, by coprime action. Thus:

(1) $C_Q(C_V(A)) \leq C_Q(A)$.

Denote by $\mathcal{B}$ the set of hyperplanes B of A such that $[C_Q(B), A] \not\leq \Phi(Q)$. For any

$B \in \mathcal{B}$ put $Y_B = [C_Q(B), A]$ and set $V_B = C_V(B)$. Thus, $\mathcal{Y} = \{Y_B\}_{B \in \mathcal{B}}$. Fix $B \in \mathcal{B}$. Then Y_B acts non-trivially on V_B, by (1). Choose $a \in A - B$, and set $X = Y_B$, $U = V_B$, $L = X\langle a \rangle$, and $\overline{L} = L/C_L(U)$. Condition (c) implies that $|U : C_U(a)| \leq p^2$, so 4.3 applies and identifies a list of possibilities for the pair $(\overline{L}, [U, X])$. Further, as $[V, B]$ is X-invariant and centralizes a, we obtain $[V, B, X] = 0$. Then $[V, X, B] = 0$, and thus $V = C_V(X) + U$. In particular, L acts faithfully on U. We have shown:

(2) For any $B \in \mathcal{B}$ we have $V = C_V(Y_B) + C_V(B)$, and for any $a \in A - B$ the pair $(Y_B\langle a \rangle, [V, Y_B])$ satisfies the hypothesis (and conclusion) of 4.3.

We may also record the following result.

(3) For any $B \in \mathcal{B}$ we have $[V, Y_B, B] = 0$.

Now let X and Y be distinct elements of $\mathcal{Y}$, and put $D = C_A(X) \cap C_A(Y)$. Then $|A : D| = p^2$, and there exist elements $a, b \in A$ such that $A = D\langle a, b \rangle$,and with $C_A(X) = D\langle b \rangle$ and $C_A(Y) = D\langle a \rangle$. Then also $X = [X, a]$ and $Y = [Y, b]$. Set $W = C_V(D)$ and set $E = \langle a, b \rangle$. We have $C_W(a) = C_W(D\langle a \rangle)$ admitting faithful action by $Y\langle b \rangle$, by (2), so $C_W(a)$ is contained properly in $C_W(E)$. Notice also that condition (c) yields $|W/C_W(E)| \leq p^4$. Thus:

(4) $|W/C_W(a)| \leq p^3$ and $|W/C_W(E)| \leq p^4$.

We aim now to show:

(5) $[X, Y] = 1$.

Suppose first that $|[W, Y]| = p^2$, so that $Y\langle b \rangle \cong SL(2, p)$. Let $x \in X$, and set $a' = a^x$ and $A' = D\langle a', b \rangle$. Then $A' = A^x$ acts quadratically on V, and so A' centralizes $[W, b]$. Put $W_0 = [W, Y] + [W, Y]^{a'}$. Thus $|W_0| \leq p^3$ and W_0 is invariant under $Y\langle a', b \rangle$. Here $p = 2$ or 3, and $Y\langle a', b \rangle$ acts as a subgroup K of $SL(3, p)$ on W_0, containing a copy of $SL(2, p)$, and with $K = O_{p'}(K)P$ where P is a p-group. However, it is easy to check that the only such subgroups K of $SL(3, p)$ are in fact isomorphic to $SL(2, p)$. (In $L_3(2)$ we are looking for the normalizer of a non-identity 3-group, and in $L_3(3)$ for the normalizer of a non-identity 2-group.) Thus $Y\langle a', b \rangle$ induces an action of $SL(2, p)$ on W_0, and so $W_0 = [W, Y]$, and $[W, Y]$ is a^x-invariant. As $X \leq \langle a^X \rangle$ we conclude that Y is X-invariant, and then $[X, Y] = 1$ since $[X, b] = 1$. Thus (5) holds in this case.

We may now assume that neither $[W, X]$ nor $[W, Y]$ is of order p^2. If $|W/C_W(a)| = p^3$ then (4) implies that b induces a transvection on $C_W(a) = C_V(D\langle a \rangle$, and then (2) implies that $|[W, Y]| = p^2$; which is a contradiction. We therefore conclude that $|W : C_W(a)| = p^2$. Further, as $|[W, X]| > p^2$, (2) shows that $[W, a] \leq [W, X]$. We now set

$R = [C_Q(D), a]$. Then $X \leq R$, and so 4.3 applies to the pair $(R\langle a\rangle, [W, R])$.

We have $X \leq R \trianglelefteq C_Q(D)E$, and $Y \leq \langle b^{C_Q(D)}\rangle$. If $[R, b] = 1$ it follows that $[R, Y] = 1$ and we have (5). So assume that $[R, b] \neq 1$. Then X is a proper subgroup of R, so 4.3 implies that R is of the form 3^2,3^{1+2}, or $Q_8 \times Q_8$, while $X \cong (SL(2, p))'$. Suppose $R \cong (SL(2, p)' \times (SL(2, p))'$. Then $[W, R] = [W, X]$, and then $[W, R, b] = 0$, by (3). Then $[W, R, Y] = 0$, so $[W, X, Y] = 0$. We have $[V, X] = [W, X]$, by (2), so $[V, X, Y] = 0$ in this case. On the other hand, suppose that $R\langle a\rangle \cong (SU(3, 2))'$ and $|[W, R]| = 64$. Then X is of order 3 and $|[W, X]| = 16$. As b centralizes $[W, X]$, by (3), and b leaves $C_W(X)$ invariant, it follows that $|[W, R]/C_{[W,R]}(b)| \leq 2$. But b either inverts $Z(R)$ (in which case $|[W, R]/C_{[W,R]}(b)| \geq 8$) or b centralizes $Z(R)$ (in which case $C_{[W,R]}(b)$ may be regarded as an $\mathbb{F}_4$-space). Thus b centralizes $Z(R)$ and $[W, R, b] = 0$. As above, we then obtain $[V, X, Y] = 0$, and thus $[V, X, Y] = 0$ in any case. Similarly, we have $[V, Y, X] = 0$, and so $[X, Y] = 1$ by the Three Subgroups Lemma. This proves (5).

Notice that $[W, b, X] \leq [W, b, \langle a^X\rangle] = 0$, and so also $[W, X, b] = 0$. Now (5) yields $[W, X, Y] = 0$, and so $[W, X] \cap [W, Y] = 0$. But $[W, X] = [V, X]$ by (2), so we may conclude that $X \cap Y = 1$. Thus, we have shown:

(6) For any distinct $X, Y \in \mathcal{Y}$ we have $\langle X, Y\rangle = X \times Y$ and $[V, X] \cap [V, Y] = 0$.

Now let $Y_1, \cdots, Y_r \in \mathcal{Y}$ and put $K = \langle Y_1, \cdots, Y_r\rangle$. Suppose that $K = Y_1 \times \cdots \times Y_r$ and that $[V, K] = [V, Y_1] \oplus \cdots \oplus [V, Y_r]$. Let $X \in \mathcal{Y}$ with $X \neq Y_i$ for any i. Then (6) implies that $[V, X] \leq C_V(K)$, and so $[V, X] \cap [V, K] = 0$. Then also $X \cap K = 1$. Induction on r then yields:

(7) $\langle \bigcup \mathcal{Y}\rangle = \prod \mathcal{Y}$ and $[V, \prod \mathcal{Y}] = \bigoplus \{[V, Y]\}_{Y \in \mathcal{Y}}$.

Put $Q_0 = \langle \bigcup \mathcal{Y}\rangle$. It now only remains to show that $Q = Q_0$. By coprime action, for each prime divisor r of $|Q|$ there is an A-invariant Sylow r-subgroup of Q, and then $Q = C_Q(A)Q_0$. Then Q_0 is a normal subgroup of Q, and since $Q = [Q, A]$ we obtain $Q = Q_0$, as required. □

4.5 Corollary. *Let the hypotheses be as in 4.4.*

(a) *Assume that there is no element $Y \in \mathcal{Y}$ with $|[V, Y]| = p^2$. Then for any $Y \in \mathcal{Y}$ there is a uniquely determined 2-transvection $a \in A$ with $Y = [Q, a]$, and we have $q(A, V) = 2$.*

(b) *Assume that $q(A, V) \leq 1$. Then $q(A, V) = 1$, and for any $Y \in \mathcal{Y}$ there is a uniquely determined transvection $a \in A$ with $Y = [Q, a]$. Moreover, we then have $Y\langle a\rangle \cong SL(2, p)$, and $[V, Y\langle a\rangle]$ is a natural module for $Y\langle a\rangle$.*

Proof. Suppose first that there exists no $Y \in \mathcal{Y}$ with $|[V, Y]| = p^2$. If $|A| = p$ then (a) holds by 4.3. So assume $|A| > p$. Let $\mathcal{Y} = \{Y_1, \cdots, Y_r\}$, and set $U_i = [V, Y_i]$. Then 4.4 yields $Q = Y_1 \times \cdots \times Y_r$ and $[V, Q] = U_1 \oplus \cdots \oplus U_r$. By construction, each Y_i centralizes a hyperplane B_i of A. Since $U_i = [U_i, Y_i] = [U_i, \langle A^{Y_i}]$, quadratic action implies that $[U_i, B_i] = 0$. By assumption, and by 4.3, we have $|U_i/C_{U_i}(A)| = p^2$ for all i. Then $|B_i|^2 \geq |V/C_V(B_i)|$ for any i, and so 4.4 applies with B_i in place of A. By induction, for any j with $j \neq i$ there is a 2-transvection $b \in B_i$ with $Y_j = [Q, b]$. In this way we obtain $[Q, A]A = Y_1\langle a_1\rangle \times \cdots \times Y_r\langle a_r\rangle$, where a_i is a 2-transvection on V, centralizing U_j for $i \neq j$. Evidently $\{a_1, \cdots, a_r\}$ is the set of all 2-transvections in A, and thus (a) holds.

Suppose next that $q(A, V) \leq 1$. If $|A| = p$ then (b) follows from 4.3, so assume $|A| > p$. As in the preceding paragraph, define Y_i, B_i, and U_i, $1 \leq i \leq r$. As $|U_i/C_{U_i}(A)| \geq p$ for all i, we have $|B_i| \geq |V/C_V(B_i)|$ for any i, and again 4.4 applies with B_i in place of A. As in the preceding paragraph, induction on $|A|$ yields (b). □

4.6 Proposition. *Assume Hypothesis 1, with $F^*(G) = F(G)$, and with $q(G, V) \leq 2$. Denote by $\mathcal{A}$ the set of elements of $\mathcal{Q}^*(G, V)$ of minimal order, and set $G_0 = \langle \mathcal{A}\rangle$ and $D = [F(G), G_0]$. If $p = 3$ and $q(G, V) = 2$ assume further that G_0/Q is of odd order. There is then a G-invariant set $\mathcal{K} = \{K_1, \cdots, K_r\}$ of subgroups of D, such that the following hold.*

(a) *$D = K_1 \times \cdots \times K_r$.*

(b) *$V = [V, K_1] \oplus \cdots \oplus [V, K_r] \oplus C_V(D)$.*

(c) *For any $K \in \mathcal{K}$, and for $U = [V, K]$, one of the following holds.*

  (i) *$p = 2$, $K \cong \mathbb{Z}_3$ and $|U| = 4$ or 16.*

  (ii) *$p = 2$, $K \cong 3^{1+2}_+$ and $|U| = 64$.*

  (iii) *$p = 2$, $K \cong \mathbb{Z}_5$ and $|U| = 16$.*

  (iv) *$p = 3$, $K \cong Q_8$ and $|U| = 9$ or 81.*

  (v) *$p = 3$, $K \cong Q_8 \circ Q_8$ and $|U| = 81$.*

(d) *Suppose that there exists $K \in \mathcal{K}$ such that $|[V, K]| > p^2$. Then $q(G, V) = 2$ and each $A \in \mathcal{A}$ is of order p*

(e) *Suppose that there exists $K \in \mathcal{K}$ such that K is not G_0-invariant. Then $p = 2$, $|[V, K] = 4$, $q(G, V) = 2$, and each $A \in \mathcal{A}$ is of order 2.*

(f) *Let $A \in \mathcal{A}$ such that A acts non-trivially on some $K \in \mathcal{K}$. Then every member of $\mathcal{K}$ is A-invariant.*

Proof. Set $Q = F(G)$ and $q = q(G, V)$. For any $A \in \mathcal{A}$, let $\mathcal{Y}_A$ be the set of subgroups Y of Q such that $1 \neq Y = [C_Q(B), A]$ for some hyperplane B of A. Let $\mathcal{K}_0$ be the set of subgroups K of Q such that, for some $A \in \mathcal{A}$ and some $Y \in \mathcal{Y}_A$, we have $K = [K, A] \leq Y$, with $K \cong (SL(2, p))'$ and with $|[V, K]| = p^2$. If $p = 2$, let $\mathcal{K}_1$ be the set of subgroups K of Q such that $K \in \mathcal{Y}_A$ for some $A \in \mathcal{A}$, and such that K is not in $\mathcal{K}_0$ and is not contained in a direct product of two elements of $\mathcal{K}_0$. If $p = 3$ let $\mathcal{Y}_1$ be the set of all subgroups Y of Q such that $Y \in \mathcal{Y}_A$ for some $A \in \mathcal{A}$, with $Y \cong Q_8$ and with $|[V, Y]| = 81$. For Y and Y' in $\mathcal{Y}_1$, write $Y\tilde{Y}'$ if $Z(Y) = Z(Y')$. We then take $\mathcal{K}_1$ be the set of subgroups K of Q of the form $\langle \mathcal{S}\rangle$, where $\mathcal{S}$ is an equivalence class for this relation. In any case, set $\mathcal{K} = \mathcal{K}_0 \cup \mathcal{K}_1$, and observe that $\mathcal{K}$ is G-invariant.

Let $A \in \mathcal{A}$, and suppose that there exists $Y \in \mathcal{Y}_A$ with $Y \notin \mathcal{K}_0$. Set $B = C_A(Y)$ and let $a \in A - B$. Then $|[V, Y]| \geq p^4$ and $[V, Y]/C_{[V,Y]}(a) \geq p^2$, by 4.4. Here $[V, Y, B] = 0$ by quadratic action, so $|V/C_V(A)| \geq p^2|V/C_V(B)|$. As $|A|^q = |V/C_V(A)|$, we then have $|B|^q \geq p^{2-q}|V/C_V(B)|$. As $q \leq 2$ the minimality of q and of A then yields $q = 2$ and $B = 1$. Thus (d) is proved.

Let K_1 and K_2 be distinct members of $\mathcal{K}$, and set $X = \langle K_1, K_2\rangle$, $U_i = [V, K_i]$, and $W = U_1 + U_2$. Suppose first that $K_i \in \mathcal{K}_0$ for both $i = 1$ and 2. If $p = 2$ then X is isomorphic to a 3- subgroup of $L_4(2)$, so $X = K_1 \times K_2$ and $W = U_1 \oplus U_2$. On the other hand, suppose that $p = 3$, so that each K_i is a quaternion group, with $|[V, K_i]| = 9$. A Sylow 2-subgroup of $GL(2, 3)$ contains a unique quaternion group, so $U_1 \neq U_2$. Suppose $U_1 \cap U_2 \neq 0$. Then each K_i has a subgroup of index 2 which lies in a fixed subgroup X_0 of $GL(W)$ with $X_0 \cong GL(2, 3)$. Then $Z(K_1) = Z(K_2)$ and since $U_i = [V, Z(K_i)]$ we arrive back at $U_1 = U_2$ in this case. Thus, $U_1 \cap U_2 = 0$, and X is contained in a subgroup X_1 of $GL(W)$ of the form $3^4 : (GL(2, 3) \times GL(2, 3)$. But then X is contained in a complement to $O_3(X_1)$ in X_1, and since $|U_i| = 9$ we then have $[K_1, K_2] = 1$ and $W = U_1 \oplus U_2$. In particular, we have thus shown that if $\mathcal{K} = \mathcal{K}_0$ then (a) and (b), and either (c)(i) or (c)(iv) (with $|U| = p^2$), hold.

Let $K \in \mathcal{K}_0$, and suppose that there exists $A \in \mathcal{A}$ such that K is not A-invariant. Let $a \in A - N_A(K)$ and set $L = KK^a$. As we have just seen, L is the direct product of K and K^a, and $|[V, L]| = p^4$. Set $A_0 = C_A(L)$. The quadratic action of A implies that L is A-invariant and that $A = \langle a\rangle \times A_0$. Then $|A|^q = |V/C_V(A)| \geq p^2|V/C_V(A_0)|$, as A_0 centralizes $[W, L]$. As $q \leq 2$ we then have $|A_0|^q \geq |V/C_V(A_0)|$. The minimality of q and of A then implies that $A_0 = 1$ and $q = 2$. Thus:

(1) If $\mathcal{K} \neq \mathcal{K}_0$, or if there exists $K \in \mathcal{K}_0$ which is not G_0-invariant, then $|A| = p$ for all $A \in \mathcal{A}$.

Thus, parts (a) through (e) of the lemma hold if $\mathcal{K} = \mathcal{K}_0$. Moreover, we may record the following result

(2) If K_1 and K_2 are in $\mathcal{K}_0$ then $[K_1, K_2] = 1$ and $U_1 \cap U_2 = 0$.

We assume henceforth that $\mathcal{K} \neq \mathcal{K}_0$. Suppose that $p = 2$, $|K_1| = 5$ and $|U_1| = 16$. If also $|K_2| = 5$ then, since any Sylow 5-subgroup of $L_8(2)$ is abelian, we have $X = K_1 \times K_2$. In this case we have also $U_1 \cap U_2 = 0$. On the other hand, suppose that K_2 is a 3-group. then $[K_1, K_2] = 1$ since Q is nilpotent. Suppose that $U_1 \cap U_2 \neq 0$. As $End_{K_1}(U_1) \cong \mathbb{Z}_{15}$ it follows that $U_1 \leq U_2$ and that $|K_2/C_{K_2}(U_1)| = 3$. Then U_2 is not a natural $SU(3, 2)$-module for K_2, with $K_2 \cong 3^{1+2}_+$. By 4.4 and the definition of $\mathcal{K}$, we then have $|K_2| = 3$ and $U_1 = U_2$. By (d), which has already been proved, there exist 2-transvections a_i with $K_i = [Q, a_i]$, ($i = 1$ and 2). But then $X\langle a_1, a_2\rangle \cong Dih(6) \times Dih(10)$, which is not a subgroup of $L_4(2)$. We therefore conclude that $U_1 \cap U_2 = 0$ in this case.

Suppose next that $p = 2$, and that both K_1 and K_2 are 3-groups in $\mathcal{K}_1$. By definition, we then have $K_i \in \mathcal{Y}_{A_i}$ for some $A_i \in \mathcal{A}$, and then (d) implies, as above, that $K_i = [Q, a_i]$ for some 2-transvection a_i. In particular, we have $K_i \trianglelefteq X$ for each i. Suppose that $|K_1| = |K_2| = 3$. Then $X = K_1 \times K_2$, and $X\langle a_1, a_2\rangle \cong Sym(3) \times Sym(3)$. Suppose $U_1 = U_2$, and set $a = a_1a_2$ and $A = \langle a\rangle$. Then a is a 2-transvection, so $A \in \mathcal{A}$, $X \in \mathcal{Y}_A$, and each K_i is contained in the direct product of two members of $\mathcal{K}_0$. This is contrary to the definition of $\mathcal{K}_1$, so we conclude that $U_1 \neq U_2$. Suppose $U_1 \cap U_2 \neq 0$. Then $|W| = 64$. Set $C_i = C_X(K_i\langle a_i\rangle)$. Then $|C_i| = 3$ and $[U_{3-i}, C_i] = U_{3-i}$ for both $i = 1$ and 2. As $X = K_iC_i$, it follows that $[W, C_i] = W$. But only one cyclic subgroup of X is without fixed points on W, so $C_1 = C_2$. As $[X, \langle a_1, a_2\rangle] = X$ we have a contradiction at this point, and so $U_1 \cap U_2 = 0$.

Suppose that $|K_1| = 3$ (with $K_1 \in \mathcal{K}_1$) and that $K_2 \cong 3^{1+2}_+$. Then $K_1 \trianglelefteq X$, so $[K_1, K_2] = 1$. If $K_1 \leq K_2$ then $[U_2, K_1] = U_2$ is of order 64, whereas $|U_1| = 16$, so in fact $K_1 \not\leq K_2$ and $X = K_1 \times K_2$. As K_2 acts irreducibly on U_2 we have $U_1 \cap U_2 = 0$. Now suppose that both K_1 and K_2 are isomorphic to 3^{1+2}_+. Then $K_i \trianglelefteq X$ and so $[K_1, K_2] \leq K_1 \cap K_2$. In particular, we have $Z(K_1)Z(K_2) \leq Z(X)$. Suppose $K_1 \cap K_2 \neq 1$. It follows that $Z(K_1) = Z(K_2)$, and since $U_i = [V, Z(K_i)]$ we get $U_1 = U_2$. Then X is isomorphic to a 3- subgroup of $L_6(2)$, which is to say that $X \cong 3 \wr 3$. There are then exactly two maximal subgroups of X which having exponent 3, and one of these two is elementary abelian. We therefore conclude that, in fact, $K_1 \cap K_2 = 1$, and $X = K_1 \times K_2$. Irreducible action of K_i on U_i then yields $U_1 \cap U_2 = 0$. We have shown:

(3) If $p = 2$ and both K_1 and K_2 lie in $\mathcal{K}_1$, or some K_i is of order 5, then $X = K_1 \times K_2$ and $W = U_1 \oplus U_2$.

Continue now to assume that $p = 2$, let $K_1 \in \mathcal{K}_0$ and let K_2 be a 3-group in $\mathcal{K}_1$. Let b be a 2-transvection such that $K_2 = [Q, b]$. Thus $K_2 \trianglelefteq X$. Suppose $|K_2| = 3$. Then $X = K_1 \times K_2$. If $U_1 \cap U_2 \neq 0$ then $U_1 \leq U_2$ and we obtain a contradiction via $X = [X, b] = K_2$. Thus, we are reduced to the case where $K_2 \cong 3^{1+2}_+$. Then $K_1 \not\leq K_2$, since $|[V, x]| \geq 16$ for any non-identity element x of K_2. By the definition of $\mathcal{K}_0$, and by (d), there exists a 2-transvection a with $K_1 = [K_1, a]$. By (3), either $K_2 = (K_2)^a$ or $U_2 \cap (U_2)^a = 0$. As a is a 2-transvection, we conclude that $K_2 = (K_2)^a$, and then that $[Z(K_2), a] = 0$. As $K_1 \leq [Q, a]$, we have $[Q, a] \not\cong 3^{1+2}$, and so $|[Q, a]| \leq 9$ by 4.3. It now follows that $[K_2, a] = 1$, and then also $[K_2, K_1] = 1$. Thus $X = K_1 \times K_2$, and we again obtain $U_1 \cap U_2 = 0$ from the irreducible action of K_2 on U_2. Thus, (a), (b) and (c) hold if $p = 2$.

Now let $p = 3$, and let $K \in \mathcal{K}_1$. By definition, and by 4.5, there then exists $Y \in \mathcal{Y}_1$ such that $K = \langle \mathcal{S} \rangle$, where $\mathcal{S}$ is the set of all $Y' \in \mathcal{Y}_1$ with $Z(Y) = Z(Y')$. Suppose that $|\mathcal{S}| > 1$, let $Y' \in \mathcal{S} - \{Y\}$, and set $K_0 = YY'$. By (d), there is are 2-transvections a and a' such that $Y = [Q, a]$ and $Y = [Q, a']$, so Y and Y' are normal subgroups of K_0, and K_0 is $\langle a, a'\rangle$-invariant. Suppose $\Phi(K_0) \not\leq Z(Y)$. Then $[Y, Y'] \not\leq Z(Y)$ and then $\Phi(K_0)$ contains both Y and As $\Phi(K_0)$ is a proper subgroup of K_0, we conclude that in fact $\Phi(K_0) = Z(Y)$. Then $K_0 = Z(K_0)X$ where X is an extraspecial group.

Set $L = K_0\langle a, a'\rangle$. Then $[C_V(Z(Y)), L] = 0$, and so L acts faithfully on the space $U = [V, Z(Y)]$. Suppose $Z(K_0) \neq Z(Y)$ We have $[Z(K_0), a] = 0$ by 4.1, and $End_{K_0\langle a\rangle}(U) \cong GL(2, 3)$, so $Z(K_0)$ is cyclic or is a fours group. If $Z(K_0)$ is cyclic then Y is the unique quaternion subgroup of K_0, contrary to $Y \neq Y'$. Thus $Z(K_0)$ is a fours group $\langle z, z'\rangle$ where $\langle z\rangle = Z(Y)$, and we have $K_0 = Y \times \langle z'\rangle$. The set $\mathcal{Q}$ of quaternion subgroups of K_0 then has cardinality 4, and it follows that $\langle a, a'\rangle$ induces the action of $Alt(4)$

on $\mathcal{Q}$. We now employ our hypothesis that, in the case $p = 3$ and $q = 2$, G_0/Q is of odd order. Thus $[L \cap Q, a]$ properly contains Y, which is contrary to $Y = [Q, a]$. This proves that $Z(K_0) = Z(Y)$, so K_0 is extraspecial of width 2. [We remark that, if the hypothesis concerning G_0/Q is dropped, then one has to face the possibility that $L \cong (Q_8 \times Q_8) : 3$, with Y and Y' equal to "diagonal" subgroups of $O_2(L)$, and with $C_Q(a)$ acting on $O_2(L)$ by interchanging the two direct factors. This appears to lead to some serious difficulties.] If $K_0 \cong 2^{1+4}_-$ then $L/C_L(K_0)K_0$ has cyclic Sylow 3-subgroups, so $\langle a \rangle$ and $\langle a' \rangle$ are congruent modulo $C_L(K_0)K_0$, contrary to $Y \neq Y'$. Thus $X \cong Q_8 \circ Q_8$. Then X has just two quaternion subgroups, and $[Y, Y'] = 1$.

We now conclude that $\mathcal{S}$ is a commuting set of quaternion groups acting on $[V, Z(Y)]$. Then $|\mathcal{S}| \leq 2$, and either $K = Y$ or $K \cong Q_8 \circ Q_8$. Returning now to the group $X = \langle K_1, K_2 \rangle$, suppose that both K_1 and K_2 lie in $\mathcal{K}_1$. Then each K_i is normal in X, and $|U_i| = 81$. In particular, we have $Z(K_1)Z(K_2) \leq Z(X)$. Here $Z(K_1) \neq Z(K_2)$, as K_1 and K_2 are defined by distinct equivalence classes on $\mathcal{Y}_1$. Then $Z(K_i) \not\leq Z(K_{3-i})$, and so $X = K_1 \times K_2$. If $U_1 = U_2$ then $Z(K_1)$ and $Z(K_2)$ induce identical actions on V, so in fact $U_1 \neq U_2$. Since there is a unique quaternion group in $End_{K_i}(U_i)$, it follows that $U_1 \cap U_2 = 0$.

Now suppose that $K_1 \in \mathcal{K}_0$ and that $K_2 \in \mathcal{K}_1$. Then $K_2 \trianglelefteq X$, and we have $[Q, a_1] = K_1$ or $[Q, a_1]$ is a direct product of two isomorphic copies of K_1. So, either $K_1 \trianglelefteq X$ or $\langle K_1^X \rangle \cong K_1 \times K_1$. Set $R = N_{K_2}(K_1)$. Then $|K_2 : R| \leq 2$, and $[K_1, R] \leq K_1 \cap K_2$. Set $R_0 = C_R(K_1)$, and suppose that R_0 has exponent 4. As $End_{K_1}(U_1) \cong \mathbb{Z}_2$, we obtain $[U_1, Z(K_2)] = 1$ in this case. So assume that R_0 has exponent 2. If $K_2 \cong Q_8$ then $K_1 \cap K_2 = 1$, as $Z(K_1) \neq Z(K_2)$, and so $R = R_0$ in this case. Here R has exponent 4, so we conclude that $K_2 \cong Q_8 \circ Q_8$, and that $R \neq R_0$. Then $K_1 \cap K_2 \neq 1$, and so $Z(K_1) \leq K_2$. Then $R = C_{K_2}(Z(K_1)) \cong D_8 \times \mathbb{Z}_2$. As $[R, a_1] \leq [Q, a_1]$, $R/C_R(U_1)$ acts as a group of inner automorphisms on K_1, and it follows that $[U_1, \Phi(R)] = 0$. Thus, $[U_1, Z(K_2)] = 0$ in any case, and so $[U_1, K_2] = 0$. Now $U_1 \cap U_2 = 0$, and since $[Z(K_2), K_1] = 1$ we then have $[U_2, K_1] = 0$. Then $X = K_1 \times K_2$, and we have thereby proved (a) through (d).

Suppose that we are given $K \in \mathcal{K}$ and $A \in \mathcal{A}$ such that K is not A-invariant. Set $U = [V, K]$ and let $a \in A - N_A(K)$. Then $U \cap U^a = 0$, by the foregoing. If $K \in \mathcal{K}_1$ then $A = \langle a \rangle$, a is a 2-transvection, and $|U| \geq p^4$. But then a is not a 2-transvection, so we conclude that $K \in \mathcal{K}_0$. If $p = 3$ we obtain $[V, K\langle a \rangle] = U \oplus U^a \oplus U^{a^2}$, contrary to quadratic action. Thus $p = 2$. Now (e) follows from (1).

Finally, by way of contradiction to (f), suppose that we are given $A \in \mathcal{A}$, and elements K_1 and K_2 of $\mathcal{K}$ such that $1 \neq [K_1, A] \leq K_1$ and such that K_2 is not A-invariant. Then $A = \langle a \rangle$ where a is a 2-transvection, by (d). But a already acts as a 2-transvection on $[V, K_2] \oplus [V, K_2]^a$, so $[V, K_1, a] = 0$, and so $[K_1, a]$ centralizes $[V, K_1]$. Then $[K_1, a]$ centralizes V, and we have the desired contradiction. □

4.7 Corollary. *Assume Hypothesis 1 with $G = QS$, $Q = O_r(G)$ for some prime q, $q \neq p$, and with S a Sylow p-subgroup of G. Assume that S acts irreducibly on $Q/\Phi(Q)$, and assume that there exists $A \in \mathcal{Q}(S, V)$ with $|A|^2 \geq |V/C_V(A)|$. Then there is a subgroup K of Q, unique up to conjugation, such that the following hold.*

(a) *$Q = K_1 \times \cdots \times K_r$, where $\{K_i\}_{1 \leq i \leq r} = K^S$.*
(b) *$V = [V, K_1] \oplus \cdots \oplus [V, K_r] \oplus C_V(Q)$.*
(c) *Setting $U = [V, K]$, one of the following holds.*
  (i) *$p = 2$, $K \cong \mathbb{Z}_3$ and $|U| = 4$ or 16.*
  (ii) *$p = 2$, $K \cong 3^{1+2}_+$ and $|U| = 64$.*
  (iii) *$p = 2$, $K \cong \mathbb{Z}_5$ and $|U| = 16$.*
  (iv) *$p = 3$, $K \cong Q_8$ and $|U| = 9$ or 81.*
  (v) *$p = 3$, $K \cong Q_8 \circ Q_8$ and $|U| = 81$.*

Moreover, if K is not invariant under $\langle \mathcal{Q}^*(S, V) \rangle$ then $p = 2$, $|K| = 3$, $|U| = 4$, and $q(S, V) = 2$.

Proof. Immediate from 4.6 and the irreducible action of S on $Q/\Phi(Q)$. □

The next result gives some information concerning the situation defined by Hypothesis $4'$.

4.8 Lemma. *Assume Hypothesis 2, with $|A|$ of order p. Assume further that $G = QA$, where $Q = [Q, A]$ is an r-group for some prime r, $r \neq p$. Finally, assume that $[V, A, A, A] = 0$ and that $[V, A, A] \neq 0$. Then $p = 3$ and one of the following holds.*

(i) *$G \cong Alt(4)$ and $|V| = 27$.*
(ii) *$G \cong SL(2, 3)$ and $|V| = 81$.*
(iii) *$Q \cong 2^{1+4}_+$ and $|V| = 81$.*
(iv) *G is a Frobenius group of order 39 and $|V| = 27$.*

Proof. Regard G as a subgroup of $SL(V)$. The minimal polynomial for a non-identity element a of A is then $(X-1)^3$, and the Hall-Higman Theorem ([HH, Theorem B], or [G, Theorem 11.1.1]) then yields $p = 3$. Also, as A is non-quadratic, we have $|V/C_V(A)| = 9$, and then since $V = [V, Q]$ it follows that V is irreducible for G. In particular, $Z(G)$ is cyclic. Moreover, it follows that $End_G(V) = \mathbb{F}_3$, and so $|Z(G)| \leq 2$.

Suppose first that Q is cyclic. Then $G = \langle A, A^g \rangle$ for some $g \in G$, and so $|V| \leq 3^4$. Here 3 divides $|Q| - 1$, while $|Q|$ divides $2^8 \cdot 3^6 \cdot 5 \cdot 13 = |SL(4, 3)|$. It follows that $|R| = 13$, and that (iv) holds.

We assume henceforth that Q is non-cyclic. There then exists a non-cyclic subgroup $Q_0 = [Q_0, A]$ of Q, with $Q_0 A$ generated by two conjugates of A, and so $|[V, Q_0]| \leq 3^4$ and $r = 2$.

Suppose that $|Q/\Phi(Q)| = 4$. Then we again have $G = \langle A, A^g \rangle$ for some $g \in G$, and $|V| \leq 3^4$. For any involution $t \in Q$ we then have $[V, t] = V$ or $|[V, t] = 9$, and since A is not quadratic on V it follows that $C_Q(A) \leq Z(SL(V))$. In particular, we have $|C_Q(A)| \leq 2$. Set $Y = [\Phi(Q), A]$, and set $W = [V, Y]$. If $Y = 1$ then (i) or (ii) holds, so assume that $Y \neq 1$. As A is non-quadratic we have $W \geq [V, A]$ and $V = W + C_V(A)$. Suppose that $YA \cong Alt(4)$. Then $|W| = 8$, and $\Phi(Q)$ is elementary abelian, of order at most 8. If $Y = \Phi(Q)$ then $W = V$, $|Q| = 16$, and $Y \leq Z(Q)$, whereas a Sylow 2-subgroup of $L_3(3)$ is semi-dihedral of order 16, with center of order 2. Thus $Y \neq \Phi(Q)$, and $|V| = 81$. There is a unique conjugacy class of elementary abelian subgroups of $SL(V)$ of order 8, and we then find that $N_{GL(V)}(\Phi(Q)) \cong 2^4 : Sym(4)$ and that Q is extraspecial of width two. This is contrary to $|Q/\Phi(Q)| = 4$, so we conclude that $YA \ncong Alt(4)$.

Suppose that $YA \cong SL(2,3)$. Then $Z(Y) = Z(SL(V))$, and $Y = \Phi(Q)$. But with Y normal in Q we have $Q = C_Q(Y)Y$, and this is contrary to $\Phi(Q) \geq Y$. Thus $YA \ncong SL(2,3)$. As A is non-quadratic on W, induction then implies that Y is extraspecial, of width 2. As $|C_Y(A)| \neq 1$ we have $Y = \Phi(Q)$. Let Q_1 and Q_2 be the two quaternion subgroups of Y. Then each Q_i is A-invariant, so each Q_i is normal in G, and we have $Q = C_Q(Q_i)Q_i = C_Q(Y)Y$. Again, this is contrary to $Y = \Phi(Q)$, so we conclude that $Q/\Phi(Q)| \geq 16$.

Suppose that $|Q/\Phi(Q)| \geq 64$ or that $Y \neq 1$. Then there are proper A-invariant subgroups R_1 and R_2 of Q, with $R_i = [R_i, A]$ of order bigger than 8, with $[R_1 \cap R_2, A] \neq 1$, and with $\langle R_1, R_2 \rangle = Q$. Here A acts non-quadratically on $[V, R_i]$ for each i, so by induction each R_i is extraspecial, of width 2. Set $W_i = [V, R_i]$ and set $X = [R_1 \cap R_2, A]$. Then XA is isomorphic to either $Alt(4)$ or $SL(2,3)$, and $|[V, X]|$ is either 27 or 81. As $[V, X] \leq W_1 \cap W_2$, where $|W_i| = 81$, we then have $|V| \leq 3^5$. Let T be a Sylow 2-subgroup of $SL(V)$ containing Q. As R_i acts irreducibly on W_i we have $C_T(R_i) \leq Z_i$, and thus $Z(T) = Z(R_1) = Z(R_2)$. Then also $[V, Z(T)] = W_1 = W_2$, and so $|V| = 81$. Set $D = C_R(A)$ and set $D_i = N_D(R_i)$. Then $|D_i/Z(R_i)| \leq 2$, and if $D_i \neq Z(R_i)$ then $D_i = Z(R_i)\langle d_i \rangle$ where d_i interchanges the two quaternion subgroups of R_i. In any case, we then have $R_i = J(R_iD_i \ mod \ Z(R_i))$, and so R_i is characteristic in R_iD_i. It follows that $[N_Q(R_i), A] \nleq R_i$, and so each R_i is normal in Q. As $Aut(R_i) \cong Sym(4) \wr 2$, we conclude that $[R_1, R_2] = Z(R_1) = Z(R_2)$, and so $Q = R_1R_2$ is extraspecial of width 3. The minimal degree of a faithful representation of Q over $\mathbb{F}_3$ is then 8, and so we have a contradiction at this point.

Suppose finally that $|Q/\Phi(Q)| = 16$ and that $Y = 1$. As $G = \langle A^G \rangle$ we then have $\Phi(Q) \leq Z(G)$. Then $|\Phi(Q)| = 2$, as follows from the first paragraph of the proof. Suppose that $\Phi(Q) \neq Z(Q)$, and set $F = [Z(Q), A]$. Then $FA \cong Alt(4)$ and $|[V, F]| = 27$. As $[V, F]$ is G-invariant we then have $|V| = 27$, and R is not faithfully represented on Q. We conclude that $Z(Q) = \Phi(Q)$, and hence Q is extraspecial of width 2. Let Q_1 and Q_2 be the two quaternion subgroups of Q. Then $Q_iA \cong SL(2,3)$ and $[V, Q_i] = [V, Z(Q)] = V$ is of order 81. Thus (iii) holds. □

Section 5: Quadratic modules for quasisimple groups

In this section we shall be concerned mostly with the situation where $F^*(G)$ is quasisimple, and in which V is a quadratic module for G. The first main step is to establish a criterion (5.4, below) for G to contain a quadratic fours group. The proof of 5.4 requires some preliminary results, all of which, perhaps, are well known, but which we include for the sake of completeness.

Lemma 5.1. *Let T be a 2-group, and let F be a subgroup of T with $F \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Suppose that $C_T(F) = F$. Then T is either dihedral or semi-dihedral.*

Proof. It will be enough to show that T has a cyclic subgroup X of index 2, as then we will have $|C_X(a)| = 2$ and $T = X\langle a\rangle$ for any $a \in F - X$. If $|T| \leq 8$ then T is dihedral and there is nothing to prove. So assume $|T| > 8$ and proceed by induction on $|T|$. Let R be a subgroup of T of index 2, containing F. Then R is dihedral or semi- dihedral, and we may write $R = T\langle t\rangle$ where $Y = \langle y\rangle$ is the unique maximal cyclic subgroup of R and where $t \in F$. Let $x \in T - R$. Then $T = R\langle x\rangle$ and $Y = Y^x$. Put $2^n = |Y|$ and let z be the unique involution in Y.

Suppose first that R is semi-dihedral. Then the coset $\langle y^2\rangle t$ is the set of non-central involutions of R, and forms a single conjugacy class in R, of order 2^{n-1}. Then $C_T(t)$ is not contained in R, and so we may take $[t, x] = 1$. But also $F = Z(R)\langle t\rangle$, and then $[F, x] = 1$, contrary to $C_T(F) = F$. Thus R is dihedral. Further, the same argument then shows that conjugation by x interchanges the two conjugacy classes of non-central involutions of R. In particular, it follows that $C_R(x)$ contains no non-cenral involutions, and so $x^2 \in Y$. If now $\langle x^2\rangle = Y$ then $\langle x\rangle$ is a cyclic subgroup of T of index 2. Setting $X = \langle x\rangle$ we then have $C_X(t) = C_X(F) = \langle z\rangle$ and then T is dihedral or semi-dihedral. Thus, we may assume:

(1) $\langle x^2\rangle \neq Y$.

Now assume that x has been chosen so that $|C_Y(x)|$ is as large as possible, and then (subject to this condition) so that $|x|$ is as small as possible. Let y_0 be a generator for $C_Y(x)$, and put $y_1 = x^2$. If $\langle y_0\rangle \neq \langle y_1\rangle$ then there exists $u \in C_Y(x)$ with $u^2 = y_1$. But in that case we have $(ux)^2 = u^2x^2 = (y_1)^2$, and the minimality of $|x|$ then gives $y_1 = 1$. This shows:

(2) Either $\langle x^2\rangle = C_Y(x)$ or $|x| = 2$.

Suppose $|x^2| \neq 2$, and then use (1) to again choose $u \in Y$ with $u^2 = x^2$. Then $[x, u]^2 = [x, u^2] = 1$, and so $[x, u] = z$. Then $(xu)^2 = x^{-2}u^{-2}[x, u] = u^{-4z}$. Minimality of $|x|$ then implies $u^4 = 1$ and $x^2 = z$. Thus, in any case we have the following result.

(3) $x^2 \in \langle z\rangle$.

Suppose that $C_Y(x) \neq \langle z\rangle$. Then $|x| = 2$ by (2) and (3). But it then also follows that x inverts no element of $Y - \langle z\rangle$, and so $\langle x, z\rangle = \Omega_1(Y\langle x\rangle)$. Then $[x, t] = z$ and $N_T(F) = N_R(F)\langle x\rangle$, whence $C_T(F)$ properly contains F. This is contrary to assumption, so:

(4) $C_Y(x) = \langle z\rangle$.

Now x inverts the subgroup of order 4 in Y, and then $|C_Y(xt)| > |C_Y(x)|$. Replacing x

by xt, we then contradict the minimality of $|C_Y(x)|$ in our choice of x. This contradiction proves the lemma. □

5.2 Corollary. *Let X be a group, t an involution in X, and suppose that $X = \langle t^X \rangle$. Assume that $Z^*(X) = 1$, and suppose that $C_X(t)$ contains no subgroup of the form $\langle t \rangle \times E$ with $|E| = 4$. Then a Sylow 2-subgroup of X is dihedral or semi-dihedral.*

Proof. Glauberman's Z^* Theorem implies that there is a fours group $F = \langle s, t \rangle$ in X, with $s \in t^X$. The hypothesis then yields $C_Y(F) = F$ for any Sylow 2-subgroup T of X containing F. Now apply the preceding lemma. □

5.3 Proposition. *Let X be a finite group acting faithfully on a vector space V over $\mathbb{F}_2$, and assume that $X = \langle t^X \rangle$ for some involution t in X. Assume further that $F^*(X)$ is quasisimple, that $O_2(X) = 1$, and that $|V/C_V(t)| \leq 4$. Then one of the following holds.*

(i) *There is a fours group E in X with $t \in E$ and with $[V, E, E] = 0$.*
(ii) *A Sylow 2-subgroup of X is dihedral or semi-dihedral.*

Proof. Suppose that t lies in no fours group in X which acts quadratically on V. There is then no involution s in $C_X(t) - \langle t \rangle$ with $[V, t, s] = 0$. As $|[V, t]| \leq 4$ it then follows that $C_X(t)$ contains no subgroup of the form $\langle t \rangle \times F$ with $|F| = 4$. Then 5.2 applies, and yields (ii). □

Remark. The known simple groups with dihedral or semi-dihedral Sylow 2-subgroups are the groups $L_2(q)$, q odd; $L_3(q)$, $q \equiv 3 \ (mod\ 4)$; $U_3(q)$, $q \equiv 1 \ (mod\ 4)$; $Alt(7)$; and M_{11}. Using this classification, we will obtain Proposition 5.5, below, on groups which contain a 2-transvection which lies in no quadratic fours group.

Proposition 5.4. *Let X, t, and V be as in 5.3, and assume that $C_V(X) \leq [V, X]$. Assume that there does not exist a fours group E in X, containing t,and such that $[V, E, E] = 0$. Then one of the following holds.*

(i) *$X \cong Alt(5)$ and V is the $O_4^-(2)$-module for X.*
(ii) *$X \cong Sym(5)$ and $[V, X]/C_V(X)$ is the natural $\Gamma L(2, 4)$-module for X.*

Proof. Set $X_0 = F^*(X)$, let S be a Sylow 2-subgroup of X containing t, and set $T = S \cap X_0$. Suppose first that $X_0/Z(X_0) \cong L_3(q)$, $q \equiv 3 \ (mod\ 4)$; or $U_3(q)$, $q \equiv 1 \ (mod\ 4)$. As S has 2-rank equal to 2, by 5.2, S contains no element which induces a field automorphism on X_0, and so $X_0 = X$. The involutions in X form a single conjugacy class, so there is a non-abelian subgroup R of X of order q^3 such that $R = [R, t]$. It then follows from 4.3 that $q = 3$, (so that $X \cong L_3(3)$), and that $|[V, R]| = 64$. Then $R\langle t \rangle$ is generated by three conjugates of t, and then X is generated by four conjugates of t. It follows that X is isomorphic to a subgroup of $L_8(2)$, whereas 13 does not divide $|L_8(2)|$. Thus, we have a contradiction via Lagrange's Theorem.

Suppose next that $Z(X_0) \neq 1$. As $O_2(X) = 1$ we then have $X_0 \cong 3^{\cdot}Alt(6)$ or $3^{\cdot}Alt(7)$. Set $V_0 = [V, Z(X_0)]$. Then $V = V_0 \oplus C_V(Z(X)0)$, and then, by induction, it suffices to show that every fours group in X containing t acts quadratically on V_0. Here, V_0 may be regarded as an $\mathbb{F}_4 X_0$-module. As $3^{\cdot}Alt(6)$ is not a subgroup of $SL(2, 4)$, we have

$dim_{\mathbb{F}_4}(V_0) > 2$, and it follows that $[Z(X_0), t] = 1$. Then $[V_0, t]$ is an $\mathbb{F}_4$- subspace of V_0 of dimension 1, and so $[V_0, t, F] = 0$ for any fours group F containing t, as required. Thus, we may assume henceforth that $Z(X_0) = 1$.

Suppose next that $X_0 \cong L_2(q)$, q odd, and suppose that $X_0 \neq X$. As before, no element of S induces a field automorphism on X_0. Suppose that $q \equiv 3$ $(mod\ 4)$, A Sylow 2-subgroup of X is dihedral, so all involutions in $X - X_0$ are conjugate, and thus t lies in a dihedral subgroup D of X of order $2q$. Then 4.3 implies that $q \leq 5$, so $q = 3$, which is contrary to our hypothesis that $q \geq 5$. Thus $q \equiv 1$ $(mod\ 4)$.

Let λ be a generator of the Sylow 2-subgroup of $\mathbb{F}_q^\times$. As in the preceding paragraph, all involutions in $X - X_0$ are conjugate, and so t may be identified with the involution ds, where d and s are represented in $GL(2, q)$ by the matrices

$$\widetilde{d} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \widetilde{s} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

respectively. Set $Y = \langle s, t \rangle$, and let z be the central involution in Y. Then Y is dihedral, of order $2(q-1)$, and since $\langle t, z \rangle$ is not quadratic it follows that Y acts faithfully on $[V, t] + [V, t]^s$. Any dihedral subgroup of $L_4(2)$ whose order is divisible by 4 has order dividing 12 or 8, so $q - 1$ divides 6 or 4. The given congruence satisfied by q then yields $q = 5$, and thus $X \cong Sym(5)$.

Set $F = \langle z, t \rangle$, and set $U = [V, F]$. As zt is conjugate to t we have $|U| \leq 16$, and since F is not quadratic we conclude that $|U| = 8$ and $U \neq [V, z]$. Thus $|V/C_V(z)| \leq 4$. As z inverts an element of order 5 in X_0, X_0 has no irreducible $\mathbb{F}_2$-modules on which z induces a transvection, and we conclude that X_0 has a unique non-trivial irreducible constituent W in V. Suppose that W is an $O_4^-(2)$- module for X_0. Then 1.3 that $W = V$, and one then observes that F acts quadratically on V. Thus, W is a natural $SL(2, 4)$-module for X_0, and outcome (ii) holds in this case.

Suppose next that $X = X_0$ and $X \cong L_2(q)$. Then three conjugates of t generate X, and so $|V/C_V(X)| \leq 64$. Then $q \leq 9$, by Lagrange's Theorem applied to $L_6(2)$. Suppose that $q = 9$, so that $X \cong Alt(6)$. Let $t \in X_1 \leq X$ with $X_1 \cong Alt(5)$. By induction, and by 1.3, we then have $V = [V, X_1] \oplus C_V(X_1)$, where $[V, X_1]$ is a natural $Sym(5)$-module for X_1. There exists a subgroup X_2 of X, with $X_1 \cong X_2$, and with X_1 not conjugate to X_2, and such that $X_1 \cap X_2$ is dihedral of order 10. Let f be an element of order 5 in $X_1 \cap X_2$. Then $[V, X_1] = [V, f] = [V, X_2]$. As $X_1X_2 = X$ we then have $|[V, X]| = 16$. Further, the elements of order 3 in X_1 and in X_2 come from different conjugacy classes in X. As $[V, X]$ is a natural $Sym(5)$-module for each X_i it follows that no element of order 3 in X is fixed-point-free on $[V, X]$. This result is inconsistent with a faithful action of $\mathbb{Z}_3 \times \mathbb{Z}_3$ on 2^4, and we therefore conclude that $q \neq 9$.

Suppose that $q = 7$, so that $X \cong L_3(2)$. There are three isomorphism classes of non-trivial irreducible $\mathbb{F}_2$-modules for X, of which one, the adjoint module for $L_3(2)$, admits no 2-transvections, and of which the other two are a dual pair of natural $L_3(2)$- modules. Suppose that there is a unique non-trivial constituent for X in V. Then 1.5 implies that $|V| \leq 16$, and either $V/C_V(X)$ or $[V, X]$ is a natural $L_3(2)$-module. One then observes that there is a maximal subgroup P of X containing S such that $|[W, O^2(P)]| = 4$, and then $O_2(P)$ is a quadratic fours group. Thus, we have a contradiction in this case, and since $|V/C_V(X)| \leq 64$ it follows that V has a submodule U such that both $U/C_U(X)$ and V/U are irreducible X-modules of order 8. Since t induces a transvection on U, and since three conjugates of t suffice to generate X, we have $|[U, X]| = 8$. Similarly, we have $|[V, X]/[U, X]| = 8$, and since $C_V(X) \cap [V, X] = 0$ we conclude that $C_V(X) = 0$. Let s be a conjugate of t such that $[s, t] = 1$, and set $F = \langle s, t\rangle$. As F is not quadratic we have $|[V, F]| = 8$, and it follows that U and V/U are not isomorphic as X-modules. We may assume that F has been chosen so that $|[U, F]| = 4$, and we then have $[V, F] = [V, t] + [U, F] \leq C_V(t)$. That is, we have $[V, F, t] = 0$, and so F is quadratic, after all.

Suppose that $q = 5$, so that $X \cong SL(2, 4)$. No involution in X induces a transvection on any irreducible $\mathbb{F}_2X$-module, so there is a unique non-trivial irreducible constituent U for X in V. If U is an $O_4^-(2)$-module for X, then 1.3 yields (i). So assume that U is a natural $SL(2, 4)$-module. Set $\overline{V} = V/C_V(X)$ and identify U with $[\overline{V}, X]$. We then have $|\overline{V}/C_{\overline{V}}(t)| = 4$, and $[\overline{V}, t] = C_{[\overline{V},X]}(t) = C_{[\overline{V},X]}(S)$. Set $V_0 = [V, X]$. Then the inverse image in V_0 of $C_{[\overline{V},X]}(S)$ is $C_{V_0}(S)$, and so S acts quadratically on V.

We are now reduced to the cases where $F^*(X)$ is isomorphic to $Alt(7)$ or M_{11}. A Sylow 2-subgroup of $Sym(7)$ has 2-rank equal to 3, while M_{11} has no outer automorphisms, so we have $X \cong Alt(7)$, or M_{11}. Then X has a subgroup X_0 with $F^*(X_0)/ \cong Alt(6)$, and with $S \leq X_0$. But it follows from what we have already shown that such an X_0 contains a quadratic fours group on V. This completes the proof of 5.4. □

5.5 Lemma. *Assume Hypothesis 3, with H quasisimple. Let A be a quadratic subgroup of H, with $|A|^2 \geq |V/C_V(A)|$. Then one of the following holds.*

(i) *$H/Z(H)$ is a group of Lie type in characteristic p.*
(ii) *We have $p = 2$, and H is an alternating group $Alt(2^n + 1)$, $n \geq 2$.*
(iii) *We have $|A| = p = 3$, $H \cong SL(2, 5)$, and V is a natural $SL(2, 9)$-module for H.*

Proof. If p is odd then Corollary 1.4 in [C3] yields (iii). So assume that $p = 2$. By 3.6 we either have (i) or G contains a fours group E, acting quadratically on V. Thus, we may assume the existence of such a quadratic fours group. If $H/Z(H)$ is a sporadic group then the main result of [A4] shows that S is not contained in a unique maximal subgroup of G, and so Hypothesis 3 is violated in this case. Assume that $H/Z(H)$ is of Lie type in odd characteristic (and that there is no isomorphism of $H/Z(H)$ with a group of Lie type in characteristic 2). The main result of [MS1] then implies that $H/Z(H) \cong U_4(3)$. The 2-local subgroups of H containing $S \cap H$ then form a diagram geometry of type $\widetilde{B}_2$ (for which see [RS], for example) and it follows that S is not contained in a unique maximal subgroup of G. Thus, we are reduced to the case where $H/Z(H)$ is an alternating group $Alt(n)$, $n \geq 7$. As S is contained in a unique maximal subgroup of G, the main theorem of [LPR] implies that $n = 2^m + 1$ for some m, $m \geq 3$, □

5.6 Proposition. *Let G be a symmetric group $Sym(n)$, $n \geq 2$, and let V be faithful $\mathbb{F}_2$-module for G, such that V is isomorphic to a constituent of the natural permutation module for G. Let A be a non-identity, elementary abelian 2-subgroup of G such that*

$|A| \geq |V/C_V(A)|$. *Then one of the following holds.*

- (i) *A is generated by a set of transpositions, and $|A| = |V/C_V(A)|$.*
- (ii) *n is even, A is generated by a set of $n/2$ pairwise distinct transpositions, $C_V(G) = 0$, $V = [V, G]$, and $|A| = 2|V/C_V(A)|$.*
- (iii) *n is even, A is a subgroup of index 2 in a group generated by $n/2$ pairwise distinct commuting transpositions, $C_V(G) = 0$, $V = [V, G]$, and $|A| = |V/C_V(A)|$.*
- (iv) *$n = 4$, $A = O_2(G)$, $|V| = 8$, and either $V = [V, G]$ and $|A| = |V/C_V(A)|$ or $C_V(G) = 0$ and $|A| = 2|V/C_V(A)|$.*
- (v) *$n = 6$, $|A| = 8$, $V = [V, G]$, and $|A| = |V/C_V(G)|$.*
- (vi) *$n = 8$, $|A| = 8$, every non-identity element of A is the product of three pairwise disjoint transpositions, $C_V(G) = 0$, $V = [V, G]$, and $|A| = |V/C_V(G)|$.*

Proof. For any $m \geq 2$, denote by $P(m)$ the permutation module of dimension m for $Sym(m)$ over $\mathbb{F}_2$, $P_0(m)$ the submodule of $P(m)$ of index 2, $\overline{P}(m)$ the quotient of $P(m)$ by $C_{P(m)}(Sym(m))$, and $\overline{P}_0(m)$ the image of $P_0(m)$ in $\overline{P}(m)$.

We proceed by induction on $|V|$. The cases where $n \leq 4$ may be verified by inspection, so we assume that $n \geq 5$. (As G acts faithfully on V, by assumption, we have $V = P(2)$ if $n = 2$, and $V \neq \overline{P}_0(4)$ if $n = 4$.) Suppose that $V \neq \overline{P}_0(n)$. If n is odd then $P(n) \cong \overline{P}_0(n) \oplus C_V(G)$, so we may assume that n is even. Set $V_0 = [V, G]$ and set $\overline{V} = V/C_V(G)$. Induction implies that one of the outcomes (i) through (vi) applies with $\overline{V}_0$ in place of V. Suppose that A is generated by a set $\mathcal{A}$ of commuting transpositions. Then $|\mathcal{A}| \leq n/2$, and

$$(1) \qquad |A| \geq |V/C_V(A)| \geq |\overline{V}_0/C_{\overline{V}_0}(A)| \geq |A|/2,$$

where the final inequality in (1) is strict unless $|\mathcal{A}| = n/2$. Thus, (i) holds if $|\mathcal{A}| < n/2$. If $|\mathcal{A}| = n/2$ and $V \neq V_0$, then $V \neq V_0 + C_V(A)$ and $|A| = |V/C_V(A)|$, and we again have (i). Otherwise, if $V = V_0$ then $C_V(A) = C_V(\langle \mathcal{A}_0 \rangle)$ for any subset $\mathcal{A}_0$ of A of cardinality $n/2 - 1$, and we have $|A| = 2|V/C_V(A)|$. Thus (ii) holds in this case. Next, take $\mathcal{A}$ to be a set of $n/2$ pairwise commuting transpositions, suppose that A is a subgroup of index 2 in $\langle \mathcal{A} \rangle$, and suppose that A is not generated by a subset of $\mathcal{A}$. Then $C_V(A) = C_V(\langle \mathcal{A} \rangle)$, and so (iii) holds in this case. Next, suppose that $n = 6$, $|A| = 8$, and A is not generated by transpositions. Then A is conjugate in G to the group $\langle (1\ 2),\ (3\ 4)(5\ 6),\ (3\ 5)(4\ 6) \rangle$, and direct calculation then shows that $C_V(A) \leq V_0$. As $|A| = |\overline{V}_0/C_{\overline{V}_0}(A)|$, we then have (v). Finally, suppose that $n = 8 = |A|$ and that every element of $A^\#$ is the product of three pairwise disjoint transpositions. Here $N_G(A) \cong 2^3 : L_3(2)$, and both the commutator series and the central series of A with $P(8)$ have the shape $(1, 3, 3, 1)$. Then $|A| \geq |V/C_V(A)|$ if and only if $V = \overline{V}_0$, and so (vi) holds in this case. Thus, we may assume henceforth that $V = \overline{V}_0 \cong \overline{P}_0(n)$, $n \geq 5$.

Let $\{x_i \ : \ 1 \leq i \leq n\}$ be the standard basis for $P(n)$, and identify V with $\overline{P}_0(n)$. Write $x_{i,j}$ for the image in V of $x_i + x_j$. Fix $a \in A^\#$ so that the number k of non-trivial orbits of a on $\{1, 2, \cdots, n\}$ is as small as possible. Identify a with $(1\ 2)(3\ 4) \cdots (2k-1\ k)$, and denote by H_1 the pointwise stabilizer in G of $\{2k+1, \cdots, n\}$ and by H_2 the pointwise stabilizer in G of $\{1, \cdots, 2k\}$. Set $K = C_{H_1}(A)$. Then $C_G(a) = K \times H_2$, and we have $K \cong 2^k : Sym(k)$ and $H_2 \cong Sym(m)$. Denote by E the subgroup of K generated by the set of pairwise disjoint transpositions whose product is a. (Thus, $E = O_2(K)$ unless $k = 2$ or 4.) Then $A \cap E = 1$, by the minimality of k. Choose a complement B to $\langle a \rangle$ in A. Also, set $V_i = [V, H_i]$, and set $U = C_{V_1}(E)$.

Suppose first that $n = 2k$, so that $K = C_G(a)$ and $V = V_1$, and $k \geq 3$. If k is odd then $U = C_V(a)$, while if k is even we have $C_V(a) = U + \langle y \rangle$ where $y = x_{1,3} + x_{5,7} + \cdots x_{2k-3,2k-1}$, and where $[y, E] = U$. In any case we have $U \cong \overline{P}(k)$ as modules for K/E, and $|V/U| = 2^{k-1}$. Define ℓ by $\ell = 1$ if k is odd, and $\ell = 2$ if k is even. By induction, we have $|B| \leq 2|U/C_U(B)|$, and so

$$|A| \geq |V/C_V(A)| \geq 2^{k-\ell}|U/C_U(B)| \geq 2^{k-\ell-1}|B| = 2^{k-\ell-2}|A|.$$

Thus $k = 3$ or 4. Suppose $k = 3$. Every fours group in $Sym(6)$ contains an element which is the product of two disjoint transpositions, so the minimality of k yields $|A| = 2$, and a acts as a transvection on V. As only the transpositions in $Sym(6)$ act as transvections, we have a contradiction in this case. So assume that $k = 4$ and $n = 8$. Then $|V/C_V(a)| = 8$, and so $|A| \geq 8$. There exists no elementary abelian subgroup of G of order 16, in which every non-identity element is the product of four pairwise disjoint transpositions, so we have $|A| = 8$. Thus, (vi) holds in this case.

We assume henceforth that $n \neq 2k$. Then $U = C_{V_1}(a)$, and $U \cong P(k)$ as modules for K/E. Also, we have $V_2 \cong P_0(m)$ as H_2-modules, where $m = n - 2k$. Set $W = V_1 + V_2$. Then $|V/W| = 2$, and $C_V(a) = U + V_2 \leq W$. Also, $|V_1 \cap V_2| = 1$ if n is odd, and 2 if n is even, and we have $|V_1/U| = 2^{k-1}$.

Set $B_1 = C_B(H_2)$ and let B_1 be a complement in B to B_2. As $U \cong P(k)$ we have $|U/C_U(B_1)| \geq |B_1|$. Then

$$\begin{aligned} |A| &\geq |V/C_V(A)| = 2|W/C_W(A)| \geq 2^k|U/C_U(B_1)||V_2/C_{V_2}(B_2)| \\ &\geq 2^k|B_1| \cdot 1/2|B_2| = 2^{k-2}|A|. \end{aligned} \tag{2}$$

Thus $k \leq 2$.

Suppose $k = 2$. As $V_2 \cong P_0(m)$, we may apply induction in (2) and find that $|A| = |V/C_V(A)|$, m is even, and B_2 induces on H_2 a group generated by $m/2$ pairwise disjoint transpositions. But B_2 contains no bona fide transpositions, by the minimality of k, so we have $[V_1, B_2] \neq 0$. Let $b \in B_2$ such that b induces a transposition on $\{2k+1, \cdots, n\}$, and such that b is non-trivial on $\{1, \cdots, 2k\}$. Then $b = xt$ where $1 \neq x \in C_K(A)$ and where t is a transposition in H_2. If $B_1 \neq 1$ then $C_K(A) = B_1\langle a \rangle$, so that $x \in A$ and $t \in A$, contrary to the minimality of k. Thus $B_1 = 1$, and now (iii) holds.

Finally, suppose that $k = 1$. Then $B_1 = 1$ and $B = B_2$. We may therefore choose B so that $B \leq K_2$. Suppose that $|A| > |V/C_V(A)|$. Then (2) implies that n is even and that B is generated by a set of $m/2$ transpositions, and so (ii) holds in this case. So assume that $|A| = |V/C_V(A)|$. If B is generated by a set of transpositions then we have (i). So assume that B is not so generated. By induction, m is even, and either (iii) or (iv) applies with B, H_2, and V_2 in the roles of A, G, and V. If (iii), then (iii) holds for G, while if (iv) then (v) holds for G. This completes the proof of the 5.6. □

5.7 Lemma. *Assume Hypothesis 2 with $p = 2$, and with $H = Alt(n)$, $n \geq 5$. Assume that there exists a non-identity subgroup A of G such that A acts quadratically on V, with $|A|^2 \geq |V/C_V(A)|$. If n is even, assume that $G \cong Sym(n)$ and that $|A| \geq |V/C_V(A)|$. Then one of the following holds.*

(i) *$n = 5$ or 7, each non-trivial constituent for H in V is a spin module (of dimension 4 over $\mathbb{F}_2$), and there are at most two such constituents.*

(ii) *$n = 6$ and V is a natural $Sp(4, 2)$-module for G.*

(iii) *$n = 8$ and V is a spin module for G, of dimension 8. Moreover, as a module for H we have $V = U \oplus U'$, where U is a natural $L_4(2)$-module for H and where U' is dual to U.*

(iv) *$n = 9$, $G = H$, $dim(V) = 8$, and V is a spin module for G. Further, A is conjugate in G to the fours group $F = \langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle$, and $|V/C_V(A)| = |V/C_V(a)| = 16$ for any $a \in A^\#$.*

(v) *V is a natural $Sym(n)$-module for G.*

(vi) *n is odd and V is a direct sum of two natural $Sym(n)$- modules for G.*

Suppose further that n is odd and that V is a natural $Sym(n)$-module or a direct sum of two natural $Sym(n)$-modules for G, and let $\mathcal{T}_A$ be the set of all transpositions t in $Sym(n)$ such that t is a factor of some $a \in A$, in a representation of a as a product of pairwise disjoint transpositions. Set $A^* = \langle \mathcal{T}_A \rangle$. Then A^* is elementary abelian, $[V, A] = [V, A^*]$, and $C_V(A) = C_V(A^*)$.

Proof. Let $a \in A^\#$, and suppose first that a is not a member of any quadratic fours group in G. Then $A = \langle a \rangle$, a is a 2-transvection on V, and 5.4 implies that $n = 5$ and that (i) or (v) holds. If (v) holds then $A = A^*$, so we may assume henceforth that a lies in a quadratic fours group B, and we take $B \leq A$ if $|A| \geq 4$.

Let U be a non-trivial irreducible HAB-invariant section of V. Then Theorem 4 of [MS2] implies that U is a spin module or a natural module for HAB. Suppose first that U is a spin module, and that $n \neq 8$. Let F be the fours group given in (vi). Lemmas 4.1 through 4.3 in [MS2] then establish that every quadratic subgroup of HAB of order bigger than 2 is conjugate to F, and that $C_U(x) = 0$ for any 3-cycle x in H. Notice that there exists a 3-cycle x inverted by a. If a is a 2-transvection it follows that $|U| \leq 16$, and that U is the unique non-trivial irreducible constituent for G in V. In that case, 1.2 yields $V = U$, and $n \leq 7$ (since $G = Sym(8)$ if $n = 8$). If now $n = 6$ then the spin module V is isomorphic to the natural $Sp(4, 2)$-module, and so (ii) holds. Suppose $n = 5$ or 7. We observe that A does not act quadratically on the natural $Sym(n)$-module for G, and so every non- trivial irreducible constituent for HA in V is a spin module. Moreover, there are at most two such constituents in V, and we obtain (i). Thus, we may assume that a is not a 2-transvection, and hence also $n \geq 7$.

Now $|A| = 4$ and we may take $A = B = F$. If n is even then $|A| \geq |V/C_V(A)|$, by assumption, and then a is a 2-transvection. Thus, n is odd, and we have $|A|^2 \geq |V/C_V(A)|$. Set $X = O^2(C_H(A))$, and set $t = 1$ if $n = 5$, and otherwise set $t = (3\ 4)(5\ 6)$. Then $X\langle t \rangle \cong Sym(n{-}4)$, and since all quadratic fours groups are conjugate to F it follows that X acts faithfully on $[V, A]$. As $|[V, A]| \leq 16$, we then have $n \leq 9$, and then $n = 9$.

Let x be a 3-cycle inverted by an element of A. As $C_U(x) = 0$ we obtain $dim(U) \leq 8$ Then since $|[U, A]| = |U/C_U(A)|$ we obtain $dim(V) = 8$, and $C_U(a) = C_U(A)$. Thus $|A|^2 = |U/C_U(A)| = |V/C_V(A)|$, and so $U = [V, H]$. Then $U = V$ by 1.2, and so (iv) holds.

Now suppose that U is a spin module for HA and that $n = 8$. Then $G \cong Sym(8)$, and so also $G \cong O_6^+(2)$. The Clifford algebra $\mathcal{C}$ associated with this orthogonal group is isomorphic to the algebra of 8×8 matrices over $\mathbb{F}_2$, by [Chev, II.2.1], and the spin module W for G is isomorphic to a minimal left ideal of $\mathcal{C}$. Thus $dim(W) = 8$. Moreover, as the characteristic is even, G is isomorphic to the spinor group associated with $O_6^+(2)$, and [Chev, II.4.2] implies that W is the direct sum of two inequivalent irreducible representations for $\Omega_6^+(2)$, which are then conjugate via $O_6^+(2)$. As $O_6^+(2) \cong Aut(L_4(2))$, we thereby obtain (iii). Thus, we have exhausted the possibilities where U is a spin module, and we may assume henceforth that U is a natural $Sym(n)$-module for HA, for every non-trivial irreducible constituent U for HA in G.

Let $\Omega = \{1, 2, \cdots, n\}$ be the set on which G has its natural permutation representation, and identify U with the unique non-trivial irreducible constituent in the permutation module $\mathbb{F}_2\Omega$. As A is quadratic, all orbits of A on Ω have length at most 2, and hence A^* is generated by a set of pairwise disjoint transpositions. One computes that $[U, A] = [U, A^*]$ and $C_U(A) = C_U(A^*)$. Suppose n is even. Then $|A^*| = 2|U/C_U(A^*)|$, and since $|A| \geq |V/C_V(A)|$ it follows that U is the unique non-trivial constituent for G in V. Thus, (v) holds in this case, and we may assume that n is odd. Then $|A|^* = |U/C_U(A^*)|$. As $|A|^2 \geq |V/C_V(A)|$, it follows that there are at most two non-trivial irreducible sections for G in V, and if there are two, then $A = A^*$. If there is only one such section then $U = V$, by 1.2. Suppose there are two. As $C_V(H) = 0$, and as $H^1(H, U) = 0$ by 1.3, it follows that we may take U to be a submodule of V, with V/U irreducible. Then 1.8 implies that there is an H-invariant complement W to U in V. As $A = A^*$ there is a transposition $a \in A$, and we have $|V/C_V(a)| = 4$. Then $W \cap W^a \neq 0$, and so $W = W^a$, and W is G-invariant. This yields (vi). □

The following result is immediate from 5.6 and 5.7.

5.8 Corollary. *Assume Hypothesis 2, with $p = 2$, and let H and A be as in 5.7. Then the following hold.*

(a) *If $|A| > |V/C_V(A)|$ then n is even, V is a natural module for G, A is generated by a set of $n/2$ pairwise disjoint transpositions, and $|A| = 2|V/C_V(A)|$.*

(a) *If $|A|^2 < |V/C_V(A)|$, n is odd, and $n \geq 9$, then V is a natural module for G.*

(c) *If $|A| = |V/C_V(A)|$, n is odd, and $n \geq 9$, then $G \cong Sym(n)$ and A is generated by a set of pairwise disjoint transpositions.*

□

5.9 Lemma. *Assume Hypothesis 3, and assume that H is a quasisimple group of Lie type in characteristic p. Then one of the following holds:*

(i) *The Lie rank of $H/Z(H)$ is equal to 1. That is, $H/Z(H) \cong L_2(p^n)$, $U_3(p^n)$, $Sz(2^n)$ (with $p = 2$) or $({}^2G_2(3^n))'$ (with $p = 3$).*

(ii) *$p = 2$, and $H/Z(H) \cong L_3(2^n)$ or $Sp(4,2^n)'$. Moreover, there exists an element t of S such that t induces a non- trivial symmetry on the Coxeter diagram for $H/Z(H)$.*

Proof. Assume that the Lie rank of $H/Z(H)$ is at least 2. Recall that the vertices of the Coxeter diagram associated with $H/Z(H)$ are in one-to-one correspondence with the maximal subgroups of H which contain $S \cap H$. Since $G \in \mathcal{M}^*(S)$, a Sylow p-subgroup of $Aut(H)$ then acts transitively on the vertices of this diagram. It follows (from the classification of Coxeter diagrams) that the diagram has just two vertices, so $p = 2$, and the diagram is of type A_2 or B_2. Thus, (ii) holds. □

Section 6: Lie rank 1 in characteristic p.

In this section we will be concerned with Hypothesis 2, with the additional assumption that H is a group of Lie type, in characteristic p, and of Lie rank 1. We begin by re-establishing some well known properties of these groups.

6.1 Lemma. *Let G be a group containing a normal subgroup $H \cong {}^2G_2(q)$, $q = 3^{2n+1}$, and with $C_G(H) = 1$. Let S be a Sylow 3-subgroup of G and set $T = S \cap H$. Then the following hold.*

(a) *We have $|T| = q^3$, $Z(T)$ is elementary abelian of order q, and $\Omega_1(T)$ is elementary abelian of order q^2. Moreover, T is a trivial intersection set in H, and we have $N_H(T) = TD$ where D is cyclic of order $q-1$, and where D acts regularly on $T/\Omega_1(T)$ and on $Z(T)$. Further, D acts irreducibly on $\Omega_1(T)/Z(T)$, with $|C_D(\Omega_1(T)/Z(T))| = 2$.*

(b) *There is a single conjugacy class of involutions in G, and for any involution t in G we have $C_G(t) = \langle t\rangle \times L$ where L is isomorphic to $L_2(q)$. Further, $C_G(t)$ is the unique maximal subgroup of G containing L, and $L \cap Z(T) = 1$.*

(c) *Any two conjugates of $Z(T)$ generate $O^3(H)$.*

(d) *Suppose that $S - H$ contains an element a of order 3. Set $X = [\Omega_1(T), a]$ and set $A = \langle a^X\rangle$. Then $A = \Omega_1(C_S(a))$, and A is elementary abelian.*

Proof. Part (a) follows from the Chevalley relations (see Tables 2.4 and 2.4.7 in [GLS3]). If $q = 3$ then it is known that H is isomorphic to $\Gamma L(2,8)$, and one observes in this case that (b) through (d) hold. Thus we may assume that $q > 3$ in proving (b) through (d).

Let t be an involution in H and set $M = C_H(t)$. It is then well known (see for example [GLS3, Theorem 4.5.1]) that $M = \langle t\rangle \times L$, where $L \cong L_2(q)$. In particular, a Sylow 2-subgroup R of H is elementary abelian, of order 8, and for any fours group F contained in R we have $C_H(F) \cong F \times D$ where D is dihedral of order $(q+1)/2$. It follows that $\langle t\rangle = C_H(L)$.

Let M be a maximal subgroup of H containing L, with $M \neq C_H(t)$. Then $Z(M) = 1$. Also, we have $O_3(M) = 1$, since every 3-local subgroup of H is contained in a Borel subgroup. For primes other than 2 or 3 the Sylow subgroups of H are cyclic, so $F(M) = 1$

and $F^*(M)$ is simple. A Cartan subgroup of H is cyclic of order $q-1$, so $F^*(L)$ is not isomorphic to $PSL(2, q')$, q' a power of 3. If $F^*(M) \cong {}^2G_2(q_0)$ for some q_0 then a Cartan subgroup of L is contained in a Cartan subgroup of M, and so $q_0 = q$ and $M = G$. Thus $F^*(M)$ is not a Ree group. As $q > 3$, M is not isomorphic to J_1 and M is not isomorphic to a linear group $L_2(r)$, r odd, r not a power of 3. The classification ([B] or [W]) of groups with abelian Sylow 2-subgroups now yields a contradiction to the presumed existence of M, and so $C_G(t)$ is the unique maximal subgroup of G containing L. Since $C_G(z) = T$ for any non-identity element z of $Z(T)$, as follows from (a), we have $L \cap Z(T) = 1$, and (b) holds.

Next, let K be a subgroup of H generated by a pair of conjugates of $Z(T)$. As $C_H(z) = T$ for any non-identity element z of $Z(T)$, we have $Z(K) = 1$, while $O_3(K) = 1$ as T is a T.I. set in H. As $q > 3$ and $O_2(K)$ is elementary abelian of order at most 8, we have also $O_2(K) = 1$, and then $F^*(K)$ is simple. As in the preceding paragraph, we find that $F^*(K)$ is not isomorphic to $L_2(r)$ for r odd, r not a power of 3, or to J_1. Hence $F^*(K)$ is a Ree group ${}^2G_2(q_0)$ or a linear group $L_2(q_0)$, q_0 a power of 3. Comparison of a Cartan subgroup of $F^*(K)$ with a Cartan subgroup of H yields $q_0 = q$, and $K \cong L_2(q)$. Then K contains a subgroup isomorphic to $L_2(3)$, and so a non-identity element z of $Z(T)$ normalizes a fours group F in H. As $C_H(F)$ is of order prime to 3, z then normalizes a Sylow 2-subgroup of $C_H(F)$, of order 8, and then $|C_H)z)|$ is even. This contradiction proves (c).

Now let X, a and A be as in (d). Then the coset Ta contains an element a_0 such that a_0 induces a field automorphism on H. A Cartan subgroup of $N_H(T)$ acts regularly on $T/\Omega_1(T)$, so we may assume that $a \in Xa_0$. Thus, $C_{\Omega_1(T)}(a_0) = C_{Omega_1(T)}(a) = [X, a_o] = [X, a]$. If g is an element of order 3 in $C_S(a)$ then $g \in T\langle a \rangle$, and $g = g_1 a^i$ for some element g_1 of $C_T(a)$ and some power a^i of a. Then $g_1 \in \Omega_1(T)$, and so $g_1 \in [X, a]$. This yields (d). $\square$

6.2 Lemma. *Let G be a group containing a normal subgroup $H \cong Sz(q)$, $q = 2^{2n+1}$, and with $C_G(H) = 1$. Let S be a Sylow 2-subgroup of G and set $T = S \cap H$. Then the following hold.*

(a) *We have $|T| = q^2$, and $Z(T) = \Omega_1(T)$ is elementary abelian of order q. Moreover, T is a trivial intersection set in H, and we have $N_H(T) = TD$ where D is cyclic of order $q-1$, and where D acts regularly on $T/Z(T)$ and on $Z(T)$.*

(b) *Any two distinct conjugates of $Z(T)$ generate $O^2(H)Z(T)$.*

(c) *We have $S = T$.*

Proof. Part (a) is well known and may be justified in the same way as part (a) of the preceding lemma. Part (c) also is well known, and follows from the fact that automorphisms of $Sz(q)$ are induced by automorphisms of $Sp(4, q)$ (where q is an odd power of 2). If $q = 2$ then $G = H$ is a Frobenius group of order 20, where (b) is obvious. So assume henceforth that we have $q > 2$.

Let L be a subgroup of H such that L is generated by two distinct conjugates of $Z(T)$. For any element x of H of odd order, $C_H(x)$ is cyclic of odd order, and it follows that $O_r(L) = 1$ for every odd prime r. Also $O_2(L) = 1$ as T is a trivial intersection set, so we conclude that $F^*(L)$ is a non-abelian simple group. As $|L|$ is relatively prime to 3, L is a Suzuki group, and then since $Z(T) \leq L$ we have $L = H$. Thus (b) holds. □

6.3 Lemma. *Let G be a group containing a normal subgroup $H \cong SU(3, q)$, $q = p^n$, and with $C_G(H) = 1$. Let S be a Sylow p-subgroup of G and set $T = S \cap H$. Then the following hold.*

(a) *We have $|T| = q^3$, and $Z(T)$ is elementary abelian of order q. Moreover, T is a trivial intersection set in H, and we have $N_H(T) = TD$ where D is cyclic of order $q^2 - 1$, and where D acts regularly on $T/Z(T)$ and $|C_D(Z(T)| = q - 1$.*

(b) *Any two distinct conjugates of $Z(T)$ generate a subgroup of H isomorphic to $SL(2, q)$. If $L = \langle Z(T), Z(T)^g \rangle$ is such a subgroup then $N_H(L) \cong GU(2, q)$, and if $q > 2$ then $N_H(L)$ is the unique maximal subgroup of H containing L.*

(c) *Suppose that $S - H$ contains an element a of order p. If p is odd then $q^{1/p}$ is an integer, and $C_H(a) \cong SU(3, q^{1/p})$. If $p = 2$ then $\Omega_1(C_S(a)) = C_{Z(T)}(a)\langle a \rangle = \langle a^{Z(T)}$.*

Proof. That T is a trivial intersection set ffollows from H having Lie rank 1. The rest of part (a) is standard fare and may be obtained by direct computation.

Let L be a subgroup of H generated by two conjugates of $Z(T)$, and let V be the natural 3-dimensional module for H over $F = \mathbb{F}_{q^2}$, endowed with the usual hermitian form. Then $[V, Z(T)]$ is a 1-dimensional singular subspace of V whose stabilizer in H is the Borel group $N_H(T)$. It follows that $[V, L]$ is a hyperbolic plane, and hence the stabilizer in H of $[V, L]$ is isomorphic to $GU(2, q)$. Then $L \cong SL(2, q)$, and this is the first part of (b).

Let M be a subgroup of H containing L, with $M \not\leq N_H(L)$. We observe that L acts transitively (in fact regularly) on the set of singular points not contained in $[V, L]$, and acts transitively on the set of singular points contained in $[V, L]$. The stabilizer in H of $[V, L]$ is equal to $N_H(L)$, so we conclude that M has just one orbit on the set of singular points of V. Then $H = N_H(Z(T))M$, and we have $\langle Z(T)^M \rangle = \langle Z(T)^H \rangle \leq M$. As H is quasisimple if $q \neq 2$, we then have $M = G$ or $q = 2$, and this completes the proof of (b).

Suppose next that we are given an element a of order p in $S - H$. There is an element a_0 of the coset Ta such that a_0 induces a field automorphism on H, and one observes that a_0 acts freely on $T/Z(T)$. Denote by T_0 the inverse image in T of $C_{T/Z(T)}(a_0)$. If $p = 2$ then a_0 acts by inversion on T_0, and otherwise $C_T(a_0)$ is isomorphic to a Sylow p-subgroup of $SU(3, q^{1/p})$. In either case, all elements of order p in $T_0 a_0$ are fused by T to elements of $C_{Z(T)}(a_0)a_0$. Let D be an a_0-invariant complement to T in $N_H(T)$. Then all elements of order p in $C_{Z(T)}(a_0)a_0$ are fused by $C_T(a_0)$, and so $\langle a \rangle$ is conjugate to $\langle a_0 \rangle$ in $N_H(T)$. This proves (c). □

We require some of the representation theory of groups of Lie type, as developed in [St1]. Thus, let X be the universal version of a group of Lie type in characteristic p, let U be a Sylow p-subgroup of X,and let H be a complement to U in $N_X(U)$. Set $q' = |H_0| + 1$ where H_0 is a cyclic subgroup of H of maximal order. (That is, $q' = e + 1$

where e is the exponent of H.) Then q' is a power of p. Set $F = \mathbb{F}_{q'}$.

If X is a Chevalley group or a Suzuki-Ree group, set $q = q'$ and set $d = 1$.

If X is a Steinberg variation (and not a Suzuki-Ree group) obtained in the standard way from a Chevalley group Y via a graph automorphism of order d ($d = 2$ or 3), set $q = (q')^{1/d}$.

With q defined in the above way, we write $X = X(q)$. Then $\mathbb{F}_q$ is the usual "field of definition" of X, as expressed, for example, in the formula for the order of X as given in Table 16.1 in [A3]. (We mention, however, that for the Suzuki-Ree groups there is an alternative formalism, whereby $d = 2$, and where q is taken to be the irrational number $(q')^{1/2}$.)

6.4 Lemma. *Let $X = X(q)$ be a group of Lie type in characteristic p, and let $F = \mathbb{F}_{q^d}$ be the field defined as above. Further, let V be an irreducible $\mathbb{F}_pX$-module, and set $F_0 = End_X(V)$. Then the following hold.*

(a) *F is a splitting field for X over $\mathbb{F}_p$.*
(b) *We have $dim_{F_0}(C_V(U)) = 1$ for any Sylow p-subgroup U of X.*

Proof. Part (a) is Corollary (a) to Theorem 46 in [St2]. Theorems 44(b) and 46(b) in [St2] yield (b).

Let $X = X(q)$ and $F = \mathbb{F}_{q^d}$ be as above, and regard X as the set of fixed points of a Steinberg endomorphism of a simple algebraic group $\overline{X}$ over an algebraic closure of F. Let $\overline{T}$ be a σ-invariant maximal torus of $\overline{X}$, let Σ be the root system of $\overline{X}$ with respect to $\overline{T}$, let Π be a fundamental system for Σ, and let Λ be the weight lattice of $\overline{T}$. A weight $\lambda \in \Lambda$ is **basic** if either

(1) X is not a Suzuki-Ree group and $0 \leq \langle \lambda, \alpha \rangle$ for all $\alpha \in \Pi$, or

(2) X is a Suzuki-Ree group and we have $0 \leq \langle \lambda, \alpha \rangle$ for all short $\alpha \in \Pi$, and $\langle \lambda, \alpha \rangle = 0$ for all long $\alpha \in \Pi$.

Let U be an irreducible FX-module, with high weight λ. Then U is a **basic module** for X if λ is a basic weight.

6.5 Lemma. *Let $X = X(q)$ and $F = \mathbb{F}_{q^d}$ have the meanings given above, and assume that X is a Steinberg variation or a Suzuki-Ree group. Let $X^* = X^*(q^d)$ be a Chevalley group such that X is obtained from X^*, in the standard way, via a graph automorphism or, in the Suzuki-Ree cases, via the composition of a graph and a field automorphism. Then the irreducible (resp., basic irreducible) modules for X over F are the restrictions to X of the irreducible (resp., basic irreducible) modules for X^*.*

Proof. Let $\overline{X}$ be a simple algebraic group such that $X^* = O^{p'}(C_{\overline{X}}(\sigma^*))$ where σ^* is a Steinberg endomorphism of $\overline{X}$, and let τ be an automorphism of X^* such that $X = O^{p'}(C_{X^*})(\tau)$. Then $\sigma \circ \tau$ is a Steinberg endomorphism of $\overline{X}$, and $X = O^{p'}(C_{\overline{X}}(\sigma \circ \tau))$. Let $\overline{F}$ be an algebraic closure of F. The theory in [St2] establishes that any irreducible

$\overline{F}X^*$-module $\overline{U}$ is the restriction to X^* of an irreducible $\overline{FX}$-module, and the same is true of any irreducible $\overline{F}X$-module. Thus any irreducible $\overline{F}X$-module is the restriction to X of an irreducible $\overline{F}X^*$-module. As F is a splitting field for both X and X^*, by 6.4(a), it follows that any irreducible FX-module is the restriction to X of an irreducible FX^*-module. The corresponding statement concerning basic modules is then immediate from the definition of the basic modules. □

6.6 Lemma. *Let $X = X(q)$, $F = \mathbb{F}_{q^d}$, V, and F_0 be as in 6.4, and set $\widetilde{V} = V \otimes_{F_0} F$. Denote by Γ the full automorphism group of the field F, and by Γ_0 the Galois group of F over F_0. Set $t = |\Gamma|$, $m = |\Gamma_0|$, and set $r = t/m$. Let $\{\phi_1, \cdots, \phi_r\}$ be a complete set of coset representatives for Γ_0 in Γ, and write $\Gamma_0 = \{\psi_1, \cdots, \psi_m\}$. Then the following hold.*

(a) *There exist basic irreducible modules $M_1, \cdots, M_r$ for X such that, upon setting*

$$N_i = M_i^{\phi_i\psi_1} \otimes \cdots \otimes M_i^{\phi_i\psi_m}$$

we have an isomorphism

$$\widetilde{V} \cong N_1 \otimes \cdots \otimes N_r$$

of FX-modules. (The modules M_i are not necessarily pairwise distinct.)

(b) *With the modules M_i as in (a), set $d_i = dim_F(M_i)$. Then*

$$dim_{F_0}(V) = dim_F(\widetilde{V}) = (d_1 \cdots d_r)^m.$$

(c) *If k is an integer such $|V| \leq |F|^k$, then $(d_1 \cdots d_r)^m \leq km$.*

Proof. Let $(\alpha_1, \cdots, \alpha_t)$ be a fixed ordering of Γ, and let $\mathcal{B}$ be a set of representatives of the isomorphism classes of basic irreducible FX-modules. As $\widetilde{V}$ is an irreducible FX-module, Steinberg's tensor product theorem states that there exists a uniquely determined sequence $(M_{i_1}, \cdots, M_{i_t})$ of elements of elements of $\mathcal{B}$ such that

$$(*) \qquad \widetilde{V} \cong M_{i_1}^{\alpha_1} \otimes \cdots \otimes M_{i_t}^{\alpha_t}.$$

Here $\widetilde{V}$ is a module for $G \times \Gamma_0$ over F_0, in a unique way compatible with the action of G. The uniqueness of the tensor decomposition in (*) then yields (a). Parts (b) and (c) are then immediate. □

6.7 Lemma. *The following hold.*

(a) *Let $X = SL(2, q)$, $q = p^n$, and for each i, $1 \leq i \leq p$, let M_i be the X-module of homogeneous polynomials of degree $i - 1$ in two variables. Then $\{M_i\}_{1 \leq i \leq p}$ contains exactly one representative from each isomorphism class of basic irreducible F_qX-modules.*

(b) *Let $X = SL(3, q)$, $q = 2^n$. Let V be the natural module for L, U the adjoint module, and 1 the trivial module. Then $\{1, V, V^*, U\}$ contains exactly one representative from each isomorphism class of basic irreducible F_qX-modules.*

(c) *Let $X = Sp(4, q)$, $q = 2^n$. Let V be the natural module for L, V' the contragredient module to V, and 1 the trivial module. Then $\{1, V, V', V \otimes V'\}$ contains exactly one representative from each isomorphism class of basic irreducible F_qX-modules.*

Proof. The number of isomorphism classes of basic irreducible modules for a (non-twisted) Chevalley group X in characteristic p, and having a root system of rank r, is p^r. So, we have the correct number of modules listed in parts (a) through (c) of the lemma, and it remains to check that the given modules for the given groups are in fact irreducible and basic. In the case of $SL(2, q)$, this result is fundamental and well known (see [St2, page 219]), and requires no further discussion here.

Set $F = \mathbb{F}_q$, $q = 2^n$, and let $\overline{F}$ be an algebraic closure of F. For the groups $\overline{L} = SL(3, \overline{F})$ or $Sp(4, \overline{F})$, let $\overline{T}$ be the maximal torus given by the diagonal matrices in $\overline{L}$, let $\overline{B}$ be the Borel subgroup given by the upper triangular matrices in $\overline{L}$, let Σ be the root system determined by $\overline{T}$, and let $\Pi = \{\alpha_1, \alpha_2\}$ be the fundamental system in Σ determined by $\overline{B}$. Then let λ_1 and λ_2 be the characters of $\overline{T}$ given in the usual way by $\langle \lambda_i, \alpha_j \rangle = \delta_{i,j}$. We may assume that the ordering of Π has been chosen so that λ_1 is the highest weight for the natural module V for L. Then λ_2 is the highest weight for the dual of V if $\overline{L} = SL(3, \overline{F})$, or for the contragredient of V if $\overline{L} = Sp(4, \overline{F})$.

Take $L = SL(3, q)$, $q = 2^n$, and let L_0 be the natural $SL(3, 2)$ subgroup of L (i.e. the subgroup in which all the matrix entries are in $\mathbb{F}_2$). Then all irreducible modules for L_0 are basic. In addition to the trivial module, the natural module, and the dual of the natural module (with high weights 0, λ_1, and λ_2, respectively), there is an irreducible module U_0 for L_0 of dimension 8; namely the Steinberg module, and its highest weight is $\lambda_1 + \lambda_2$. By direct calculation, the adjoint module $\overline{U}$ for $\overline{L}$ contains a high weight vector v with corresponding weight $\lambda_1 + \lambda_2$. As $dim_{\mathbb{F}_2}(U_0) = dim_{\overline{F}}(\overline{U})$, it follows that $\overline{U} \cong U_0 \otimes \overline{F}$ as modules for L_0. In particular, $\overline{U}$ is an irreducible $\overline{F}L_0$-module, and hence also an irreducible $\overline{F}L$-module. The adjoint module U for L is an F-form of $\overline{U}$, and so U is irreducible for L with highest weight $\lambda_1 + \lambda_2$. This weight is basic, so we have (b).

Now take $L = Sp(4, q)$. The module $V \otimes V'$ is irreducible by [St2, pages 218-19], and its highest weight is $\lambda_1 + \lambda_2$. As this weight is basic, we then have (c). $\square$

6.8 Lemma. *Assume Hypothesis 2, with $H/Z(H)$ isomorphic to $L_2(q)$, $q = p^n$. Let A be an elementary abelian p-subgroup of S such that $|A|^2 \geq |V/C_V(A)|$. Then $|A| \leq |V/C_V(A)|$, and one of the following holds.*

(i) *V is a natural $SL(2, q)$-module for H.*

(ii) *For any irreducible H-submodule W of V, both V and V/W are natural $SL(2, q)$-modules for H. Moreover, we have $|A|^2 = |V/C_V(A)|$, and A is a Sylow p-subgroup of H.*

(iii) *q is odd, V is a natural $\Omega_3(q)$-module for H, $|A|^2 = |V/C_V(A)|$, and A is a p-Sylow subgroup of H.*

(iv) *q is a perfect square, $H \cong \Omega_4^-(q^{1/2})$, and V is a natural orthogonal module for H.*

(v) *$q = 4$, $G \cong O_4^-(2)$, and for any irreducible G- submodule W of V, both W and V/W are natural orthogonal modules for G. Moreover, we have $|A|^2 = |V/C_V(A)|$, and $A \not\leq H$.*

Proof. Let E be an elementary abelian subgroup of S such that $|E|^2|C_V(E)|$ is as large as possible and, subject to this condition, so that E is maximal with respect to inclusion. Then E is weakly closed in $C_G(T)$, by 2.2. Let U be a non-trivial, irreducible H- invariant section of V, and set $F_0 = End_H(U)$. Set $F = \mathbb{F}_q$, and define the integers r, m, and t, the modules M_i and N_i, and the dimensions d_i, $(1 \leq i \leq r)$ as in 6.6. We observe that since $q+1$ divides the order of H, 2.1 implies that $|V| \geq q^2$.

Set $T = S \cap H$, and suppose first that $E \not\leq T$. Let $a \in E - T$. Then all elements of order p in the coset Ta are fused by T, and so a induces a (non-trivial) field automorphism on H. Denote by T_0 the largest subgroup of T such that $[T_0, a, a] = 1$. Then $[T_0, a] = C_T(a) = C_T(E)$, and since E is weakly closed in $C_G(E)$ we then have $E = C_T(a)\langle a \rangle$.

We claim that two conjugates of E suffice to generate HE. Indeed, if p is odd then the claim follows from a theorem of L.E. Dickson (Theorem 2.8.4 in [Gor]) on subgroups of $L_2(q)$. On the other hand, suppose that $p = 2$. Then an element b of $C_T(a)$ lies in a dihedral subgroup X of H of order $2 \cdot (q+1)$, and X is maximal in H. Thus, our claim holds if $q \neq 4$. If $q = 4$ then $HE \cong Sym(5)$, and the image of E under such an isomorphism is generated by two commuting transpositions. One confirms that $Sym(5)$ is generated by the conjugate fours groups $\langle (12), (34) \rangle$ and $\langle (14)(35) \rangle$, so our claim holds for all q. As $|E| = p \cdot q^{1/p}$, we then have $|V| \leq p^4 q^{4/p}$. As $p^{2n} \leq |V|$ we obtain $p(1 - 2/n) \leq 2$, and then either $p = 2$ or $p = n = 3$. Moreover, we have $|V| \leq 16 \cdot q^2$ if $p = 2$, and $V \leq 3^8$ if $p = n = 3$. We have proved the following result.

(1) If $E \not\leq T$ then $E = C_T(a)\langle a \rangle$ for any $a \in E - T$, and either $p = n = 3$ and $|V| \leq 3^8$, or $p = 2$ and $|V| \leq 16 \cdot q^2$.

On the other hand, suppose that $E \leq T$. As $N_H(T)$ acts irreducibly on T, and as E is weakly closed in $C_H(E)$, we then have $E = T$ and $|E| = q$. Then two conjugates of E suffice to generate H, and so $|V| \leq q^4$. Also, in this case we have $|C_U(E)| = |F_0|$, 6.4(b). Thus:

(2) If $E \leq T$ then $E = T$, $|V| \leq q^4$, and $|U| \leq q^2 q_0$, where $q_0 = |F_0|$.

With (1) and (2) we conclude that $|V| \leq q^4$ in any case. Then 6.6 yields the following information.

(3) We have $(d_1 \cdots d_r)^m \leq 4m$.

Set $d = d_1 \cdots d_r$, and suppose that $m > 1$. Then $d = 2$ and $m \leq 4$. If $m = 4$ then $|U| = q^4$ and $q \geq p^4$, and so (1) shows that $E \leq T$. Then $E = T$, and we have $|U| < q^3$, by (2), so we conclude that $m \leq 3$.

Suppose that $m = 3$. Then $|U| = q^{8/3}$. If $E = T$ then (2) yields $|U| \leq q^2 q^{1/3}$, so in fact we have $E \neq T$. Suppose that $p = 2$. Then (1) gives $16 \cdot q^2 \geq q^{8/3}$. Here n is divisible by 2 (as $E \neq T$) and by 3 (as $m = 3$), and we conclude that $q = 64$. Moreover, we then have $|U/C_U(E)| = |E|^2$, so U is the unique non-trivial constituent for H in V. Then $U = V$, by 1.2. Now $C_V(E \cap H)$ is a subspace of V over F_0, while a acts F_0- semilinearly on V. It follows that $|C_V(E \cap T)| = |C_V(E)|^2$, and then $|E \cap T|^2 |C_V(E \cap T)| > |E|^2 |C_V(E)|$. This is contrary to the definition of E, so we conclude that $p \neq 2$.

With p odd, (1) shows that $G \cong \Gamma L(2, 27)$ and that $|U| = 3^8$. Here $|V/C_V(E)| \leq |E|^2 = 81$, while $|U/C_U(E)| = 81$ since G is generated by two conjugates of E. Thus $V = U$, by 1.2, and we have an F_0-linear action of G on U. Then G acts F-linearly on $\widetilde{U}$. Identify $\widetilde{U}$ with $N \otimes N^{\phi} \otimes N^{\phi^2}$, where ϕ is an automorphism of F of order 3, and identify a with a standard field automorphism of H. Then a acts on $\widetilde{U}$ by permuting the three tensor factors. Explicitly, let $x = (1, 0)$ and $y = (0, 1)$ be the standard basis elements for N. One may then identify a standard basis for $\widetilde{U}$ with the set of monomials of degree 3 in the non-commuting variables x and y, and then $C_{\widetilde{U}}(a)$ is the F-linear span of

$$\{x^3, x^2y + xyx + yx^2, xy^2 + yxy + y^2x, y^3\}.$$

Thus $dim_F(C_{\widetilde{U}}(a) = 4$. One observes that the given basis for $C_{\widetilde{U}}(a)$ is not invariant under $E \cap T$, so $dim_F(C_{\widetilde{U}}(E)) \leq 3$. Then also $dim_{F_0}(C_U(E)) \leq 3$, and so $|U/C_U(E)| \geq 3^5 > |E|^2$. With this contradiction, we have shown that $m \neq 3$, and so $m \leq 2$.

If $m = 2$ then U is an $\Omega_4^-(q_0)$-module, where $q_0 = q^{1/2}$. On the other hand, suppose that $m = 1$. Then (3) yields $d \leq 4$. If $d = 4$ then $|U| = q^4$, so (1) and (2) imply that $E \not\leq T$ and $q = 4$. Then $U \cong N \otimes N^{\phi}$, where N is the natural $SL(2, 4)$-module for H and where ϕ is the non-identity field automorphism. But then U is reducible as an $\mathbb{F}_2H$-module, and contrary to the definition of U. Thus, we have $d \leq 3$. This shows the following.

(4) U is a natural $SL(2, q)$-module, a natural $\Omega_3(q)$- module, or a natural $\Omega_4^-(q_0)$-module ($q_0 = q^{1/2}$), for H. Moreover, if $E \neq T$ then $p = 2$.

We observe that if U is not E-invariant then $E \not\leq T$ and $|C_U(E \cap T)| \geq p^2$. Then $|U/C_U(E \cap T)| \geq |E \cap T|$. For any minimal HE-invariant section W of V involving U we then have

$$|E \cap T|^2 |C_W(E \cap T)| > p^2 |E \cap T|^2 |C_W(E)| \geq |E|^2 |C_W(E)|,$$

and

$$|W/C_W(E\cap T)| \geq |E\cap T|^2.$$

Then $|W| \geq |E|^2|C_W(E)|$, so $|W| = |V| = |E|^2|C_V(E)|$, and

$$|E\cap T|^2|C_V(E\cap T)| > |E|^2|C_V(E)|.$$

This is contrary to the definition of E, so we conclude that U is E-invariant. Moreover, the preceding estimates show that HE has at most two non-trivial irreducible constituents in V, and if there are two then for any choice of U we have $|E| = |U/C_U(E)|$.

If H has only one non-trivial constituent in V then 1.2 gives $V = U$. So assume that H has two non-trivial constituents in V. If $E = T$ then $|U/C_U(E)| = |U|/|F_0| \leq q$, so $|U| \leq q\cdot q_0$, and then $q = q_0$ and U is a natural $SL(2,q)$-module for H. On the other hand, suppose that $E \neq T$. Then (1) and (4) yield $p = 2$ and $|U/C_U(E)| \leq |E| = 2\cdot q^{1/2}$. As two conjugates of E generate G we then have $|U| \leq 4\cdot q$, and since $|U| \geq q^2$ we then have $q = 4$ and $|U| = 16$. If U is a natural $\Gamma L(2,4)$-module for G then $|U/C_U(E)| = 8$, so in fact U is a natural $O_4^-(2)$-module for G. Thus:

(5) Suppose that $U \neq V$. Then H has exactly two non-trivial irreducible constituents in V. Moreover, these constituents are E- invariant, and for any such irreducible constituent U we have $|E| = |U/C_U(E)|$. Either both irreducible constituents are natural $SL(2,q)$-modules for H, or else $q = 4$ and both are natural $O_4^-(2)$- modules for G.

Suppose that $U \neq V$, and suppose that there is a trivial constituent for H in V. As $C_V(H) = 0$ and $V = [V,H]$, by hypothesis, there is then an indecomposable H-submodule W of V such that $[W,H]$ is irreducible for H and such that $|W/[W,H]| = p$. Take $U = [W,H]$. Then (5) says that either U is a natural $SL(2,q)$-module for H, or $q = 4$ and U is a natural $O_4^-(2)$-module for G. In either case, we have $W = U + C_W(E)$. Suppose that U is a natural $SL(2,q)$- module. As $|E| = |U/C_U(E)|$ we then have $E = T$ and $W = U + C_W(T)$. As two conjugates of T generate H we then have $C_W(H) \neq 0$, and W is decomposable. Thus $q = 4$ and U is an $O_4^-(2)$-module, but in that case we contradict 1.4. Thus, H has no trivial constituents in V.

Now let A be any elementary abelian subgroup of S such that $|A|^2 \geq |V/C_V(A)|$. Suppose first that $|E|^2 = |V/C_V(A)|$. Then we may take $A \leq E$ (by definition of E). In particular, if V is a natural $\Omega_3(q)$-module for H we have $A \leq E = T$, and then $A = E$. Thus, (iii) holds in this case. In the same way, if H has two non-trivial irreducible constituents in V then $A \leq E = T$. In the case that these constituents are natural $SL(2,q)$- modules we find that $A = E$, and (ii) holds. In the case that these constituents are natural $O_4^-(2)$-modules we observe that $E\cap H$ induces a 2-transvection on each irreducible constituent, and so $|E\cap H|^2 < |V/C_V(E\cap H|$. Thus $A \neq E\cap H$, and so (v) holds in this case. If V is a natural $\Omega_4^-(q)$-module or a natural $SL(2,q)$-module for H then we make no assertion about A, and we have (iv) or (i).

In order to complete the proof of the lemma, it remains to show that $|A| \leq |V/C_V(A)|$. Suppose false. Then (i) or (iv) holds, by what has already been proved, and we then observe that $A \neq T$. By [REF] we may assume that A is weakly closed in $C_G(A)$, and therefore $A \nleq T$. Setting $A_0 = A \cap T$ we then have $T \neq A_0 \neq 1$ and $|A_0| \geq |V/C_V(A_0)|$. This condition excludes (i), and so (iv) holds. But $\langle A_0^{N_H(T)} \rangle = T$, and [REF] then implies that $|T| \geq |V/C_V(T)|$, which is not the case in (iv). Thus, we have a contradiction, and the lemma is proved. □

6.9 Lemma. *Assume Hypothesis 2, with H isomorphic to the commutator subgroup of a group of Lie type and of Lie rank equal to 1, in characteristic p. Assume that $H/Z(H) \ncong PSL(2,q)$. If $G \cong {}^2G_2(3)$ set $T = S$, and otherwise set $T = S \cap H$. Then $|A|^2 = |V/C_V(A)|$, $A \leq H$, and one of the following holds.*

(1) *(i) $H \cong SU(3,q)$ and V is a natural module for H. Moreover, either $A = Z(T)$ and $[V,A,A] = 0$, or else p is odd, $|A| = q^2$, and $[V,A,A] \neq 0$.*

(2) *(ii) $H \cong Sz(q)$ and V is a natural module for H. Moreover, we have $A = Z(T)$ and $[V,A,A] = 0$.*

Proof. As in the proof of the preceding lemma, we fix an elementary abelian subgroup E of S such that $|E|^2|C_V(E)|$ is as large as possible and, subject to this condition, so that E maximal with respect to inclusion. Then 2.2 implies that E is weakly closed in $C_G(E)$ with respect to G.

Suppose first that $HT/Z(H)$ is isomorphic to ${}^2G_2(q)$, $q = 3^{2n+1}$. Surveying the Schur multipliers of these groups, we find that $Z(H)$ is a 3-group, and so $Z(H) = 1$. We observe right away that $q^3 + 1$ divides $|G|$, and hence $|V| \geq q^6$ by 2.1. Let D be a subgroup of $N_H(T)$ of order $q - 1$, let d be an involution in D, and set $L = O^2(C_H(t))$. Then $L \cong L_2(q)$, and $L \cap T$ is a complement in $\Omega_1(T)$ to $Z(T)$, by 6.1. Suppose that $E \nleq T$. Then 6.1(d) implies that $E = \Omega_1(C_S(a))$ for any $a \in E - T$. We may choose $a \in E - T$ so that a centralizes an involution in $N_H(T)$, and so we may assume that $[a,d] = 1$. Set $X = C_{E \cap T}(d)$. Then $|X| = q^{1/3}$. Here q is an odd power of 3, so $q \neq 9$, and a theorem of L.E. Dickson (2.8.4 in [Gor]) implies that two conjugates of X suffice to generate L. As $E \cap T \nleq X$ we then conclude from 6.1(b) that two conjugates of E suffice to generate HE. Then $|V| = |V/C_V(HE)| \leq 81 \cdot q^{8/3}$. As $q \geq 3^3$ in this case, we then have $|V| \leq q^{4/3}q^{8/3} = q^4$, contrary to $|V| \geq q^6$. We therefore conclude that $E \leq T$. As $\Omega_1(T)$ is abelian, E is normal in $N_H(T)$, and then $E = Z(T)$ or $E = \Omega_1(T)$.

If $E = Z(T)$ then two conjugates of E suffice to generate H, by 6.1(c), and so $|V| \leq q^4$. We therefore conclude that $E = \Omega_1(T)$. Now two conjugates of E generate HE, and so $|V| \leq q^8$. Let U be a non- trivial, irreducible L-invariant section of V. Then $|U/C_U(E \cap L)| \leq q^4$ and since $E \cap L$ is a Sylow subgroup of L it follows from 6.4(b) that $|U| \leq q^5$. Set $F_0 = End_L(U)$, $F = \mathbb{F}_q$, and denote by Γ_0 the Galois group of F over F_0. Define the integers t and m by $|F : \mathbb{F}_p| = t$ and $|F : F_0| = m$, and set $r = t/m$. Set $\widetilde{U} = U \otimes_{F_0} F$, and let modules M_i and N_j, $(1 \leq i, j \leq m)$ be given as in 6.6. Write d_i for the dimension of M_i over F. As $p = 3$ we have $d_i \leq 3$, and there are exactly three basic irreducible modules for $SL(2,q)$. Thus, any M_i is either a trivial module, a natural

$SL(2,q)$-module, or a natural $\Omega_3(q)$-module for the universal cover $SL(2,q)$ of L. As $|U| \leq q^5$, 4.6(c) yields

$$(d_1 \cdots d_r)^m \leq 5m.$$

As $\widetilde{U}$ affords a representation of $SL(2,q)$ with the scalar matrix $-I$ acting trivially, there are an even number of occurances of the natural $SL(2,q)$-module in the tensor decomposition of $\widetilde{U}$ given by 6.6. As $|\Gamma_0|$ is odd, it follows that there are an even number (possibly 0) of the non-trivial modules N_i for which the associated basic irreducible modules M_i are natural $SL(2,q)$-modules. Taking d_1 to be maximal among the numbers d_i, we then have either $d_1 = 3$ and $3^m \leq 5m$, or else $d_1 = d_i = 2$ for some $i \neq 1$ and $4^m \leq 5m$. As also m is odd, we conclude that $d_1 = 3$, $m = 1$, $F_0 = F$, and U is a natural $\Omega_3(q)$-module for L. As $|V| \leq q^8$ there are then at most two non-trivial irreducible constituents for L in V.

Suppose that there L has two non-trivial constituents in V. As $|U/C_U(E \cap L)| = q^2$ we then have $|V/C_V(E \cap L)| = |V/C_V(E)| = q^4$. Then $C_V(L) \leq C_V(E)$, and since $\langle L, E\rangle = H$, by 6.1(b), we conclude that $C_V(L) = 0$. Then 1.5 implies that there are no trivial constituents for L in V, and so $|V| = q^6$. As all involutions in H are conjugate, all have non-trivial fixed points on V, and so the involution d centralizes a subspace of V of order q^3. But one observes that for any involution $x \in L$ we have $|C_U(x)| = q$, and so $|C_V(x)| = q^2$. With this contradiction we conclude that L has a unique non-trivial constituent in V. Then $V = U \oplus C_V(L)$, by 1.3, and so $|E \cap L|^2 = |V/C_V(L)| = q^2$. Then $|E|^2 = |V/C_V(E)| = q^4$, and so $|C_V(E)| \geq q^2$. As $C_V(E) \leq C_V(E \cap L) = C_U(E \cap L) \oplus C_V(L)$, it follows that $C_V(L) \cap C_V(E) \neq 0$, and so $C_V(H) \neq 0$. We therefore conclude that H is not isomorphic to ${}^2G_2(q)$.

It remains to treat the cases where $H/Z(H)$ is a Suzuki group or a 3-dimensional unitary group. Again, let U be a non-trivial, irreducible H-invariant section of V and set $F_0 = End_H(U)$. If $H \cong Sz(q)$ set $F = \mathbb{F}_q$, while if $H/Z(H) \cong U_3(q)$ set $F = \mathbb{F}_{q^2}$. Set $\widetilde{U} = U \otimes_{F_0} F$, and let Γ, Γ_0, M_i, N_i, d_i, m, r, and t be given as in 6.6.

Suppose that $p = 2$ and that $H \cong Sz(q)$. Here we have $S = T$, by 6.2(c). As $\Omega_1(T) = Z(T)$, and since $N_H(T)$ acts irreducibly on $Z(T)$, we then have $E = Z(T)$. Then two conjugates of E suffice to generate H, by 6.2(b), and since $C_V(H) = 0$, it follows that $|V| \leq q^4$. Then 6.6 yields $(d_1 \cdots d_r)^m \leq 4m$. But also, as $q^2 + 1$ divides $|H|$, it follows from 2.1 that $d_i \geq 4$ for any i for which $d_i \neq 1$. As m is odd, we then have $m = 1$ and $d_i = 1$ for all but one index i. That is, U is an algebraic conjugate of a basic irreducible module for H, of dimension 4 over F. The basic irreducible modules for H are obtained by restriction from those for $Sp(4,q)$, by 4.5, so 4.7 implies that U is a natural $Sp(4,q)$-module for H. One then observes that $|U/C_U(Z(T))| = |E|^2$, so $A = E$, and $V = U + C_V(E)$. As $H = O^2(H)$ we then have $U = [V,H]$, and then 1.2 implies that $U = V$. Thus, (ii) holds in this case.

Suppose next that $H/Z(H) \cong U_3(q)$. Then $q^3 + 1$ divides $|H|$, and so $|V| \geq q^6$, by 3.1. Consider first the case where $E \nleq T$. Then 6.3(c) shows that $E = (E \cap T)\langle a\rangle$ where a induces a field automorphism on H. Suppose further that p is odd, so that $C_T(a)$ is isomorphic to a Sylow p- subgroup of $U_3(q^{1/p})$. In particular, we note that $q \neq 9$. Let X

be the largest subgroup of T for which $[X, a, a] = 1$. Then $[X \cap Z(T), a] = C_{Z(T)}(a) = C_{Z(T)}(E)$, and since E is weakly closed in $C_H(E)$ we then have $C_{Z(T)}(a) \leq E$. We claim that $E \cap T \nleq Z(T)$. Suppose false, and let $x \in X - Z(T)$. Then $[x, a] = [x, E] \leq C_T(E)$, and so $\langle E, E^x \rangle$ is elementary abelian and properly contains E. This is contrary to E being weakly closed in its centralizer, and proves the claim.

We next claim that HE is generated by two conjugates of E. Indeed, we have $E \cap Z(T) \leq L$ where L is a subgroup of H isomorphic to $SL(2, q)$. As q is odd and $q \neq 9$, it follows from [Gor, 2.8.4] that L is generated by two conjugates of $E \cap Z(T)$, and then 6.3(b) yields our claim. As $|E| \leq p \cdot q^{2/p}$ it follows that $|V| \leq p^4 \cdot q^{8/p}$. As $q \geq p^3$ we then have $|V| \leq q^4$. But we have seen already that $|V| \geq q^6$, so we have a contradiction at this point. On the other hand, suppose that $E \nleq T$ and that $p = 2$. Then $\Omega_1(T) = Z(T)$, and we conclude from 6.3(c) that $E \cap T = Z(T)$. Let L be a subgroup of H, generated by $Z(T)$ and a conjugate of $Z(T)$, with $L \cong SL(2, q)$. If L is E-invariant then E induces inner automorphisms on L, and there is then an element a_1 of $E - Z(T)$ such that $[L, a_1] = 1$, and we have $L_1 = C_H(a_1)$. As $|E - Z(T)| = q$, and since there are at least q^2 conjugates of L under T, we may therefore choose L so that L is not E-invariant. It then follows from 6.3(b) that two conjugates of E suffice to generate HE. We then obtain a contradiction to $|V| \geq q^6$, just as in the case where p is odd.

We now have $E \leq T$. Suppose that $E \leq Z(T)$. As $N_H(T)$ acts irreducibly on $Z(T)$ we then have $E = Z(T)$. Now 6.3(b) implies that three conjugates of E suffice to generate H, and so $|V| \leq q^6$. Here $F = \mathbb{F}_{q^2}$, so 6.6 yields $(d_1 \cdots d_r)^m \leq 3m$. But also $d_i \geq 3$ if $d_i \neq 1$, so we obtain $m = 1$, and U is a natural $SU(3, q)$-module for H. Here $|E|^2 = |V/C_V(E)|$, so $U = [V, H]$, and then $U = V$, by 1.2. Further, E acts quadratically on V, and since $|E_0|^2 < |V/C_V(E_0)|$ for every proper non- identity subgroup E_0 of E, we conclude that $A = Z(T)$ if $A \leq Z(T)$.

On the other hand, suppose that $E \nleq Z(T)$. As already mentioned, $Z(T) = \Omega_1(T)$ if $p = 2$, so we must have p odd in this case. Now $q < |E| \leq q^2$, and two conjugates of E suffice to generate H. Then $|V| \leq q^8$, and so $(d_1 \cdots d_r)^m \leq 4m$. Again, as $d_i \geq 3$ for all i for which $d_i \neq 1$, we obtain $m = 1$ and $U = V$ is an irreducible FH-module with $dim_F(U) = 3$ or 4. By 4.5, V is the restriction to H of an irreducible module for the group $H^* = SL(3, F)$. Regard H as a subgroup of H^*. Then T is contained in two non-conjugate parabolic subgroups P_1 and P_2 of H^*, and we have $Z(T) \leq O_p(P_1) \cap O_p(P_2)$. Also, we have $P_i = \langle E^{P_i} \rangle$ for both $i = 1$ and 2, and not both P_1 and P_2 centralize $C_V(Z(T))$. It follows that $C_V(Z(T)) \neq C_V(E)$. But $dim_F(C_V(E) \geq 2$ since $|E|^2 \geq |V/C_V(E)|$, so we conclude that $dim_F(C_V(Z(T)) \geq 3$. Then $|V/C_V(Z(T))| = q^2$, and since three conjugates of $Z(T)$ generate H we obtain $|V| \leq q^6$. This contradiction shows that $dim_F(V) = 3$. That is, V is the restriction to H of a natural $SL(3, F)$-module, which is to say that V is a natural $SU(3, q)$-module for H. Then $|E| = q^2$, in order to achieve $|E|^2 \geq |V/C_V(E)|$.

Since E was chosen so that $|E|^2|C_V(E)|$ is as large as possible, we now conclude that $|A|^2|C_V(A)| = |V|$. The maximality of E then yields $A \leq E$ for some choice of E. Then $A \leq H$, and since $|E_0|^2 < |V/C_V(E_0)|$ for any non-identity subgroup E_0 of E other than E and $Z(T)$, we conclude that $A = Z(T)$ or $A = E$. Thus (i) holds, and the lemma is proved. □

We now consider the case in which A acts quadratically on V.

6.10 Lemma. *Assume Hypothesis 4, and suppose that $H/Z(H)$ is a simple group of Lie type in characteristic p and of Lie rank 1. Let A be a non-identity subgroup of S such that $|A|^2 \geq |V/C_V(A)|$ and such that $[V, A, A] = 0$. Then one of the following holds.*

(i) *$H \cong SL(2, q)$, V is a natural $SL(2, q)$-module for H, and $A \leq H$. If $|A| \geq |V/C_V(A)|$ then equality holds, and A is a Sylow subgroup of H.*

(ii) *$H \cong SL(2, q)$, V is a direct sum of two natural $SL(2, q)$-modules for H, A is a Sylow subgroup of H, and $|A|^2 = |V/C_V(A)|$.*

(iii) *$H \cong L_2(q^2)$ and V is a natural $\Omega_4^-(q)$-module for H. If $A \leq H$ then $|A|^2 = |V/C_V(A)|$ and A is conjugate to a Sylow p-subgroup of a subgroup K of H with $K \cong L_2(q)$. If $|A|^2 > |V/C_V(A)|$ then $p = 2$, $|A|^2 = 2 \cdot |V/C_V(A)|$, and either:*

  (a) *$A = (A \cap H)\langle a\rangle$, where a induces a field automorphism on H and where $A \cap H$ is a Sylow subgroup of $C_H(a)$, or*

  (b) *$q = 4$, $|A| = 2$, and A induces a transvection on V.*

(iv) *$G \cong Sym(5)$, V is a direct sum of two natural $O_4^-(2)$-modules for G, $|A|^2 = |V/C_V(A)|$, and $A \not\leq H$.*

(v) *$H \cong SU(3, q)$, V is a natural module for H, $|A|^2 = |V/C_V(A)|$, and A is the center of a Sylow subgroup of H.*

(vi) *$H \cong Sz(q)$, V is a natural module for H, $|A|^2 = |V/C_V(A)|$, and A is the center of a Sylow subgroup of H.*

Proof. Suppose that $H \cong SL(2, q)$, that H has more than one non- trivial irreducible constituent in V. Then 6.8 shows that there are just two such constituents, and no trivial constituents, for H in V. Suppose that the constituents are natural $SL(2, q)$- modules for H. Then 6.8 says that A is a Sylow subgroup of H, and then V is a completely reducible H-module, by 1.6. Thus (ii) holds in this case. On the other hand, suppose that not both of the irreducible constituents for H in V are natural $SL(2, q)$-modules for H. Then 6.8 says that $q = 4$, that $A \not\leq H$, and that both irreducible constituents are natural $O_4^-(2)$-modules for G. Let a be an element of $A - H$. If $|A| = 2$ then $A = \langle a\rangle$ and a induces a 2-transvection on V. Suppose instead that $|A| = 4$. Then $|C_V(A)| = 16$ and for any irreducible constituent U for G in V we observe that $|C_U(A)| = 4$. Since a commutes with an element g of H of order 3, and A is not g-invariant, it follows that $|C_V(a)| = 64$, and that a is a 2-transvection in this case as well. Let K be a subgroup of G generated by three conjugates of a, with $K \cong Sym(4)$. Then, in any case, we have $|V/C_V(K)| = 4$, and if V_0 is a fixed irreducible submodule of V we may choose $v \in C_V(K)$ so that $v \notin V_0$. Now $|v^G| = 5$, and so $\langle v^G\rangle$ is a proper subspace of V. This shows that V is completely reducible, and thus (iv) holds in this case.

We are now reduced to the case where V is irreducible. If $H \cong L_2(q)$ and V is a natural $\Omega_3(q)$-module for H then $A \leq H$, by 6.8. But here p is odd and no non-identity element of H acts quadratically on V, so Hypothesis (4) is violated in this case. If $H \cong SL(2, q)$ and V is a natural $SL(2, q)$-module for H then (i) follows. Assume that

$H \cong L_2(q^2)$ and that V is a natural $\Omega_4^-(q)$-module for H. Suppose further that $A \leq H$. No element of H centralizes a 3-dimensional $\mathbb{F}_q$-subspace of V, so we have $|A| \geq q$. Let K be a subgroup of H with $K \cong L_2(q)$ and with $K \cap S$ a Sylow p-subgroup of K. Set $B = K \cap S$. The conjugates of $B^\#$ under $N_H(T)$ then form a partition of $(H \cap S)^\#$. Here B acts quadratically on V, and for any $b \in B^\#$ we have $C_V(b) = [V, b] = [V, B] = C_V(B)$ is a 2-dimensional subspace of V. Let C be a conjugate of C under $N_H(H \cap S)$, $C \neq B$. Then $H \cap S = BC$, and so $C_V(BC)$ is of dimension 1. Then $C_V(B) \neq C_V(C)$, and so $[V, b, c] \neq 0$ for any non-identity elements $b \in B$ and $c \in C$. We conclude that A is conjugate to B and that $|A|^2 = |V/C_V(A)|$. On the other hand, suppose that $A \nleq H$ and that $|A|^2 > |V/C_V(A)|$. Then the foregoing shows that either $A \cap H = 1$, or $|A \cap H|^2 = |V/C_V(A \cap H)| = |V/C_V(A)|$ and that $A \cap H$ is conjugate to the group B given as above. If $A \cap H \neq 1$ we then have (iii)(a), while if $A \cap H = 1$ then $|V/C_V(A)| = 2$ and we have (iii)(b). Thus (iii) holds if V is a natural $\Omega_4^-(q)$-module for H.

It remains to consider the cases in which $H/Z(H)$ is not a linear group. We then have (v) or (vi), as follows from 6.9 and from elementary properties of the natural modules for $SU(3, q)$ and for $Sz(q)$. □

Section 7: Lie rank 2 in characteristic p

7.1 Lemma. *Let $G = L_3(2)$ and let W be an indecomposable G-module of dimension 4 over $\mathbb{F}_2$. Then there exists a fours group $A \leq G$ with $|C_W(A)| = 2$.*

Proof. Since G is generated by three involutions, and all involutions in G are conjugate, no involution induces a transvection on W. Put $Z = C_W(G)$, and suppose first that $Z \neq 0$. Then $|Z| = 2$ and W/Z is a natural G-module. Let P be a rank-1 parabolic subgroup of G such that $C_{W/Z}(P) = 0$, and put $A = O_2(P)$. Then $C_{W/Z}(A)$ is a fours group on which P acts irreducibly, and since A contains no transvections we conclude that $C_W(A) = Z$. On the other hand, suppose that $Z = 0$. Then W has a submodule U of order 8, on which every involution in G act as a transvection. Now let P be the rank-1 parabolic subgroup with $|C_U(P)| = 2$, and put $A = O_2(P)$. Then $C_U(A) = C_U(P)$, and since A contains no transvections on W we have $C_W(A) \leq U$. Thus $|C_W(A)| = 2$. □

7.2 Lemma. *There are exactly four isomorphism classes of irreducible modules for $Alt(6)$ over $\mathbb{F}_2$. These classes are represented by the principal module 1, a natural $Sp(4, 2)$-module U, the module U' contragredient to V, and a module V of dimension 8 which is a direct summand of the Steinberg module for $Sp(4, 2)$*

Proof. Set $H = Alt(6)$ and $G = Sp(4, 2)$, and identify H with $[G, G]$. There are four 2-regular conjugacy classes in H, and so, by a well known result of Brauer, there are also four isomorphism classes of irreducible modules for H. The modules 1, U, and U' represent three of these classes (with U and U' distinguishable by their restrictions to subgroups of order 3 in H). Let W be the Steinberg module for G. Then W is the reduction mod 2 of an irreducible complex representation of G, written over $\mathbb{Z}$, and since H has no irreducible characters of degree 16 we conclude that W is reducible for H.

Let S be a Sylow 2-subgroup of G, and set $T = S \cap H$. Then S acts freely on W, and so $dim(C_W(T)) = 2$. But W is a direct sum of G-conjugate, irreducible H-submodules, so we conclude that W has an H-submodule V of dimension 8. Now $\{1, U, U', V\}$ is a complete set of representatives of the isomorphism classes of $\mathbb{F}_2H$-modules. □

7.3 Lemma. *Assume Hypothesis 2 with $p = 2$, and assume that $H/Z(H) \cong L_3(2^n)$ or $Sp(4, 2^n)'$. Suppose further that $Z(H) \neq 1$. Then $H \cong SL(3, 2^n)$.*

Proof. Suppose false. As $O_2(H) = 1$, a survey of the Schur multipliers of the groups in question yields $H/Z(H) \cong Alt(6)$ and $|Z(H)| = 3$. Without loss, V is irreducible, and then V may be regarded as a vector space over the field $F = \mathbb{F}_4$. Evidently $dim_F(V) \geq 3$. Also, we may assume that A has been taken to be as small as possible, subject to the condition that $|A|^2 \geq |V/C_V(A)|$. Therefore:

(1) Let B be a subgroup of index 2 in A. Then $|C_V(B)/C_V(A)| \leq 2$, or $B = 1$.

Let X_1 and X_2 be the two maximal subgroups of H containing $S \cap H$, and set $T = N_S(X_1)$. Then also $T = N_S(X_2)$, and since S is contained in a unique maximal subgroup of G we have $|S : T| = 2$. Set $Z = C_V(S \cap H)$, and set $U_i = \langle Z^{X_i} \rangle$, $(i = 1, 2)$. As V is irreducible we have $C_V(H) = 0$, and then since X_1 and X_2 are fused by S, we conclude that $dim_F(U_i/Z) \geq 1$, $(i = 1, 2)$. As $[U_i, O_2(X_i)] = 0$, we have $[U_1 + U_2, Z(S \cap H)] = 0$, and so $V \neq U_1 + U_2$, and $dim_F(V) \geq 4$.

Let R be a Sylow 3-subgroup of H. Then $N_H(R)$ contains a representative from each conjugacy of involutions in HT, and one observes that all involutions in $HT - H$ act non-trivially on $Z(H)$. That is, there does not exist a central extension of the form $3^{\cdot}Sym(6)$.

Suppose that $A = \langle a \rangle$ is of order 2. Then a is a 2-transvection, and since $dim_F(V) \geq 3$ it follows from the preceding paragraph that a commutes with $Z(H)$. Suppose $a \in T$. Then $a \in H$, and three conjugates of a generate H, so $|V| = |V/C_V(H)| \leq 4^3$. This is contrary to $dim_F(V) \geq 4$, so we conclude that $a \notin T$. Then a interchanges the two fours groups in $S \cap H$, and so $(S \cap H)A$ is dihedral of order 16. Then $Z(H)(S \cap H)A$ is a maximal subgroup of HA, and so again, three conjugates of A suffice to generate HA, with a contradiction as before. We therefore conclude that $|A| > 2$.

Suppose that $A \nleq T$, and let $a \in A - T$. Then $C_S(a) \leq Z(S \cap H)$, and so $[U_1 + U_2, A \cap T] = 0$. But a interchanges U_1 and U_2, so $|(U_1 + U_2)/C_{U_1+U_2}(a)| \geq 4$. This is contrary to (1), so we conclude that $A \leq T$. Now suppose that $A \nleq H$, and let $a \in A - H$. Then a centralizes an $\mathbb{F}_2$-hyperplane of $C_V(A \cap H)$, by (1), and so $dim_F(C_V(A \cap H) = 1$. Thus $|C_V(A)| = 2$, and since $|A| \leq 8$ we obtain $|V| \leq 2^7$. but then $dim_F(V) = 3$, and we have the same contradiction as before. Thus $A \leq H$, and $|A| = 4$. Now $A \leq O_2(X_i)$ for some i, and we may take $i = 1$. By conjugating A within X_1 we may assume also that $A \nleq O_2(X_2)$. Set $B = A \cap O_2(X_2)$. Then $|B| = 2$ and $C_V(B) \geq U_1 + U_2$. As $O^{2'}(X_2)$ acts non-trivially on U_2, we have $[U_2, A] \neq 1$, and then $|U_2/C_{U_2}(A)| \geq 4$. This contradicts (1), and the lemma is thereby proved. □

7.4 Lemma. *Let $L = L_3(q)$ or $Sp(4, q)$, $q = 2^n$, and identify L with the group of inner automorphisms of L. Let t be a non-inner automorphism of L of order 2. Then all* *involutions in Lt are conjugate via L. Moreover, the following hold.*

(a) *If $L = L_3(q)$ and n is odd, and t is conjugate to a standard graph automorphism of L, and $C_L(t) \cong L_2(q)$.*

(a) *If $L = L_3(q)$ and n is even, then t is conjugate to a standard graph automorphism (with $C_L(t) \cong L_2(q)$), or a field automorphism (with $C_L(t) \cong L_3(q^{1/2})$), or a graph-field automorphism (with $C_L(t) \cong U_3(q^{1/2})$.*

(c) *If $L = Sp(4, q)$ and n is odd, then t is conjugate to an automorphism of L which induces a non-trivial polarity on the Dynkin diagram of L, and $C_L(t) \cong Sz(q)$.*

(d) *If $L = Sp(4, q)$ and n is even, then t is conjugate to a field automorphism of L, and $C_L(t) \cong Sp(4, q^{1/2})$.*

Proof. Let $\overline{F}$ be an algebraic closure of $F = \mathbb{F}_q$, set $\overline{L} = L_3(\overline{F})$ (resp. $Sp(4, \overline{F})$), and view L as the set of fixed-points for a Steinberg endomorphism σ of $\overline{L}$. Fix a σ- invariant Borel subgroup $\overline{B}$ of $\overline{L}$, a σ-invariant maximal torus $\overline{T}$ of $\overline{B}$, let Σ be the root system determined by $\overline{T}$, and let Π be the fundamental system of roots determined by $\overline{T}$ and $\overline{B}$. Let $\overline{S}$ be the unipotent radical of $\overline{B}$, and set $S = C_{\overline{S}}(\sigma)$, so that S is a Sylow 2-subgroup of L. If $n = 2m$ is even, set $r = 2^m$, and let ϕ be the standard field automorphism of L of order 2, given by $(x_\alpha(v))^\phi = x_\alpha(v^r)$ for $\alpha \in \Sigma$ and $v \in F$. Let ρ be the unique automorphism (resp. angle-preserving, length-changing bijection) of Σ of order 2 which preserves Π, and let γ be the automorphism of L given, in the case of $L = L_3(q)$, by

$$x_\alpha(v)^\gamma = x_{\alpha^\rho}(v),$$

and in the case of $L = Sp(4, q)$ by

$$x_\alpha(v)^\gamma = \begin{cases} x_{\alpha^\rho}(v) & \text{if } \alpha \text{ is long,} \\ x_{\alpha^\rho}(v^2) & \text{if } \alpha \text{ is short.} \end{cases}$$

If $L = L_3(q)$ set $\tau = \gamma$, and if $L = Sp(4, q)$ set $\tau = \gamma^n$. Notice that if $L = Sp(4, q)$ we have $Aut(L) = Inn(L)\langle\gamma\rangle$, $\tau = 1$ if n is even, and τ is an involution if n is odd. Further, if $L = Sp(4, q)$ and n is odd then $C_L(\tau) \cong Sz(q)$. (See [GLS3, 2.5.1].) It therefore only remains to show that all involutions in St are conjugate via L.

Identify L with $Inn(L)$. Let E and F be the two maximal (under inclusion) elementary abelian subgroups of S, and set $Z = E \cap F$. Then $Z = Z(T)$. Suppose first that $F = E^t$. Then either $t \in S\tau$ or $L \cong L_3(q)$ and $t \in S\tau\phi$. Set $J = \{zxx^t \mid z \in C_Z(t),\ x \in E\}$. Then J is the set of elements of S inverted by t, and so Jt is the set of involutions in St. Let $\mu : E \times C_Z(t) \longrightarrow J$ be the mapping given by $(x, z) \mapsto zxx^t$. Then for any $(x, z) \in E \times C_Z(t)$ we have $\mu^{-1}(zxx^t) = \{(xu, zuu^t) \mid u \in Z\}$. Thus $|J| = |E \times C_Z(t)|/|Z|$. If $t \in S\tau$ we then have $|J| = q^2$, while if $L = L_3(q)$ and $t \in S\tau\phi$ we have $|J| = q^{3/2}$. Thus, $|Jt| = |J| = |S : C_S(\tau)|$ if $t \in S\tau$, and again $|Jt| = |J| = |S : C_S(\tau\phi)|$ if $t \in S\tau\phi$. It follows that $t \in \tau^S$ or $(\tau\phi)^S$, and so we are done if t interchanges E and F.

We are now reduced to the case where $t \in S\phi$. Let P be a maximal parabolic subgroup of L containing S, set $X = O^{2'}(P)$, and take $E = O_2(P)$. Then P is ϕ-invariant, and

$|C_{S/E}(\phi)| = |S/E|^{1/2}$. It follows that the number of involutions in $(S/E)\phi$ is equal to the number of S/E-conjugates of ϕ, and so we may take $t \in E\phi$. But also $|C_E(\phi)| = |E|^{1/2}$, and so the number of involutions in $E\phi$ is equal to $|\phi^E|$. Thus t and ϕ are conjugate via S, and the lemma is proved. □

7.5 Proposition. *Assume Hypothesis 3 with $p = 2$, and assume that H is isomorphic to the commutator subgroup of a group of Lie type in characteristic p, with Lie rank greater than 1. Then $p = 2$, and $HA \cong SL(3, q)$ or $Sp(4, q)$, with $q = 2^n$. Moreover, there exists an element s of S which interchanges the two maximal parabolic subgroups of HA containing $S \cap HA$, and one of the the following holds.*

(i) *$H \cong SL(3, q)$ and V is the direct sum of H-submodules U and U^s, where U is a natural $SL(3, q)$-module for H. If $A \not\leq H$ then $q = 2$, $|A| = 4$, $[V, A, A] \neq 0$, and $|A|^2 = |V/C_V(A)|$.*

(ii) *$HA \cong Sp(4, q)$ and V is the direct sum of HA-submodules U and U^s, where U is a natural $Sp(4, 2^n)$-module for H. Further, we have $|A|^{3/2} < |V/C_V(A)|$, and if $[V, A, A] = 0$ then $|A|^2 = |V/C_V(A)|$ and A is conjugate in G to $Z(S \cap HA)$.*

Proof. By 5.9 we have $p = 2$ and $H/Z(H) \cong L_3(q)$ or $Sp(4, q)$ $(q = 2^n)$, or $Alt(6)$. If H is not isomorphic to $Alt(6)$ set $T = S \cap H$, and if $H \cong Alt(6)$ set $T = (S \cap H)C_S(S \cap H)$. Thus, either $T = S \cap H$ or $HT \cong Sp(4, 2)$. Let P_1 and P_2 be the two maximal subgroups of HT containing T. We use the following notation:

$$H_i = O^{2'}(P_i), \;\; Z_i = C_S(H_i), \;\; Q_i = O_2(H_i), \text{ and } V_i = \langle C_V(T)^{H_i} \rangle.$$

For the sake of easy reference, we record also the following basic facts.

(1) Either $Z_i \leq H_i$ or $HT \cong Sp(4, 2)$.

(2) $H_i/Q_i \cong SL(2, q)$, and Q_i/Z_i is a natural $SL(2, q)$-module for H_i/Q_i.

We list a few well known (and easily checked) facts about the Sylow 2-subgroups of $SL(3, q)$, $Sp(4, q)$, and $Alt(6)$, as follows.

(3) We have $T = Q_1Q_2$, $Z(T) = Q_1 \cap Q_2$, and every elementary abelian subgroup of T is contained in Q_1 or in Q_2.

As S is contained in a unique maximal subgroup of G, we have the following result.

(4) There exists $s \in S$ with $(H_1)^s = H_2$, and with $(H_2)^s = H_1$. In particular, the number c of non-trivial irreducible constituents for H_i in V_i is independent of i.

Let X be a non-central chief factor for some H_i in V, and let B be a non-identity subgroup of T. Then for any i, $i = 1$ or 2, B is conjugate in G to a subgroup B_1 of T with $B_1 \not\leq Q_1$. We have $|X| \geq q^2$ and $|X/C_X(B_1)| \geq q$, by 6.8. Thus:

(5) For any non-identity subgroup B of T, we have $|V/C_V(B)| \geq q^c$.

Notice that $[V_1 + V_2,\ Z(T)] = 0$. Then $V \neq V_1 + V_2$, and so $[V, O^2(H_i)] \not\leq V_i$. Since $C_V(H) = 0$, we also have $[V_i, O^2(H_i)] \neq 0$. Then (5) yields the following result.

(6) $c \geq 2$, and $|V/C_V(B)| \geq q^2$ for any non-identity subgroup B of T.

We now choose an elementary abelian subgroup E of S in the following way. If there exists a non-identity elementary abelian subgroup F of T, with $|F|^2 \geq |V/C_V(F)|$, then we take $E \leq T$ so that $|E|^2|C_V(E)|$ is as large as possible and, subject to these conditions, so that $|E|$ is as large as possible. Otherwise, if no such subgroup F of T exists, we take E so that $|E|^2|C_V(E)|$ and then $|E|$ are as large as possible. Then E is weakly closed in $C_G(E)$, by 3.2. In particular, E is invariant under $N_T(C_S(E))$. As $C_S(T) \leq T$ it follows that $E \cap T \neq 1$. Notice that our way of choosing E then yields the following information.

(7) If $E \not\leq T$ then

$$|V| > |F|^2|C_V(F)| < |E|^2|C_V(E)|$$

for any non-identity subgroup F of $E \cap T$.

Let W be a non-trivial, irreducible G-invariant section of V and let U be an irreducible HT-submodule of W. Set $F_0 = End_{HT}(U)$, $F = \mathbb{F}_q$, and note that $F_0 \leq F$, by 6.4(a). Denote by Γ_0 the Galois group of F over F_0, and by Γ the full automorphism group of F. Write $|F_0| = q_0 = 2^m$, and set $r = |\Gamma_0|$. Thus $n = mr$. Set $\widetilde{U} = Y \otimes_{F_0} F$. Let the modules M_i and N_i, $1 \leq r$, be given as in 6.6, and set $d_i = dim_F(M_i)$ and $d = d_1 \cdots d_r$. Further, let the indexing be given so that $d_1 \geq \cdots \geq d_r$, and denote by c_0 the number of irreducible constituents for HT in W.

Suppose first that $HT = HE$ and that HT is not isomorphic to $Alt(6)$. That is, suppose that HE is a group of Lie type. With $E \leq T$, it follows from (3) that $E \leq Q_i$ for some i, (say $i = 1$), and with $HT = HE$ we then have $\langle E^{H_1} \rangle = Q_1$, and thus $E = Q_1$. Let $s \in S$ be as in (4). Then $EE^s = T$ and $E \cap E^s = Z(T)$. Then 2.2 implies that $|T|^2|C_V(T)| \geq |E|^2|C_V(E)|$. In particular, we have $|T|^2 \geq |V/C_V(T)|$ and $|T|^2 \geq |W/C_W(T)|$. As $|C_U(T)| = q_0$, by 6.4(b), we then have $|W| \leq (q_0)^{c_0}q^6$ (resp. $|W| \leq q_0^{c_0}q^8$) if $H/Z(H) \cong L_3(q)$ (resp. $HT \cong Sp(4, q)$). By 6.6(c) we have $d^m \leq 6m+1$ (resp. $8m+1$). Here $d_1 = 3$ or $d_1 \geq 8$ (resp. $d_1 = 4$ or $d_1 \geq 16$) by 6.7, so in fact $d_1 = 3$ (resp. $d_1 = 4$), and if $m > 1$ then $m = 2$ and $d_i = 1$ for $1 < i \leq r$. Further, if $m = 1$ and $r > 1$ it follows that $r = 2$. Thus, we have proved the following result.

(8) Suppose that $HT = HE \ncong Alt(6)$. Then $HT/Z(HT) \cong L_3(q)$ (resp $Sp(4, q)$) and one

of the following holds.

(i) U is a natural module of dimension 3 (resp. 4) for HA.

(ii) $q = q_0^2$, and $\widetilde{U} \cong M \otimes_F M^\phi$ where M is a natural module for HT, and where $\langle \phi \rangle = \Gamma_0$.

With U as in (8i) or (8ii) one observes that $C_U(Q_1) \not\cong C_U(Q_2)$, so U is not invariant under s. Then W contains $U \oplus U^s$, and we obtain

$$6m + 2 \geq 2 \cdot 3^m \qquad (\text{resp. } 8m + 2 \geq 2 \cdot 4^m).$$

It follows that $m = 1$ and that (8i) holds. Moreover, we have shown that any non-trivial, irreducible, $HE\langle s\rangle$-invariant section of V is isomorphic to $U \oplus U^s$, and from this, and from the preceding estimates, it follows that there is a unique such section. Then 1.2 yields $V \cong U \oplus U^s$.

Suppose now that $HE \cong Sp(4, q)$, and then suppose that $A \leq T$. Then $A \leq Q_i$ for some i, and we set $A* = \langle A^{H_i}\rangle$. Thus $A* = Z(H_iT)$, or $O_2(H_iT)$, or $O_2(H_i)$, and it is now a straightforward matter to check that $|A * |^{3/2}|C_V(A*)| < |V|$. Then also $|A|^{3/2}|C_V(A)| < |V|$, by 2.2. Assume that $|A|^{3/2}|C_V(A)| \geq |V|$, and let A be minimal for this property. Then $A \not\leq T$ and we may take A so that $|A_0|^{3/2}|C_V(A_0)| < |A|^{3/2}|C_V(A)|$ for any proper subgroup A_0 of A. Then $N_A(U) = N_A(U^s) = A$. Then any element a of $A - T$ induces a non-identity field automorphism on L, by 7.4. Then $[C_V(T), a] \neq 0$, and so $A \cap T = A$, contrary to what has just been shown. Thus $|A|^{3/2}|C_V(A)| < |V|$.

Continuing to assume that $HE \cong Sp(4, q)$, suppose now that $A \leq HE$ and that $[V, A, A] = 0$. Inspection of the structure of U and of U^s allows us to fix the indices so that $C_U(H_1) \neq 0$ and $C_{U^s}(H_1) = 0$. By (3), and possibly after conjugation by s, we may assume that $A \leq Q_1$. Let R_i, $1 \leq i \leq 3$, be root subgroups of Q_1, with respect to a standard set-up of HT as a group of Lie type, with $Q_1 = R_1R_2R_3$, and taking $Z(H_1) = R_1$ and $Z(T) = R_1R_2$. Set $U_1 = [U, H_1]$. Then $C_U(x) \leq U_1$ for any non-identity element x of Q_1. Here both $U_1/C_U(H_1)$ and Q_1/R_1 are natural $SL(2, q)$-modules for H_1/Q_1, and the commutator map defines a pairing of $U_1/C_U(H_1) \times Q_1/R_1$ into $C_U(H_1)$, defined over F. Suppose that $AR_1 \cap R_i \neq 1$ for both $i = 2$ and 3. Then $C_U(R_i) = C_U(ER_1 \cap R_i)$ for any i, and thus $C_U(AR_1) = C_U(Q_1) = C_U(H_1)$ is of order q. But we also have $R_1 = C_{Q_1}(U/C_U(H_1))$ so $[U, A] \not\leq C_U(H_1)$, and thus A fails to act quadratically on U. We therefore conclude that $AR_1 \cap R_i = 1$ for some i. In particular, we have $|AR_1| \leq q^2$.

If $|C_U(A)| > q^2$ then $A \leq R_1$ and $C_V(A) = C_U(R_1) + C_{U^*}(R_1)$ is of index q^3 in V. In that case we have $|V/C_V(A)| > |A|^2$, so we conclude that $|C_U(A)| \leq q^2$. On the other hand, we have $|C_{U^*}(x)| = q^2$ for any non-identity element x of Q_1, so we have $|V/C_V(A)| \geq q^4$, and hence $|A| = q^2$. It follows that R_1‘A. Now view Q_1/R_1 as a 2-dimensional vector space over F, for the action of H_1/Q_1. This action is doubly transitive on 1-spaces, and the 1-spaces partition the space. As $R_i \cap A = 1$ for some i, and since the same is true for any H_1-conjugate of A, it follows that A is conjugate in H_1 to R_1R_2. Thus, (ii) holds if $HE \cong Sp(4, q)$.

Now assume that $HE \cong SL(3,q)$, and suppose that $A \not\leq H$. Then 7.4 implies that $|A| \leq 2q$, and so $|V/C_V(A)| \leq 4q^2$. Suppose $q > 2$. Then $|V/C_V(A)| \leq q^3$, while 7.4 shows that $|C_V(a)| = q^3$ for any $a \in A - H$. Then $|A| > 4$, so $A \cap T \neq 1$, and $C_V(a) \leq C_V(A \cap T)$. But for $a \in A - H$, either $V = U + U^a$ or a induces a field automorphism on L (and on V), and one checks in either case that $[C_V(a), x] \neq 0$ for any $x \in T$. Thus, we have a contradiction in this case, and so $q = 2$. Then $A = Z(T)\langle a \rangle$, where a induces a graph automorphism on H, and (i) holds. We are thus reduced to the following cases.

(9) Either $E \not\leq T$ or $HE \cong Alt(6)$.

Suppose that $HE \cong Alt(6)$, and set $T_0 = S \cap H$. By (3) and 3.2 we have $E = T_0 \cap Q_i$ for some i, and then $|V/C_V(E)| \leq 16$. Suppose that U is a natural $Sp(4,2)$-module for H. Then $U \neq U^s$, and one checks that $|(U + U^s)/C_{U+U^s)}(E)| \geq 32$. Thus $|V/C_V(E)| > 16$, and we conclude that U is not a natural $Sp(4,2)$-module. Then 7.2 implies that $dim(U) = 8$ and that U is a direct summand of the Steinberg module for $Sp(4,2)$. It follows that E acts freely on U, and thus $64 = |U/C_U(A)| > |E|^2$. This contradiction shows that $HE \ncong Alt(6)$, and thus $E \not\leq T$.

Set $E_1 = E \cap T$, and suppose next that E normalizes H_1 and H_2. Then $|E/E_1| = 2$, and by 7.4 there is an element $b \in E - E_1$ such that b induces a non-identity field automorphism on H. In particular, we then have $q \geq 4$. By (3) we may choose indexing so that $E_1 \leq Q_1$, and then $[Q_1, b] = C_{Q_1}(b)$. We then have $E = \langle b^{Q_1} \rangle$, by 3.2. If $|V_1/C_{V_1}(b)| \geq 4$ then $|V/C_V(E_1)| \leq |E_1|^2$, in violation of (7), so in fact $|V_1/C_{V_1}(b)| = 2$. Then 6.8 implies that $q = 4$ and that $V_1/C_{V_1}(H_1)$ is a natural $O_4^-(2)$-module for $H_1\langle b \rangle$. Now $|E| = 8$ (resp. 16) if $H/Z(H) \cong L_3(q)$ (resp. $(Sp(4,q))'$), and so $|V/C_V(E)| \leq 64$ (resp. 2^8). Then also $|V/C_V(E_1)| \leq 2^5$ (resp 2^7). Set $E_2 = A \cap Z(T)$. Then $|E_1/E_2| = 2$, and we observe that $[V_2, E_2] = [V_2, Z(T)] = 0$, while $|V_2/C_{V_2}(E_1)| \geq 4$. Thus $|V/C_V(E_2)| \leq 8$ (resp 32). If $H/Z(H) \cong L_3(4)$ we then contradict (6), so in fact we have $H \cong Sp(4,4)$ and $|E_2| = 4$. Let $x \in C_{H_1}(b) - T$, and set $E_3 = (E_2)^x$. Then $|E_3/(E_3 \cap Z(T))| = 2$, and it follows, by a repetition of the preceding argument, that $|V/C_V(E_3 \cap Z(T)| \leq 8$. Thus, we violate (6) in this case as well. We have shown:

(10) There exists $a \in E$ such that $(H_1)^a = H_2$.

Fix a as in (10). Set $E_0 = N_E(H_1)$ and, as above, set $E_1 = E \cap T$. Then $|E/E_0| = 2$, $|E/E_1| \leq 4$, and $E_1 = E \cap Z(T)$. Moreover, by 7.4 we have $|E/E_1| = 2$ if $HT \cong Sp(4,q)$. Also, we have $E_1 \leq C_T(a) = C_{Z(T)}(a)$, and so 3.2 implies that $E_1 = [C_{Z(T)}(E_0), a]$. Notice that $|V_1/(V_1 \cap V_2)| = |V_1/C_V(T)| \geq q$, by 6.8. If $|E/E_1|^2 \leq q$ then $|V/C_V(E_1)| \leq |E_1|^2$, which is contrary to (7). Thus $|E/E_1|^2 > q$. Then $q \leq 4$.

Suppose $q = 4$. Then $|E_1| = 2$ and $|E| = 8$. Moreover, we have $|V/C_V(E)| \leq 64$, while $|V/C_V(E_1)| \geq 16$ by (6). It follows that $|V_1/C_V(T)| = 4$, and so $V_1/C_{V_1}(H_1)$ is a natural $SL(2,4)$-module for H_1/Q_1. Then an element of $E_0 - E_1$ induces a field automorphism on $V_1/C_{V_1}(H_1)$, and so $|V_1/C_{V_1}(E)| \geq 8$. But then $|V/C_V(E_1)| \leq 8$, and so we have a contradiction in this case. We therefore conclude that $q = 2$, and $H \cong Alt(6)$ or $L_3(2)$.

Suppose that $H \cong Alt(6)$. Then $|A| = 4$, and $C_H(a)$ is a dihedral group of order 10. Let X be the subgroup of $C_H(a)$ of order 5, and let c be the involution in $A \cap H$. Suppose that X has more than one non- trivial constituent in V. Then $|[V,c]| \geq 16$, and since $|V/C_V(A)| \leq 16$ we obtain $|[V,c]| = 16$ and $C_V(c) = C_V(A)$. Then $[V,A,A] = 0$, and $[V,X,a] = 0$. But also $C_V(X) \leq C_V(c) \leq C_V(a)$ in this case, and so a centralizes V. So, we conclude that X has a single non-trivial irreducible constituent in V. We again obtain $[V,X,a] = 0$. As two conjugates of X suffice to generate H, we have $|C_V(X)| \leq 16$, and so $|V| \leq 2^8$. Let D be a dihedral group of order 8 generated by two conjugates of a. Then $Z(D) = \langle c \rangle$, and since c is not a 2-transvection, by (7), it follows that a is not a transvection. Then $|C_V(X)| = 16$ and $|V| = 2^8$. In particular, we have $|[V,A]| \geq 16$. Moreover, we now have $|V/C_V(a)| = 4$, and $|V/C_V(A)| = 16$. Now also $C_V(A) = C_V(D)$ and, again since D is generated by two conjugates of a, $[V,D] = [V,A]$ is of order 16. Then $[V,A,A] = 0$, and then also $[V,D,D] = 0$, which implies that D is elementary abelian. With this, we conclude that H is not isomorphic to $Alt(6)$.

Suppose finally that $H \cong L_3(2)$. Let U be an irreducible H-submodule of V, and suppose first that U is a natural $L_3(2)$-module. Then $U \not\cong U^a$ as H-modules, and we find that $|(U + U^a)/C_{U+U^a}(A)| = 16$. In view of 1.1, it follows that $V = U + U^a$, and so outcome (i) of the lemma holds in this case. On the other hand, suppose that U is of dimension 8. Then U is the Steinberg module for H, so $|U : C_U(A \cap H)| = 16$. As $|A| = 4$ we then have $U = [V,H]$, $C_U(A) = C_U(A \cap H)$, and A acts quadratically on U. Here $A \cap H = Z(T)$, so we have also $[C_U(Q_1) + C_U(Q_2), A] = 0$. As a interchanges H_1 and H_2, it follow that $[C_U(Q_1), Q_2] = 0$, and then $[C_U(Q_1), H_1] = 0$. Then $[C_U(T), \langle H_1, H_2 \rangle] = 0$, contrary to $C_V(H) = 0$. With this contradiction, the proof of the 7.5 is complete. □

Section 8: Alternating groups, p odd

Theorem. *Let $G = Alt(n)$, $n \geq 5$, and let V be an irreducible G-module over $\mathbb{F}_3$. Suppose that there exists a 3-cycle a in G such that $|V/C_V(a)| = 9$ and such that $0 = [V,a,a,a] \neq [V,a,a]$. Then V is isomorphic to the unique non-trivial constituent in the natural permutation module for G over F.*

Proof. For any m, denote by $P(m)$ the permutation module for $Alt(m)$ over $\mathbb{F}_3$, with basis vectors $x_1, \cdots x_m$ permuted in the natural way by $Alt(m)$. Denote by $P_0(m)$ the codimension-1 submodule of $P(m)$ consisting of the vectors $a_1x_1 + \cdots + a_mx_m$ for which $a_1 + \cdots + a_m = 0$. Set $F(m) = C_{P(m)}(Alt(m))$, and set $\overline{P}(m) = P(m)/F(m)$. Take a to be the 3-cycle (1 2 3), and let H be the subgroup of G fixing the point 1 in the natural permutation representation for G. Similarly, let K be the subgroup of G fixing both 1 and 2, and let L be the subgroup fixing each of 1, 2, and3. Thus $[a,L] = 1$.

(1) We have $dim\ F(m) = 1$. Further, $P(m) = P_0(m) \oplus F(m)$ if n is not divisible by 3,

and otherwise $F(m) \leq P_0(m)$.

The irreducibility of $\overline{P}_0(m)$ will be assumed for $m \leq n$. We shall see that the irreducibility of $\overline{P}_0(n)$ will follow by induction.

(2) Let ℓ be the least integer such that $3+2\ell \geq n$. Then $\ell+1$ conjugates of a generate G.

We will need the following result.

(3) Let W be an $\mathbb{F}_3G$-submodule of V, such that $P_0(n)$ is a submodule of W, and such that with $dim(W/P_0(n)) = 1$. Suppose that there exists a 3- cycle a in G such that $|V/C_V(a)| = 9$ and such that $1 = [V,a,a,a] \neq [V,a,a]$. Then $C_W(G) \neq 0$.

The proof of (3) is as follows. If 3 divides n then $P_0(n) \geq F(n)$ and there is nothing to prove. So assume that 3 does not divide n. Suppose first that $3+2\ell = n$. Then $dim(W/C_W(G)) \leq 2\ell+2 = n-1$, by (2). As $dim(P_0(n)) = n-1$ we then have $W = P_0(n) \oplus C_W(G)$, and $C_W(G)$ has dimension 1. Suppose finally that $3+2\ell = n+1$. Then $3+2(\ell-1) = n-1$ and so H is generated by ℓ 3-cycles. Then $dim(W/C_W(H)) \leq 2\ell = n-2$. As $dim(P_0(n)/C_{P_0(n)}(H)) = n-2$ we conclude that $C_W(H) \not\leq P_0(n)$. Let $x \in C_W(H) - P_0(n)$. Assuming that $[x,G] \neq 0$ we obtain $|x^G| = n$ and so $\langle x^G \rangle$ is a homomorphic image of $P(n)$. Then $W \cong P(n)$, and thus $C_W(G) \neq 0$, proving (3).

Suppose now that 8.1 is false, and let n be minimal for this property. Suppose $C_V(H) \neq 0$ and let $0 \neq x \in C_V(H)$. Then $|x^G| = n$ and $V = \langle x^G \rangle$, and so V is a homomorphic image of $P(n)$. As V is irreducible we are done in this case. We may therefore assume henceforth that $C_V(H) = 0$.

Suppose that 3 divides n. As $C_V(H) = 0$ it follows from (3), and induction on n, that $V \cong P_0(n-1)$ as a module for H. Then also $V \cong P_0(K) \oplus C_V(K)$ as a module for K, where $dim\ C_V(K) = 1$. Further, we then have $V \cong P(n-3) + C_V(L)$, where $C_V(L)$ is of dimension 2. Here $[V,L] \cong P_0(n-3)$, and $[V,L,a] = 0$. As $C_V(L)$ is a-invariant, we then have $C_V(L) = [V,a]$.

(4) If 3 divides n then $[V,L,a] = 0$, $C_V(L) = [V,a]$, and $C_{[V,L]}(L) = [V,a,a]$.

We continue to suppose that 3 divides n. Identify G with the image of G in $GL(V)$, and let t be the element of order 2 in $GL(V)$ given by $C_V(t) = [V,K]$ and $[V,t] = C_V(K)$. Then $[N_G(K),t] = 1$, where $N_G(K) \cong Sym(n-2)$.

Set $G^* = \langle t, G\rangle$. We claim that $G^* \cong Sym(n)$. To prove this, it now suffices to show that $a^t = a^{-1}$, by the standard presentation of $Sym(n)$ as a Coxeter group. This calculation can be made as follows. Take $b = (3\ 4\ 5)$, set $J = \langle a,b\rangle$, and set $U = [V,J]$. Then $J \cong Alt(5)$ and $U \cong P_0(5)$ as a module for J. Identify J with $Alt(5)$, let $\{x_i \mid 1 \leq i \leq 5\}$ be the standard basis of $P(5)$, and identify U with $P_0(5)$. As $b \in K$, t centralizes $[U,b]$. Also, we have $[V,a,a] = C_{[V,L]}(L) \leq [V,K] \leq C_V(t)$, and so $C_U(t) \geq [U,b]+[U,a,a] = \langle x_3 - x_4,\ x_4 - x_5,\ x_1 + x_2 + x_3\rangle$. Now observe that $[U,a] = C_V(L)$, by (4). As $K = \langle b, L\rangle$ we then have $C_{[U,a]}(b) = C_V(K)$, and thus $C_V(K) = \langle x_1 - x_2\rangle$. As t acts as -1 on $C_V(K)$, the action of t on U has now been completely determined, and one may compute directly that t inverts a. In detail: on the 3-dimensional subspace of U with ordered basis $(x_3+x_4+x_5, x_2-x_1, x_1+x_2+x_3)$ the matrices of a and of t are given respectively by

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and one then checks that the matrix for t inverts the matrix for a. This shows:

(5) Suppose that 3 divides n, let t be the element of $GL(V)$ defined above, and identify G with the image of G in $GL(V)$. Set $G^* = \langle t, G\rangle$. Then $G^* \cong Sym(n)$.

We continue to suppose that 3 divides n, and we now form the semi-direct product VG^*. The usefulness of (5) lies in its providing us with a means to produce complements to V in VG^*, by means of generators and relations. (This would be a more difficult task if we were forced to work with the smaller group VG.)

The key to the proof of 8.1 is the following result.

(6) If 3 divides n then $H^1(G,V) \cong \mathbb{F}_3$.

The proof of (6) is as follows. Assume that 3 divides n, and denote by K^* the pointwise stabilizer in G^* of $\{1,\ 2\}$. Then K^* is generated by conjugates of t, i.e. by transvections, and it follows that $C_V(K) = C_V(K^*)$. Using multiplicative notation in VG^*, let w be a non-identity element of $[V,t] = C_V(K^*)$ and set $t_i = tw^i$, $0 \leq i \leq 3$. Then $[t_i, K^*] = 1$. Identify t with the transposition $(1\ 2)$ in G^*, and set $s = (2\ 3)$. Then each t_i is conjugate to t via an element of $C_V(s)$, and so $|t_i s| = 3$ for all i. Setting $G_i^* = \langle t_i, s, K^*\rangle$, it now follows that $G_i^* \cong Sym(n)$, and that G_i^* is a complement to V in VG^*.

Suppose next that there exists $x \in VG$ and indices i and j such that $(G_i^*)^x = G_j$. We may take $x \in V$. We have $G_i^* \cap (G_i^*)^x \geq H$, so that $H^{x^{-1}} \leq G_i^* \cap VH = H$. Thus $x \in N_V(H) = C_V(H) = 1$ and so $G_i^* = G_j^*$. Thus there are at least three conjugacy classes of complements to V in VG^*, and so $|H^1(G^*,V)| \geq 3$. Now let $\hat{G}$ be a complement to V in VG^*. We have $H^1(H,V) = 0$, as follows from (3), so we may assume (after conjugation) that $H \leq \hat{G}$, and then $\hat{G} = \langle tx, H\rangle$ for some $x \in V$. Here $[tx, K^*] = 1$, so $x \in C_V(K) = [V,t]$, and so $\hat{G} = G_i$ for some i. This shows that $|H^1(G^*,V)| = 3$. But then also $|H^1(G,V)| = 3$, as the reader may verify. This completes the proof of (6).

We may now complete the proof of 8.1. Suppose first that $n \equiv 2\ (mod\ 3)$. As $C_V(H) = 0$ it follows from (3), and from induction, that $V \cong P_0(n-1)$ as a module for H. In particular, we have $dim\ V = n-2$. As 5 does not divide the order of $SL(3,3)$ we then have $n > 5$. Now $V \cong P(n-2)$ as a module for K, and then $V \cong P_0(n-3) \oplus C_V(L)$ as a module for L. As $dim\ P_0(n-3) = n-4$ we then have $dim\ C_V(L) = 2$. As $P_0(n-3)$ is irreducible for L we then have $[V, L, a] = 0$ and a induces a transvection on V, contrary to hypothesis.

Suppose next that $n \equiv 1\ (mod\ 3)$. Then V has an H-submodule V_0 with $V_0 \cong \overline{P}_0(n-1)$, and (6) implies that either $V = V_0$ or $V \cong \overline{P}(n-1)$ as a module for H. In particular, we have $dim\ V = n-3$ or $n-2$. As an L- module we then have $V \cong P_0(n-3) \oplus C_V(L)$, where $dim\ C_V(L) \leq 2$. We therefore obtain a contradiction as in the preceding paragraph.

Suppose that $n \equiv 0\ (mod\ 3)$. Then $V \cong P_0(n-1)$ as an H-module. By (6) V is a submodule of an indecomposable G-module W with $dim\ W/V = 1$, and by (3) we have $C_W(H) \neq 0$. Then W is spanned by x^G for any non-zero $x \in C_W(H)$, and W is then a homomorphic image of $P(n)$. Thus, $W \cong \overline{P}(n)$ and $V \cong \overline{P}_0(n)$, as required. □

Lemma 8.2. *Let H be the group $2^{\cdot}Alt(9)$ and let V be a non-trivial, irreducible H-module over $\mathbb{F}_3$, of dimension at most 8. Then either $dim(V) = 8$ and V is a spin module for H, or $dim(V) = 7$ and V is isomorphic to the non-trivial constituent in the natural permutation module for H.*

Proof. Let x be an element of order 3 in H such that the image of x in $H/Z(H)$ is a 3-cycle. If x acts quadratically on V then V is a spin module of dimension 8, by [M]. So we may assume that x does not act quadratically. Let J be a matrix in Jordan canonical form which represents x on V, let m be the number of 3×3 blocks of J, and let n be the number of 2×2 blocks. As x is not quadratic, we have $m \geq 1$. Set $L = E(C_H(x))$. Then $L \cong SL(2, 9)$ or $L_2(9)$, and so any non-trivial module for L over $\mathbb{F}_3$ is of dimension at least 4. Suppose that $m \geq 2$ or that $n \geq 1$. As $dim(V) \leq 8$, it follows that L centralizes the chain $[V, x] > [V, x, x] > 0$, and the chain $C_V(x) \geq C_V(x) \cap [V, x] \geq C_V(x) \cap [V, x, x] \geq 0$. But also, with $m \geq 2$ or $n \geq 1$ we have $dim(V/([V, x] + C_V(x)) \leq 3$. As $[V, L] \neq 0$, we conclude that $m = 1$ and $n = 0$. Then V is isomorphic to the non-trivial constituent in the natural permutation module, by 8.1. □

Theorem 8.3. *Assume Hypothesis $4'$, with p odd, and assume that $G/Z(G) \cong Alt(n)$, $n \geq 5$. If $p = 5$ assume also that $n \neq 5$, and if $p = 3$ assume $n \neq 6$. Then $p = 3$, $|A|^2 = |V/C_V(A)|$, and one of the following holds.*

(i) *$|A| = 3$, A acts non-quadratically on V, $G \cong Alt(n)$, and V is isomorphic to the unique non-trivial irreducible constituent in the natural permutation module for G over $\mathbb{F}_3$.*

(ii) *$G \cong SL(2, 5)$ and V is isomorphic to the natural $SL(2, 9)$-module for H.*

(iii) *$G \cong 2^{\cdot}Alt(9)$, $|A| = 27$, and V is a spin module for G, of dimension 8 over $\mathbb{F}_3$.*

Proof. If A acts quadratically on V then (ii) holds, by 5.6(iii). Thus, we may assume that A is not quadratic. If V is reducible, then 2.2 shows that G has more than one non-trivial constituent in V, and then, by induction, we may assume that a proper submodule U satisfies the conclusion of the lemma. But then $V = C_V(A) + U$ and $[V, G] = U$, so we may in fact assume that V is irreducible.

Suppose first that $|A| = p$, and then suppose further that $p \geq 5$. Then A is not quadratic on V, as follows from [Sa] or from [C3]. Let $a \in A^{\#}$, let a_1 be a p-cycle of a, and put $b = a(a_1)^{-1}$. Then two conjugates of a generate a group $L = K \times \langle b \rangle$, where $K/Z(K) \cong Alt(p)$. As $|V/C_V(a)| \leq p^2$ there is then a homomorphism of L into $SL(4,p)$ which is non-trivial on K. If $p \geq 13$ then K contains an elementary abelian subgroup of order 81, whereas $SL(4,p)$ contains no such subgroup. Thus $5 \leq p \leq 11$, and one observes in these three cases that K has a subgroup K_0 with $K_0/Z(K_0) \cong L_2(p)$. As A acts non-quadratically, and as $[V, A, A, A] = 0$, it follows from 6.8 that K_0 has a unique non-trivial constituent U in V, and that U is a natural $O_3(p)$-module for K_0. In particular, we have $Z(K_0) = 1$, and so $K \cong Alt(p)$ or $3^{\cdot}Alt(7)$. As $Alt(6)$ has no faithful complex representation of degree 4, we conclude that $p = 5$ or $K \cong 3^{\cdot}Alt(7)$. It is easy to check for any element d of order 3 in $X = SL(4,7)$, that any component of $C_X(d)$ is isomorphic $SL(2,7)$ or $SL(3,7)$, and then since $|SL(3,7)|$ is not divisible by 5, we conclude that $p = 5$ and $K \cong Alt(5)$. Here $K = K_0$, and with U as above we have $H^1(K,U) = 0$ by 1.4. Thus $V = U \oplus C_V(K)$. But $|U/C_U(A)| = 25$, so $[C_V(K), A] = 0$, and so $A \leq K$. That is, a is a 5-cycle. Since $n \neq 5$, by hypothesis, it follows that there is a subgroup J of H with $J \cong Alt(6)$ or $3^{\cdot}Alt(6)$, and with J generated by two conjugates of A.

Set $W = [V, J]$. As $|SL(3,5)|$ is not divisible by 9 we have $W \neq U$, and so $|W| = 5^4$. As $|SL(4,5)|$ is not divisible by 27 we have $J \cong Alt(6)$. There is a subgroup K_1 of J with $N_J(A) \leq K_1 \cong Alt(5)$ and with $\langle K, K_1 \rangle = J$. Just as with K, we find that $[V, K_1]$ is an $O_3(5)$-module for K_1, and $W = [V, K_1] \oplus C_W(K_1)$. As $C_W(K) \neq C_W(K_1)$ it follows that $C_W(N_J(A))$ is of dimension 2. Then $C_U(N_J(A)) \neq 0$. But this is contrary to the case, as one may check that an involution in K inverting A acts non-trivially on $C_U(A)$. We conclude that $|A| = 3$.

Fix an identification of $G/Z(G)$ with $Alt(n)$, and suppose that $aZ(G)$ corresponds to a 3-cycle. Then two conjugates of a generate a subgroup X of G containing $Z(G)$ and with $X/Z(G) \cong Alt(5)$. Then $dim([V, X]) = 4$, and it follows from 3.1 that $X \cong Alt(5)$ and $Z(G) = 1$. Then 8.1 yields (i). So assume that a does not correspond to a 3-cycle. Then $n \geq 7$, and one may observe that two conjugates of a suffice to generate a subgroup of G whose order is divisible by 7. (Indeed, if a corresponds to a product of two disjoint 3-cycles then a is contained in a Frobenius subgroup of G of order 21, and if a corresponds to a product of three or more pairwise disjoint 3-cycles then one has only to observe that (1 2 3)(4 5 6)(7 8 9)(1 3 5)(2 6 9)(4 8 7) is a seven-cycle.) As 7 does not divide the order of $SL(4,3)$, we have a contradiction at this point. Thus $|A| > p$.

We continue to fix an identification of $G/Z(G)$ with $Alt(n)$. Fix $a \in A^{\#}$ so as to minimize the number k of p-cycles in writing the permutation $aZ(G)$ as a product of pairwise disjoint p-cycles. Set $C_a = O^2(C_G(a))$. Then $C_a = EK_1 \times K_2$, where E is a normal elementary abelian p-subgroup of C_a of order p^k, $K_1 \cong Alt(k)$, and $K_2/Z(K_2) \cong Alt(n - pk)$. The minimality of k implies that $E \cap A = \langle a \rangle$, and so p divides $|C_a/E|$.

Suppose that A acts non-trivially on some $K \in \{K_1E/E, K_2\}$, and if possible choose K so that $K = K_1E/E$. (Notice that A acts non-trivially on some such K if $p \geq 5$.) As $[V, A, A, A] = 0$ we have $[V, A, A] \leq C_V(a)$, and so A acts quadratically on $V/C_V(a)$.

Also, A acts quadratically on $C_V(a)$, by Hypothesis $4'$. There is then a non-trivial irreducible constituent U for K in V, admitting A, and on which A acts quadratically. As $K/Z(K)$ is an alternating group it follows from [C3] that $p = 3$, or that $p = 5$ and $K \cong SL(2, 5)$. Suppose $p = 5$. Then K may be identified with a component of C_a, and we have $1 \neq Z(K) \leq Z(H)$ Then every non-trivial constituent for K_0 in V is a natural $SL(2, 5)$-module. A Sylow 5-subgroup B of K acts quadratically on every irreducible constituent for K in V, and it then follows from 1.6 that B acts quadratically on V. This is contrary to what has aleady been shown, so we conclude that $p = 3$. Then [M] yields $K \cong 2^{\cdot}Alt(m)$ for some m, $m \geq 4$, so $K = K_2$, $Z(K) = Z(G) \neq 1$, and either $|A/C_A(K)| = 3$ or $m = 6$. As V is irreducible for G, $Z(K)$ acts as -1 on V, and so every irreducible constituent for K in V is non-trivial.

Set $W = C_V(C_A(K))$. Suppose that $|A/C_A(K)|^2 \leq |W/C_W(A)|$. Then 3.3 implies that $C_A(K)$ is an $F2$-offender on V. Induction on $|A|$ then yields $|C_A(K)| = 3$ and that (i) holds with $C_A(K)$ in place of A. This is contrary to $1 \neq Z(H)$, so we conclude that, in fact, we have $|A/C_A(K)|^2 > |W/C_W(A)|$. Then W is irreducible, $m = 4$ or 6, and W is a natural $SL(2, 3)$-module (if $m = 4$) or a natural $SL(2, 9)$-module (if $m = 6$). Moreover, if $m = 6$ then $|A/C_A(K)| = 9$. In either of our two remaining cases, the choice of K implies that $k \leq 3$, and so $|C_A(K)| \leq 9$.

Suppose $m = 6$. Then $|A| \leq 81$ and $C_V(A) = C_W(A)$ is of order 9, so $|V| \leq 3^10$. Since all irreducible constituents for K in V are natural $SL(2, 9)$-modules we then have $|V| = 3^8$ and there are just two such constituents. Then $C_a \cong \langle a\rangle \times K$, so $k = 1$ and $n = 9$, and $|C_V(a)| = 3^4$. Here $[V, a] = C_V(a)$, so a acts quadratically on V. Now [M] implies (iii).

Suppose $m = 4$. If $k = 3$ then $n = 13$, and the minimality of k implies that $A \cap K = 1$, and so $|A| = 9$. If $k < 3$ then $A \cap EK_1 = \langle a\rangle$, and so $|A| = 9$ in any case. As $C_V(A) = C_W(A)$ is of order 3, we then have $|V| \leq 3^5$. Then $|V| = 3^4$ (and V/W is a natural $SL(2, 3)$-module for K). As 7 doesn't divide the ordr of $SL(4, 3)$ we then have $n \leq 6$, and with $|A| = 9$ we get $n = 6$, contrary to hypothesis.

We have now reduced to the case where no K as above exists. Thus $p = 3$, and A acts trivially on C_a/E, whence also $[K_2, A] = 1$. Suppose $k > 3$. Then $C_{C_a}(EK_1/E) = EK_2$, so $A \leq EK_2$, and then $n - 3k = 3$. Then $|A| = 9$ and, by the minimality of k, any $b \in A - \langle a\rangle$ is a product of at least k disjoint 3-cycles, $k - 1$ of which represent orbits of $\langle a\rangle$. But with $k > 3$ we can then choose b so that two at least of the 3-cycles in b are 3- cycles of a^{-1}, and then ab has fewer than k 3-cycles. With this contradiction we conclude that $k \leq 3$.

Suppose $k = 1$. Then $C_a/Z(H) \cong 3 \times Alt(n - 3)$, and since $|A| > 3$ and $[A, K_2] = 1$ we have $n = 6$, contrary to hypothesis.

Suppose that $k = 2$. Then $C_a \cong 3^2 \times Alt(n - 6)$, and $EK_1 = E$. As $A \cap E = \langle a\rangle$ and $[A, K_2] = 1$, we then have $n = 9$ and $|A| = 9$. Here we may identify $Z(H)A/Z(H)$ with

$$\langle (1\ 2\ 3)(4\ 5\ 6),\ (4\ 5\ 6)(7\ 8\ 9)\rangle.$$

There is then a unique element c of A such that c can be represented as aproduct of three disjoint 3-cycles. By [M], c is not quadratic on V, and so c acts non-trivially on

$V/C_V(c)$. Here $\langle c\rangle = Z(S)$ for some Sylow 3-subgroup S of H, and so S acts faithfully on $V/C_V(c)$. Then $|V/C_V(c)| \geq 3^4$, and we conclude that $C_V(c) = C_V(A)$ has index 3^4 in V. Now observe that since a is represented as a product of two disjoint 3-cycles, there exists a subgroup J of H with $a \in J \cong Alt(4)$, and such that every involution t in J is represented as a product of four disjoint transpositions. Suppose $C_V(a) \neq C_V(A)$. Then $|V/C_V(a)| \leq 27$, from which it follows that J has a unique non-trivial constituent in V. That is, we have $|[V, O_2(J)]| = 27$, and $|V/C_V(t)| = 9$. On the other hand, t inverts an element of order 7 in H, whereas 7 does not divide $|GL(4,3)|$. This shows that, in fact, we have $C_V(a) = C_V(A)$, and thus $C_V(A) = C_V(d)$ for all $d \in A^{\#}$.

Set $X = N_H(EA)$. Here $EA = J(S)$ for a Sylow 3-subgroup S of H (so EA is elementary abelian of order 27), and we have $X/EA \cong Sym(4)$, with X acting irreducibly on EA. Now

$$X \leq \langle g \in H \ : \ A \cap A^g \neq 1\rangle$$

and so $C_V(A)$ is invariant under X. Then $C_V(A) = C_V(EA)$. Let x be an element of EA such that x is represented by a 3-cycle, and let L be the component in $C_H(x)$ ($L/Z(H) \cong Alt(6)$). No 3-element of L induces a transvection on $C_V(x)$, by [M] so we have $C_V(x) = C_V(EA)$, and indeed we have shown that $C_V(EA) = C_V(y)$ for all $y \in (EA)^{\#}$. Then $C_V(EA)$ is invariant under the group

$$X^* = \langle g \in H \ : \ EA \cap (EA)^g \neq 1\rangle.$$

We now ask the reader to perform the fairly straightforward exercise of showing that $X^* = H$. With this we have H acting on the 4-space $V/C_V(EA)$, and an evident contradiction.

Finally, suppose that $k = 3$. Then $EK_1 \cong \mathbb{Z}_3 \wr \mathbb{Z}_3$, and the minimality of k implies that $|A \cap EK_1| \leq 9$. Suppose that $|A| > 9$. Then $A \not\leq EK_1$, and since $[A, K_2] = 1$ we conclude that $|K_2| = 3$ and $n = 12$. Let S be a Sylow 3-subgroup of H containing A. Then $S \cong (3 \wr 3) \times 3$, and the minimality of $k = 3$ implies that $A \not\leq J(S)$. Then $A = C_S(A) \geq Z(S)$, so A contains a 3- cycle, and so $k = 1$. We conclude from this contradiction that $|A| = 9$.

For any $b \in A$ such that b is represented as a product of three disjoint 3-cycles, we have $|V/C_V(b)| \geq 3^4$, by the same reasoning as in the treatment of the case $k = 2$. Then, for such an element b, we have $C_V(b) = C_V(A)$, of index 3^4 in V. Suppose next that $A \leq EK_1$. In this case we may identify $Z(H)A/Z(H)$ with the group

$$\langle (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9),\ (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)\rangle. \tag{1}$$

Here every non-identity element of A has a representation as a product of three disjoint 3-cycles. We may assume that $n = 9$, by restricting to an appropriate subgroup of H. Set $X = \langle C_H(b) \ : \ b \in A^{\#}\rangle$. Then $C_V(A)$ is X-invariant. On the other hand, $Z(H)X/Z(H)$ contains all the 3-cycles in the two generators given in (1), and one may check that these six 3-cycles generate $Alt(9)$. Then $C_V(A) = C_V(H)$, and indeed $[V, H] = 0$. We conclude that $A \not\leq EK_1$.

Now $n = 12$ (as $[A, K_2] = 1$) and there are, up to conjugation, two possibilities for $Z(H)A/Z(H)$. These are as follows:

$$\langle (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9),\ (4\ 6\ 5)(7\ 8\ 9)(10\ 11\ 12)\rangle, \qquad \text{or} \tag{2}$$

$$\langle (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9),\ (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)(10\ 11\ 12)\rangle. \tag{3}$$

Suppose that A is as in (2). Then every element of $A^\#$ is represented as a product of three disjoint 3-cycles. Now set $X = \langle C_H(b)\ :\ b \in A^\# \rangle$, as before. Then $C_V(A)$ is X-invarian, and X contains a subgroup $X_0 \cong 3^4 : Alt(4)$, and $O_3(X_0) = \langle A^{X_0} \rangle$. Then $C_V(A) = C_V(O_3(X_0))$, and so $O_3(X_0)$ is an $F1$- offender on V. By Thompson Replacement there then exists a quadratic $F1$- offender B on V. This is contrary to [M], and we thereby conclude that A is as in (3). Take $Z(H)a = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$ and let $b \in A$ with $Z(H)b = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)(10\ 11\ 12)$. Then $\langle b \rangle$ is contained in a subgroup J of H with $J/Z(J) \cong Alt(4)$. If $C_V(b) \neq C_V(A)$ then, as in the case $k = 2$, we find that an involution t in J satisfies $|[V, t] = 9$ and that t inverts an element of H of order 7, contrary to 7 not being a divisor of $|GL(4, 3)|$. Thus $C_V(b) = C_V(A)$. Set $Y = O^2(C_H(b))$. Then $Y \cong 3^4 : Alt(4)$, and $O_3(Y)Z(H)/Z(H)$ is generated by the 3-cycles of $Z(H)b$. Then $a \notin O_3(Y)$, and since we now have $C_V(b) = C_V(a)$ we conclude that $[C_V(b), Y] = 0$. Then $O_3(Y)$ is an $F1$-offender on V, and again, Thompson Replacement yields a quadratic $F1$-offender and a contradiction to [M]. This completes the proof of the theorem. □

Section 9: Alternating groups, $p = 2$

This section contains a single result, which is as follows.

9.1 Proposition. *Assume Hypothesis $4'$, with $p = 2$. Suppose that $F^*(G) = H \cong Alt(n)$, n odd, $n \geq 7$. Then there exists $a \in A^\#$ and an involution $t \in G - \langle a \rangle$ such that $[V, a, t] = 0$.*

Proof. Fix A as in Hypothesis $4'$, and assume that 9.1 is false. The following is then obvious.

(1) For any involution $a \in A$ and for any subgroup D of $C_G(a)$ of even order with $a \notin D$, we have $[V, a, D] \neq 0$.

Suppose first that V is reducible for G. Then 1.2 implies that G has at least two non-trivial constituents in V. As $|A|^{3/2} \geq |V/C_V(A)|$, by Hypothesis $4'$, there then exists a non-trivial irreducible constituent W for G in V such that $|A|^{3/4} \geq |W/C_W(A)|$.

By Timmesfeld Replacement, there is then a quadratic subgroup B of A with $|B|^{3/4} \geq |W/C_W(B)|$, and then 9.4 yields n even, contrary to hypothesis. Thus:

(2) V is irreducible for G.

Let $a \in A^{\#}$. As $n \geq 7$ it follows from (1) and from 5.5 that $|V/C_V(a)| \geq 8$. Suppose that we have $|V/C_V(a)| = 8$. Then $|[V,a]| = 8$, and since $L_3(2)$ has 2-rank equal to 2 it follows from (1) that the 2-rank of $C_G(a)$ is at most 3. Then $n = 7$, and we may record this result as follows.

(3) We have $|V/C_V(a)| \geq 8$ for any involution a in A, with equality only if $n = 7$.

In particular, (3) implies that $|A| > 2$. As A contains no quadratic fours group, we have $C_V(a) \neq C_V(A)$ for $a \in A^{\#}$. If $|A| = 4$ then $|V/C_V(A)| \leq 8$ and $|V/C_V(a)| \leq 4$, contrary to (3). Suppose that $|A| = 8$. Then $|V/C_V(A)| \leq 16$ and $|V/C_V(a)| \leq 8$. Then (3) yields $n = 7$, and since the 2-rank of $Alt(7)$ is just 2 we obtain $G \cong Sym(7)$. Then a may be chosen to be a transposition, whence $C_G(a)$ contains a subgroup X isomorphic to $Alt(5)$, and we have $[V,a,X] = 0$. This is contrary to (1), so:

(4) We have $|A| \geq 16$.

Let $\Omega = \{1, 2, \cdots, n\}$ be the set supporting the natural permutation representation of G. We now fix $a \in A^{\#}$ so that the number of orbits of length 2 for $\langle a \rangle$ on Ω is as small as possible. Denote this number by k, and identify a with the permutation $(1\ 2) \cdots (2k-1\ 2k)$. Set $m = n - 2k$.

Set $C_a = O^2(C_G(a))$. We then have

$$C_a \cong 2^{k-1} : Alt(k) \times Alt(m).$$

Denote by K_1^* the pointwise stabilizer in $C_G(a)$ of $\{2k+1, \cdots, n\}$, and by K_2^* the pointwise stabilizer in $C_G(a)$ of $\{1, 2, \cdots, 2k\}$. Denote by E^* the subgroup of $C_G(a)$ generated by the set of pairwise disjoint 2-cycles whose product is a. Set $K_i = K_i^* \cap C_a$, and $E = E^* \cap C_a$. Then E is elementary abelian of order 2^{k-1}, $K_1/E \cong Alt(k)$, $E/\langle a \rangle$ is a natural $Sym(k)$-module for K_1/E, and $K_2 \cong Alt(m)$. The minimality of k yields:

(5) $A \cap E^* = \langle a \rangle$.

Set $L = O^2(\langle A^{C_G(a)} \rangle$. Suppose that L is solvable, and then suppose that K_1 is non-solvable. Then $[K_1, A] \leq E$, and so $A \leq E^* K_2^*$. Then (4) and (5) imply that the 2-rank of K_2^* is at least 3, so K_2 is non-solvable, $K_2 \leq L$, and L is non-solvable, contrary to assumption. On the other hand, suppose that K_2 is non-solvable. Then $A \leq K_1^*$, and then (4) and (5) imply that K_1 is non-solvable and $K_1 \leq L$. Thus, under the assumption that L is solvable we conclude that C_a is solvable. That is, we have $k \le 4$ and, as n is odd, $m \le 3$. Suppose that $k = 3$ or 4. No involution in K_2^* is the product of 3 or 4 pairwise disjoint transpositions, so the minimality of k yields $A \cap K_2^* = 1$. Let b be an involution in $E^*K_2^*$. As $m \le 3$, either b or ab is a product of fewer than k disjoint transpositions, and so $A \cap E^*K_2^* = \langle a \rangle$. Then $C_A(K_1/E) = \langle a \rangle$, and $|A| \le 8$, contrary to (4). We conclude that $k \le 2$. Then $n \le 7$, again contrary to (4). This proves:

(6) L is non-solvable.

Set $L_i = L \cap K_i$, $i = 1, 2$. Then $L = L_1 \times L_2$. Set $X = C_V(a)$ and $Y = [V, a]$. By Hypothesis $4'$, A acts quadratically on X, and hence also on Y.

Set $A_0 = C_A(L/O_2(L))$. Then $\langle a \rangle \le A_0 = A \cap O_2(LA)$. Suppose that $A_0 \ne \langle a \rangle$. Then $O_2(LA) \ne E^*$, and it follows that either L_1 is solvable (which includes the possibility that $L_1 = 1$) or that $L_2 = 1$. Suppose that $L_2 = 1$. Then $A \le K_1^*$, and L_1 is non-solvable, by (6), and then $A_0 = A \cap E^* = \langle a \rangle$. So in fact $L_2 \ne 1$, and L_1 is solvable. Then $A_0 \le K_1^*$. If $k = 1$ we have $K_1^* = \langle a \rangle$, while if $k = 3$ we have $C_{K_1^*}(K_1) = \langle a \rangle$. So $k = 2$ or 4. Suppose $k = 2$. Then $L_1 = 1$, K_1^* is dihedral of order 8, and $|A_0| \le 4$. On the other hand, suppose that $k = 4$. If $L_1 \ne 1$ then $A \not\le O_2(K_1^*)K_2^*$, and $|C_{O_2(K_1^*)}(A)E^*/E^*| = 2$. Therefore $|A_0| \le 4$ in this case. If instead we have $L_1 = 1$ then $|A_0| \le 8$ since the 2-rank of $O_2(K_1^*)/E^*$ is 2. Thus:

(7) Suppose $A_0 \ne \langle a \rangle$. Then $A_0 \le O_2(K_1^*)$, $k = 2$ or 4, and $|A_0| \le 8$. Moreover, we have $|A_0| = 4$ unless $k = 4$ and $L_1 = 1$.

Fix a complement B to A_0 in A. Set $B_1 = C_B(K_2)$ and let B_2 be a complement to B_1 in B. Set $Y_i = [Y, L_i]$, and set $U_i = Y_i/C_{Y_i}(L_i)$, $(i = 1, 2)$. We will obtain the following result.

(8) Suppose that $C_B(L_2) \ne 1$. Then $[Y_1, L_2] = [Y_2, L_1] = 0$, and

$$|Y/C_Y(B)| \ge |U_1/C_{U_1}(B_1)||U_2/C_{U_2}(B_2)|.$$

Indeed, set $D = C_B(L_2)$. If $L_2 = 1$ then $B_1 = B$ and (8) follows trivially. So we may assume that $L_2 \ne 1$. As $L_2 = [A, L_2] = [B, L_2]$, we have

$$0 = [Y, B, D] = [Y, \langle B^{L_2} \rangle, D] \ge [Y, L_2, D] \ge [Y, L_2, \langle D^{L_1} \rangle].$$

As $D \ne 1$, by assumption, we have $L_1 \le \langle D^{L_1} \rangle$, and thus $[Y, L_2, L_1] = 0$. The Three Subgroups Lemma yields also $[Y, L_1, L_2] = 0$, so it remains only to prove the second assertion in (8). Set $U = U_1 \oplus U_2$. Then U is a homomorphic image of the submodule $Y_1 + Y_2$ of Y, so

$$|Y/C_Y(B)| \ge |U/C_U(B)| \ge |U_1/C_{U_1}(B_1)||U_2/C_{U_2}(B_2)|,$$

and we have (8).

The next step is to show:

(9) $|B| \leq |Y/C_Y(B)|$.

Suppose that (9) is false. If $C_B(L_2) = 1$ then, since m is odd, 5.8 yields $|Y_2/C_{Y_2}(B)| \geq |B|$, and then (9) follows. Thus, we may assume that $C_B(L_2) \neq 1$, and then $|Y/C_Y(B)| \geq |U_1/C_{U_1}(B_1)||U_2/C_{U_2}(B_2)|$, by (8). Again, as m is odd, 5.8 implies that $|U_2/C_{U_2}(B_2)| \geq |B_2|$, and hence $|U_1/C_{U_1}(B_1)| < |B_1|$. In particular, we have $L_1 \neq 1$, and $L_1 = K_1$. Notice that there exists $t \in C_G(a)$ such that $K_1\langle t\rangle/E \cong Sym(k)$. It then follows from 5.8 that k is even and that if $k > 4$ then U_1 is a natural $Sym(k)$-module for K_1/E and B_1 is generated by elements which correspond to transpositions in $Sym(k)$. That is, either $k = 4$ or B contains elements which are the product of two disjoint transpositions. The minimality of k then yields $k = 4$. Then $|B_1| = 2$, and so $|U_1/C_{U_1}(B_1)| \geq |B_1|$. This completes the proof of (9).

We have $|A| = |A_0||B|$, so

$$(*) \qquad |A_0|^{3/2}|B|^{3/2} \geq |V/C_V(A)|.$$

Notice that $V/X \cong Y$ as modules for $C_G(a)$. Then

$$(**) \qquad |V/C_V(A)| = |V/X||X/C_X(B)| \geq |Y||Y/C_Y(B)| = |Y/C_Y(B)|^2|C_Y(B)|.$$

As $|Y/C_Y(B)| \leq |B|$, by (9), we then have

(10) $|A_0|^3 \geq |B||C_Y(B)|^2$, and if $|Y/C_Y(B)| > |B|$ then $|A_0|^3 \geq 16|B||C_Y(B)|^2$.

Suppose that $A_0 = \langle a\rangle$. Then (10) yields $|B| = 2$, $|C_Y(B)| = 2$, and $|Y/C_Y(B)| = 2$. But $L/\langle a\rangle$ has a non- solvable direct factor which, by (1), acts faithfully on Y, and so we have a contradiction in this case. Now (6) and (7) yield:

(11) $|A_0| > 2$, $k = 2$ or 4, and $m \geq 5$.

Suppose next that $k = 4$ and that $|Y| \leq 32$. Then (1) implies that $L_5(2)$ has a subgroup of the form $2^4 : 3 \times Alt(m)$. As $m \geq 5$ we may choose $x \in L_2$ of order 5, and find that $[Y, x]$ is a hyperplane of Y, and that $[Y, x, O_2(K_1)] = 0$. Here $O_2(K_1)/\langle a\rangle$ is elementary abelian of order 16, and contains its centralizer in $L_5(2)$, so we have a contradiction. Thus:

(12) If $k = 4$ then $|Y| \geq 64$.

Suppose that $|Y/C_Y(B)| > |B|$. If also $|A_0| = 4$ then (10) yields $|B| = 1$, which is contrary to (4). Thus $|A_0| = 8$, and (7) implies that $k = 4$, $L_1 = 1$, and $A_0E^* = O_2(K_1^*)$.

Now (10) yields $|B| \leq 8$ so $|A| \leq 64$ and $|V/C_V(A)| \leq 2^9$. Note also that if $|B| = 4$ then $|V/C_V(A)| \leq 2^7$, and if $|B| = 2$ then $|V/C_V(A)| \leq 2^6$. But $|V/C_V(A)| \geq |Y||Y/C_Y(B)|$, by (**), and so $|Y| \leq 32$, contrary to (12). Thus:

(13) We have $|Y/C_Y(B)| = |B|$.

Suppose that $L_1 = 1$. Then $L = L_2$, and B acts faithfully on L_2. Set $Y_0 = U_2/C_{U_2}(L_2)$. Notice that there exists an involution t in $C_H(a)$ such that $L_2\langle t\rangle \cong Sym(m)$. As m is odd it follows from (13) and 5.7 that either Y_0 is a natural module for LB, or $m = 5$ and Y_0 is a spin module for LB, of dimension 4. Suppose that $m = 5$ and Y_0 is a spin module (i.e. a natural $SL(2,4)$-module). Then $|B| = 4$, and since $|A_0| \leq 8$, by (7), we get $|A| \leq 2^5$. Moreover, if $|A| = 2^5$ then $|A \cap L_2| = 4$ and so $k = 2$. But with $k = 2$ we have $|A_0| \leq 4$, so we conclude that, in fact, $|A| \leq 16$, and thus $|V/C_V(A)| \leq 64$. As $C_V(A) \neq C_V(a)$, by (1), it follows that $|Y| \leq 32$. By (11), we may choose $a_0 \in A_0 - \langle a\rangle$, and then (1) implies that $\langle a_0\rangle \times L_2$ acts faithfully on Y. But $2 \times L_2(4)$ has no faithful action on a 5-dimensional space over $\mathbb{F}_2$, so we conclude that Y_0 is not a spin module.

Suppose that $k = 2$. Then $L_1 = 1$, and the preceding paragraph applies. As m is odd, (13) and 9.4 imply that B contains an element b which acts as a transvection on U_2. As $k \neq 1$, $b \notin K_2^*$. Notice that either $K_1^* = A_0$ or K_1^* is dihedral of order 8. In either case we have $C_G(A_0) = A_0K_2^*$. Thus, there exists $c \in A_0$ so that $bc \in K_2^*$. But $[U_2, c] = 0$, so bc is a transvection on U_2, and then bc is a transposition in K_2^*. This is contrary to the minimality of k, so we now conclude that $k = 4$. If also $|A_0| = 4$ then (10) yields $|B| \leq 16$, $|A| \leq 64$, and $|V/C_V(A)| \leq 2^9$. Then also $|Y| \leq 32$, and we contradict (12). Thus $|A_0| = 8$. As $A_0 \leq O_2(K_1^*)$, by (7), it follows that $E^*A_0 = O_2(K_1^*)$, and since $[B, A_0] = 1$ we get $[L_1, B] \leq E$. Then $L_1 = 1$. As in the case $k = 2$, there then exists $b \in B$ such that b induces a transvection on U_2, and we have $b = xt$ where $x \in O_2(K_1^*)$ and t is a transposition in K_2^*. Then $a_0x \in E^*$ for some $a_0 \in A_0$. Then either a_0x or aa_0x is the product of fewer than three pairwise disjoint transpositions. Replacing a_0 by aa_0 if necessary, it follows that $a_0b = a_0xt$ is the product of fewer than four pairwise disjoint transpositions, and we again contradict the minimality of k. This completes the proof of 9.1. □

Section 10: Lie type groups in cross characteristic

10.1 Hypothesis. *Hypothesis $4'$ holds, and S is contained in a unique maximal subgroup of G. Further, $H/Z(H)$ is a quasisimple group of Lie type, whose defining characteristic r is different from p. Indeed, it is assumed that there exists no isomorphism between $H/Z(H)$ and a group of Lie type in characteristic p*

Our aim in this section is to prove the following result.

10.2 Theorem. *Assume Hypothesis 10.1. Then $|A| = 3$, and one of the following holds.*

(a) $G/Z(G) \cong L_2(5)$.
(b) $G \cong Sp(6,2)$, $C_G(A) \cong 3 \times Sp(4,2)$, *and* $|V| = 3^7$.

We remark that there is a natural embedding of $Sp(6,2)$ in $\Omega_7(3)$, which one obtains by identifying $2 \times Sp(6,2)$ with the Weyl group of E_7. Further, it is the case that in $Sp(6,2)$ a Sylow 3-subgroup is contained in a unique maximal subgroup (isomorphic to $Aut(U_4(2))$.

Whenever Hypothesis 10.1 is in effect we set $\overline{G} = G/Z(H)$. We begin the proof of 10.2 by considering the case where $\overline{H} \cong Sp(6,2)$.

10.3 Lemma. *Assume Hypothesis 10.1, and assume that $\overline{H} \cong Sp(6,2)$. Then $p = 3$ and one of the following holds.*

(i) $|A| = 3$, $G \cong Sp(6,2)$, $C_G(A) \cong 3 \times Sp(4,2)$, *and* $|V| = 3^7$.
(ii) $|A| = 27$, $|Z(G)| = 2$, *and* $|V| = 3^8$.

Proof. We have $G = H$ and $|Z(G)| \leq 2$. Let U be the natural $\mathbb{F}_2$-module for $\overline{G}$. There are three conjugacy classes of subgroups of order 3 in G, which are distinguished by the dimensions of the commutators $[U,X]$, X a representive of the class. We will say that a subgroup (or element) X of order 3 is in the class $3A$ (resp. $3B$, resp. $3C$) if $dim([U,X]) = 1$ (resp. 2, resp. 3). There is a subgroup M of G with $\overline{M} \cong L_2(8) : 3 \cong {}^2G_2(3)$, and M contains representatives of the classes $3C$ (in $[M,M]$) and $3B$ (in $M - [M,M]$).

Suppose first that $|A| = 3$, so that $|V/C_V(A)| \leq 9$. By 5.6, A is not quadratic on V, and so $|V/C_V(A)| = 9$. Then $A \not\leq M$, as follows from 6.9. Thus, A is of type $3A$. Then there is a maximal subgroup K^* of G containing A, with $\overline{K}^* \cong Sym(8)$, and such that $\overline{A}$ is generated by a 3-cycle in $\overline{K}^*$. Let K be a subgroup of K^* containing A, with $\overline{K} \cong Alt(7)$. Then 8.3 implies that $K \cong Alt(7)$ and that $[V,K]$ is a natural module for K, of dimension 6 over $\mathbb{F}_3$. In particular, we now have $Z(G) = 1$. Let K_0 be a subgroup of K containing A, with $K_0 \cong Alt(6)$, and let b be an element of of order 3 in $C_G(K_0)$. By [C2, Theorem 4.2], $[K^*,K^*]$ is the unique proper subgroup of G which properly contains K and which is generated by conjugates of A. Since $\langle b \rangle$ is conjugate to A we then have $\langle K, b \rangle = G$. We may then assume that $K^b \not\leq K^*$, and so also $G = \langle K, K^b \rangle$. Here b centralizes $[V,K_0]$, which has codimension 1 in $[V,K]$, so we get $V = [V,K] + [V,K^b]$ of dimension at most 7. But $Sp(6,2)$ has no faithful representation on degree 6 over $\mathbb{F}_3$, by [SZ], so $dim(V) = 7$. Thus, (i) holds in this case.

We next consider the various conjugacy classes of subgroups of $\overline{G}$ of order 9. Any such class is characterized by the conjugacy classes of its four cyclic subgroups, and in this way we find that there are exactly four such classes, which we list as follows, and where we list also a subgroup of $\overline{G}$ containing a representative of the given class.

$Y_1 = (3A, 3A, 3B, 3B) \leq Alt(7)$,

$Y_2 = (3C, 3B, 3B, 3B) \leq L_2(8) : 3$,

$Y_3 = (3A, 3B, 3C, 3C) \leq Sym(3) \times Sym(6)$,

$Y_4 = (3C, 3C, 3C, 3C) \leq 3^{1+2} : GL(2, 3)$.

Suppose that $|A| = 9$, so that $|V/C_V(A)| \leq 3^4$. Then A is not of type Y_1, by 8.3, and A is not of type Y_2 by 6.9. Thus A is of type Y_3 or Y_4, and so A contains a subgroup $\langle a \rangle$ of type $3C$. Set $K = C_G(a)$, and observe that $\overline{K} \cong 3^{1+2} : SL(2, 3)$. Theorem 1.3 of [C3] implies that any quadratic element of order 3 in G is of type $3A$, so a is not quadratic. Set $W = [V, a]$. Then $dim(W) \leq 4$, and $[W, a] \neq 0$, so K acts faithfully on W. It follows that $dim(W) = 4$, and then $C_V(a) = C_V(A)$. As $\langle A^K \rangle \geq O_3(K)$ we then have $C_W(a) = C_W(O_3(K))$. Also, by Hypothesis 4$'$ we have $[W, A, A] = 0$, so $[W, A, O_3(K)] = 0$, and then $O_3(K)$ acts quadratically on W, contrary to $\Phi(O_3(K)) \neq 1$. We therefore conclude that $|A| \neq 9$.

Suppose finally that $|A| = 27$. Let Y be a subgroup of A of type Y_2. Then two conjugates of Y suffice to generate a maximal subgroup M of G with $M \cong L_2(8) : 3$, and since $A \not\leq M$ it follows that two conjugates of A suffice to generate G. As $dim(V/C_V(A)) \leq 6$ we then have $dim(V) \leq 12$. Let $A \leq L \leq G$ with $\overline{L} \cong Sym(3) \times Sym(6)$, set $L_0 = E(L)$, set $A_0 = C_A(L_0)$, and set $V_0 = [V, A_0] + C_V(A_0)$. Then $A \cap L_0$ acts quadratically on V_0, by Hypothesis 4$'$, and so 1.7 implies that $[V_0, L_0]$ is a direct sum of natural $SL(2, 9)$-modules for L_0. As $V/C_V(A_0) \cong [V, A_0]$ as L_0-modules, we have $[V_0, L_0] \neq 0$, so we conclude that $Z(L_0) = Z(G) \neq 1$. We may assume that V is irreducible for G, so $V = [V, Z(G)]$, and since $dim(V) \leq 12$, V_0 is a direct sum of one or two natural modules for L_0. Then also V/V_0 is a natural module for L_0. If A_0 is not quadratic on V we then have $dim(V) = 12$ and $|C_V(A)| = |C_{V_0}(A)| = 3^4$, so that $|V/C_V(A)| > |A|^2$. Thus, A_0 is quadratic on V, and $dim(V) = 8$. Thus, (ii) holds in this case.

□

The following lemma is given by Table I in [SZ].

10.4 Lemma. *Let X be a simple group of Lie type, in characteristic different from p, and let V be a non-trivial projective $\mathbb{F}_p X$-module. Assume that X is not isomorphic to any of the groups in the following list $\mathcal{L}_0$.*

$$\mathcal{L}_0 = \{L_2(4),\ L_2(9),\ L_3(2),\ L_3(4),\ L_4(2)\ L_4(3),\ PSp(4,2),\ U_4(3),\ P\Omega_8^+(2),\ P\Omega_7(3),\ F_4(2),\ G_2(3),\ G_2(4),\ Sz(8)\}$$

Then the dimension of V is at least ℓ, where ℓ is given as follows.

(1) $L_2(q)$*:* $\ell = (1/d)(q-1)$, $d = (2, q-1)$.

(2) $L_n(q)$, $n \geq 3$*:* $\ell = (q^n - 1)/(q-1) - n$.

(3) $PSp(2n, q)$, $n \geq 2$*:*

$$\ell = \begin{cases} (q^n-1)/2 & \textit{if } q \textit{ is odd, and} \\ q(q^n-1)(q^{n-1}-1)/2(q+1) & \textit{if } q \textit{ is even.} \end{cases}$$

(4) $U_n(q)$, $n \geq 3$*:*

$$\ell = \begin{cases} q(q^{n-1}-1)/(q+1) & \textit{if } n \textit{ is odd, and} \\ (q^n-1)/(q+1) & \textit{if } n \textit{ is even.} \end{cases}$$

(5) $P\Omega_{2n+1}(q)$, *q odd,* $n \geq 3$*:*

$$\ell = \begin{cases} (q^{2n}-1)/(q^2-1) - n & \textit{if } q \neq 3, \textit{ and} \\ (3^{2n}-1)/8 - (3^n-1)/2 & \textit{if } q = 3. \end{cases}$$

(6) $P\Omega_{2n}^+(q)$, $n \geq 4$*:*

$$\ell = \begin{cases} q(q^{2n-2}-1)/(q^2-1) + q^{n-1} - n & \textit{if } q \neq 2, 3, \textit{ and} \\ q(q^{2n-2}-1)/(q^2-1) - (q^{n-1}-1)/(q-1) - 7\delta_{2,p} & \textit{if } q \textit{ is even.} \end{cases}$$

(7) $P\Omega_{2n}^-(q)$, $n \geq 4$*:* $\ell = q(q^{2n-2}-1)/(q^2-1) - q^{n-1} - n + 2$.

(8) $E_6(q)$*:* $\ell = q^9(q^2-1)$.

(9) $E_7(q)$*:* $\ell = q^{15}(q^2-1)$.

(10) $E_8(q)$*:* $\ell = q^{27}(q^2-1)$.

(11) $F_4(q)$*:* $\ell = q^6(q^2-1)$.

(12) ${}^2E_6(q)$*:* $\ell = q^9(q^2-1)$.

(13) $G_2(q)$*:* $\ell = q(q^2-1)$.

(14) ${}^3D_4(q)$*:* $\ell = q^3(q^2-1)$.

(15) ${}^2F_4(q)$*:* $\ell = (\sqrt{q/2})q^4(q-1)$.

(16) $Sz(q)$*:* $\ell = (\sqrt{q/2})(q-1)$.

(17) ${}^2G_2(q)$*:* $\ell = q(q-1)$. □

We insert the following lemma, as support for the case where $H \cong L_2(q)$.

10.5 Lemma. *Set $L = L_2(q)$, q odd, and identify L with the group $Inn(L)$ of inner automorphisms of L. Let A be an elementary abelian 2-subgroup of $Aut(L)$. Then one of the following holds.*

(i) *q is a perfect square, $A \nleq L$, and there exists an element t of $A - L$ such that t is conjugate via $Aut(L)$ to a field automorphism of L. Further, we have $A = (A \cap L)\langle t\rangle$ and $|A| \leq 8$.*

(ii) *$A \nleq L$, and $LA = L\langle d\rangle$, where d is a diagonal automorphism of L. Here $|A/(A \cap L)| = 2$, $|A| \leq 4$, and all involutions in $LA - L$ are conjugate. If $|A| = 4$ then $LA = \langle A, A^g\rangle$ for some $g \in L$.*

(iii) *$A \leq L$, $|A| \leq 4$, and if $|A| = 4$ then $LA = \langle A, A^g\rangle$ for some $g \in L$.*

Proof. Set $G = LA$, and let T be a Sylow 2-subgroup of G containing A. Also, set $G_1 = PGL(2, q)$, and set $G^* = G_1T$. Further let T^* be a Sylow 2-subgroup of G^* containing T and set $T_1 = T^* \cap G_1$.

We first note the following.

(1) T_1 is dihedral, and G_1 has exactly two classes of involutions.

Suppose that $q = r^2$ is a perfect square, and let α be the standard field automorphism of L of order 2, induced by the automorphism of $GL(2, q)$ which raises matrix entries to the power r (and which we denote also by α). Our first step will be to provide a proof of the following (well known) fact.

(2) We have $C_{G_1}(\alpha) = C_L(\alpha) \cong PGL(2, r)$.

The proof is as follows. Set $\widetilde{G}_1 = GL(2, q)$, let Z be the group of scalar matrices in $\widetilde{G}_1$, and set $Z_0 = \{\lambda^{q-1}I \parallel \lambda \in \mathbb{F}_q\}$. Denote by $\widetilde{C}_1$ the set of matrices $\widetilde{x} \in \widetilde{G}_1$ such that $[\widetilde{x}, \alpha] \in Z$. As $Z \leq Z(\widetilde{C}_1)$, there is a homomorphism $\phi : \widetilde{C}_1 \longrightarrow Z$ given by $\phi(\widetilde{x}) = [\widetilde{x}, \alpha]$. Then the image of *phi* is Z_0, and the kernel of ϕ is $C_{\widetilde{G}_1}(\alpha) = GL(2, r)$. One observes that $\phi|_Z$ maps Z onto Z_0, so $\widetilde{C}_1 = Ker(\phi)Z$. We then have

$$C_{G_1}(\alpha) = Ker(\phi)Z/Z \cong Ker(\phi)/(Ker(\phi) \cap Z) \cong PGL(2, r).$$

On the other hand, let $\omega \in \mathbb{F}_q - \mathbb{F}_r$ so that $\langle\omega\rangle = \mathbb{F}_r^\times$, and let d be the linear fractional transformation $x \mapsto \omega^2 x$. Then $\omega^r = -\omega$, and so $[d, \alpha] = 1$. Also, $d \in L$, and d induces an outer automorphism on the subgroup $PSL(2, r)$ of L. Thus $C_L(\alpha)$ contains a subgroup isomorphic to $PGL(2, r)$, and this yields (2).

Next, suppose that there exists an element $t \in A - G_1$. As $|t| = 2$ we have $g^\alpha = g^{-1}$, and then t is conjugate either to α or to $z\alpha$, where z is an involution in $C_{G_1}(\alpha)$. Suppose that t is not conjugate to α. Then $z \in L$, by (2). We now apply (1) to $C_L(t)$ in place of G_1, and find that, up to conjugation in L, there are two choices for z. One (in $L_2(r)$) is given by the linear fractional transformation $z_1 : x \mapsto -1/x^{-1}$, and the other (in $C_L(\alpha) - L_2(r)$) is given by $z_2 : x \mapsto -\omega^2 x$, where ω is as above. To show that α and $z_i\alpha$ are conjugate, we suffices to display elements g_i of G_1 such that $g_i^\alpha = g_i z_i$. Let $\rho \in \mathbb{F}_q$ with $\rho^{1+r} = -1$. The transformations $g_1 : x \mapsto (x + \rho^r)/(\rho x + \rho^{2r})$ and $g_2 : x \mapsto (x - \omega)/(\omega x + \omega^2)$ perform this trick, as the careful reader may check. Thus (i) holds if $A \not\leq G_1$.

Suppose next that $A \leq G_1$, suppose that $A \not\leq L$, and let $t \in A - L$. As T_1 is dihedral, we have $|C_T(t)| = 2$, and thus $|A| \leq 4$. Let s be the involution in $C_T(t)$, and set $D = C_L(s)$. Then D is dihedral of order $q - \epsilon$, $\epsilon = 1$ or -1, and where $q \cong \epsilon (mod\ 4)$. Further, $D\langle t\rangle$ is dihedral, and so $C_D(t) = \langle s\rangle$. It follows that $C_L(t)$ is dihedral, of twice-odd order. Now let D_1 be a dihedral subgroup of L, containing s, of order $q+\epsilon$. Suppose that D_1^x is t-invariant, for every $x \in C_L(s)$. Then $[D, t] \leq N_L(D_1)$. As D_1 is maximal in L, and $|D \cap D_1| = 2$, we conclude that $[D, t] = \langle s\rangle$, $|D| = 4$, and $q = 5$. In this case we have $G_1 \cong Sym(5)$, and one checks that two conjugates of $\langle(1\ 2), (3\ 4)\rangle$ suffice to generate $Sym(5)$. On the other hand, suppose that there exists $x \in C_L(s)$ such that D_1^x is not t-invariant. We may then take $x = 1$, and we conclude that $G = \langle s, t, s^g, t^g\rangle$, where g is a generator for the maximal cyclic subgroup of D_1. Thus (ii) holds in this case.

Finally, suppose that $A \leq L$, and that $|A| > 2$. Then A is a fours group. Let s be an involution in A, and let D be a dihedral subgroup of L containing s, of twice-odd order $q - 1$ or $q + 1$. Then D is maximal, so D is not A-invariant, and so $G = L = \langle A, A^g\rangle$ for any generator g of $[D, D]$. Thus, (iii) holds in this case, and the lemma is proved. □

10.6 Lemma. *Assume Hypothesis 10.1, and suppose that $H/Z(H) \cong L_2(q)$, q a power of r. Then $q = 5$, $r = 3$, and $|V| = 81$.*

Proof. First of all, if $|Z(H)| > 2$ then $|Z(H)|$ is divisible by 3, and $H/Z(H) \cong L_2(9)$. Then $p = 2$ or 5, and since $L_2(9) \cong (Sp(4, 2))'$ we have $p = 5$. Then $|A| = 5$ and H is generated by two conjugates of A, so that $|V| \leq 5^4$. As 3 divides $|Z(H)|$, V may then be regarded as a 2-dimensional space over $\mathbb{F}_{25}$. But $L_2(9)$ is not a subgroup of $L_2(25)$, so we conclude that $|Z(H)| \leq 2$.

Suppose that G contains a quadratic subgroup of order at least 3. If p is odd then 3.1 yields $H \cong SL(,2,5)$, $p = 3$, and V is a natural $SL(2,9)$-module for H. Thus, the lemma holds in this case. If $p = 2$ then the main result of [MS1] implies that $H/Z(H) \cong U_4(3)$, contrary to $H/Z(H) \cong L_2(q)$. Thus, we may assume henceforth that any quadratic subgroup of G has order at most 2.

Suppose first that $p = 2$. Then q is odd, and since $H/Z(H)$ is not isomorphic to a group of Lie type in characteristic 2 we have $q \geq 11$. By 5.4 we have $|V/C_V(a)| \geq 8$ for any $a \in A^\#$. Also, $|A|^{3/2} \geq |V/C_V(A)|$ by Hypothesis 4′, and so $|A| \neq 2$. If $|A| = 4$ we have $|V/C_V(A)| \leq 8$, and then $C_V(a) = C_V(A)$ for all $a \in A^\#$, and A is a quadratic fours group. Thus $|A| \neq 4$. Then 10.5 implies that $|A| = 8$, $|A \cap H| = 4$, and there exists $a \in A - H$ such that a induces a field automorphism on $H/Z(H)$. Further, if we apply 10.5 to $A \cap H$ then we find that H is generated by two conjugates of $A \cap H$. Here $|V/C_V(A)| \leq 16$, so $dim(V) \leq 8$. But $dim(V) \geq (q - 1)/2$, by 10.4(1), and so $q \leq 17$. As q is odd and a perfect square we then have $q = 9$, and thus $H/Z(H) \cong (Sp(4, 2))'$. We therefore conclude that p is odd.

Suppose that $|A| = p$, so that $|V/C_V(A)| \leq p^2$. Suppose also that $A \leq H$. The group $L_2(r)$ is a homomorphic image of $L_2(\mathbb{Z})$, and $L_2(\mathbb{Z})$ contains the free product $\mathbb{Z}_3 * \mathbb{Z}_3$ as a subgroup of index 2, so $L_2(r)$ is generated by two elements of order 3. Thus, if $p = 3$ then two conjugates of A generate a subgroup Y of H with $Y/Z(Y) \cong L_2(r)$, and 2.2 then yields $r = 5$. Then in any case, we may choose a conjugate B of A so that $\langle A, B\rangle$ is nonsolvable, and then $\langle A, B\rangle$ is quasisimple. By 2.2 we then have $p \geq 5$ (resp. $p = 3$), $\langle A, B\rangle \cong L_2(p)$ (resp. $L_2(5)$), and $|[V, \langle A, B\rangle]| = p^3$ (resp. 81). Any quasisimple subgroup of $H/Z(H)$ is isomorphic to $L_2(5)$ or $L_2(q_1)$ for some power q_1 of r, so we have $p = 3$ or 5 at this point. If $p = 3$ and $q = 5$ we have the conclusion of the lemma. Assuming that the lemma is false, choose a conjugate C of A, not contained in $\langle A, B\rangle$, so that $\langle A, C\rangle$ is quasisimple, and set $X = \langle A, B, C\rangle$. Then $|[V, X]| \leq p^4$ (resp. 3^6), and $X/Z(X) \cong L_2(q_1)$ for some power q_1 of r (with $q_1 \geq 25$ if $p = 3$). Then $q_1 > 5$. If $q_1 = 7$ then $p = 3$ and X contains a Frobenius group of order 21, which is contrary to 4.2. If $q_1 = 9$ then $p = 5$ and we may choose B so that $\langle A, B\rangle = X$, which is contrary to 2.2. Thus $q \geq 11$. If $p = 5$ then $dim([V, X]) \leq 4$, and 10.4(1) yields $q \leq 9$. So in fact $p = 3$, $dim([V, X]) \leq 6$, and 10.4(1) yields $q \leq 13$. But we have seen that $q_1 \geq 25$ if $p = 3$, so we have a contradiction at this point. Thus, $A \nleq H$.

Let $a \in A - H$. By Theorem 4.9.1 of [GLS3], a induces a field automorphism on H, and thus A normalizes a Sylow r-subgroup R of H. Then also $[R, A]$ is non-cyclic. Suppose that $|A| = p$. Then 2.1 implies that $p = 3$ and that $|[R, A]| = 4$. It follows that $q = 8$ and that $HA \cong {}^2G_2(3)$, contrary to $H \notin Lie(p)$. We therefore conclude that $|A| = p^2$. Set $X = C_H(a)$. Then $X/Z(H) \cong L_2(q_0)$ where $(q_0)^p = q$. Hypothesis $4'$ implies that $A \cap X$ acts quadratically on the subspace $W = [V, a] + C_V(a)$ of V, and since $V/C_V(a)$ is X-isomorphic to $[V, a]$ it follows that X acts non-trivially on W. Then 5.6 yields $p = 3$ and $X \cong SL(2, 5)$, so that $q = 5^3$. Evidently, three conjugates of A suffice to generate HA, so $dim(V) \leq 12$. But 10.4(1) yields $dim(V) \geq 62$, so we have a final contradiction, and the lemma is proved. □

In the following lemma we shall eliminate from consideration a further number of “small” groups, including groups having exceptional Schur multipliers, and the groups in the list $\mathcal{L}_0$ from 10.4. Conspicuously missing from this expanded list are any of the groups $PSp(4, q)$. These will be addressed later, in 10.10.

10.7 Lemma. *Assume Hypothesis 10.1, and let $\mathcal{L}$ be the set of groups whose members* *are as follows:*

$L_3(q)$, $3 \leq q \leq 5$,

$L_n(q)$, *with* $n = 4$ *or* 5, *and with* $n + q \leq 7$,

$U_3(q)$, $q \leq 7$,

$U_4(q)$, $q \leq 3$,

$U_n(2)$, $n \leq 7$,

$PSp(2n, q)$, *with* $n = 3$ *or* 4, *and with* $q \leq 3$,

$\Omega_7(3)$, $\Omega_8^+(2)$, $\Omega_8^-(2)$, *and* ${}^3D_4(2)$

${}^2E_6(2)$, $F_4(2)$, ${}^2F_4(2)$, $G_2(3)$, $G_2(4)$, *and* $Sz(8)$.

Assume that $\overline{H}$ *is isomorphic to a group in the list* $\mathcal{L}$. *Then* $\overline{H} \cong Sp(6, 2)$.

Proof. Assume that $\overline{H}$ is not isomorphic to $Sp(6, 2)$. We shall consider the various groups individually, and we shall make free use of the ATLAS, in deciding whether a Sylow p-subgroup of a particular group G is contained in a unique maximal subgroup of G. This task will be simplified by the following reduction.

(a) Set $H^* = HS$. Then there exists at most one maximal subgroup of $\overline{H}^*$ containing $\overline{S}$, and at most one $\overline{H}$-invariant maximal subgroup of $\overline{S}$.

Indeed, if (a) is false then the unique maximal subgroup M of G containing S contains H. But M contains also $N_G(S \cap H)$, and the Frattini argument then yields $M = G$.

We may also employ the following consequence of 2.2.

(b) A Sylow p-subgroup of G has order greater than p.

Most groups in $\mathcal{L}$, and most primes, may be eliminated at once by recourse to (a) and (b). The only exceptions will be given by the groups $L_3(4)$ and ${}^3D_4(2)$ with $p = 3$, and the groups $L_3(3)$ and $L_4(3)$ with $p = 2$. Apart from the treatment of these four exceptions, the argument will consist simply of a list, in which we give the isomorphism type of $\overline{H}$, the order of $\overline{H}$ and of $Out(\overline{H})$, and then, for each prime p different from r, and for which p^2 divides the order of $Aut(\overline{H})$, a pair of distinct maximal subgroups of $\overline{H}^* = \overline{HS}$ containing $\overline{S}$.

(1) $\overline{H} \cong L_3(3)$, $|\overline{H}| = 2^4 \cdot 3^3 \cdot 13$, $|Out(\overline{H})| = 2$, $(p = 2)$.
There is a unique maximal subgroup containing S if $S \not\leq H$. This case will be treated below.

(2) $\overline{H} \cong L_3(4)$, $|\overline{H}| = 2^6 \cdot 3^2 \cdot 5 \cdot 7$, $|Out(\overline{H})| = 12$, $(p = 3)$.

There is a unique maximal subgroup of $\overline{H}^*$ containing $\overline{S}$ if $S \not\leq H$, so this case will be considered separately below.
Maximal subgroups when $S \leq H$:

$$M_{10}, \qquad U_3(2).$$

(3) $\overline{H} \cong L_3(5)$, $|\overline{H}| = 2^5 \cdot 3 \cdot 5^3 \cdot 31$, $|Out(H)| = 2$, $(p = 2)$.
Maximal subgroups when $S \leq H$:

$$5^2 : GL(2,5), \qquad 4^2 : Sym(3).$$

Maximal subgroups when $S \not\leq H$:

$$GL(2,5).2, \qquad 4^2.(Sym(3) \times 2).$$

(4) $\overline{H} \cong L_4(2)$, $|\overline{H}| = 2^6 \cdot 3^2 \cdot 5 \cdot 7$, $|Out(H)| = 2$, $(p = 3)$.
Maximal subgroups:

$$Alt(7), \qquad 2^4 : (Sym(3) \times Sym(3)).$$

(5) $\overline{H} \cong L_4(3)$, $|\overline{H}| = 2^7 \cdot 3^6 \cdot 5 \cdot 13$, $|Out(\overline{H})| = 4$, $(p = 2)$.
There may be a unique maximal subgroup of $\overline{H}^*$ containing $\overline{S}$, if $S \not\leq H$. This will be treated below.

(6) $\overline{H} \cong L_5(2)$, $|\overline{H}| = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$, $|Out(\overline{H})| = 2$, $(p = 3)$.
Maximal subgroups:

$$2^4 : L_4(2), \qquad 2^6 : (L_3(2) \times L_2(2)).$$

(7) $\overline{H} \cong U_3(3) \cong (G_2(2))'$, $|\overline{H}| = 2^5 \cdot 3^3 \cdot 7$, $|Out(\overline{H})| = 2$, cyclic Sylow subgroups in cross characteristic.

(8) $\overline{H} \cong U_3(4)$, $|\overline{H}| = 2^6 \cdot 3 \cdot 5^2 \cdot 13$, $|Out(\overline{H})| = 2$, $(p = 5)$.
Two maximal subgroups $GU(2,4)$.

(9) $\overline{H} \cong U_3(5)$, $|\overline{H}| = 2^4 \cdot 3^2 \cdot 5^4 \cdot 7$, $|Out(\overline{H})| = 6$, $(p = 2$ or $3)$.
Maximal subgroups for $p = 3$, with $S \leq H$:

$$Alt(7), \qquad M_{10}.$$

Maximal subgroups of $\overline{H}^*$, for $p = 3$, with $S \not\leq H$:

$$6^2 : Sym(3), \qquad 3^2 : SL(2,3).$$

$\overline{S}$-invariant maximal subgroups of $\overline{H}$, for $p = 2$:

$$M_{10}, \qquad 2.Sym(5).$$

(10) $\overline{H} \cong U_4(2) \cong PSp(4,3)$, $|\overline{H}| = 2^6 \cdot 3^4 \cdot 5$, $|Out(\overline{H})| = 2$, cyclic Sylow subgroups in cross characteristic.

(11) $\overline{H} \cong U_4(3)$, $|\overline{H}| = 2^7 \cdot 3^6 \cdot 5 \cdot 7$, $|Out(\overline{H})| = 8$, $(p = 2)$.
In this case, the existence of a pair of proper subgoups of G, containing S, and generating G, is evident from the $\tilde{B}_2$ geometry of 2-local subgroups of $\overline{G}$. See [K].

(12) $\overline{H} \cong U_5(2)$, $|\overline{H}| = 2^{10} \cdot 3^5 \cdot 5 \cdot 11$, $|Out(\overline{H})| = 2$, $(p = 3)$.
Maximal subgroups of $\overline{H}$ containing $\overline{S}$:

$$Sym(3) \times GU(3,2), \qquad GU(4,2).$$

(13) $\overline{H} \cong U_6(2)$, $|\overline{H}| = 2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$, $|Out(\overline{H})| = 6$, $(p = 3)$.
Maximal subgroups of $\overline{H}$ containing $\overline{S}$, if $\overline{S} \leq \overline{H}$:

$$3^{1+4}.[2^7.3], \qquad U_4(3) : 2.$$

Maximal subgroups of $\overline{H}^*$ containing $\overline{S}$, if $\overline{S} \not\leq \overline{H}$.

$$3^{1+4}.[2^7.3], \qquad 3^5 : Sym(6).$$

(14) $\overline{H} \cong U_7(2)$, $|\overline{H}| = 2^{21} \cdot 3^8 \cdot 5 \cdot 7 \cdot 11 \cdot 43$, $|Out(\overline{H})| = 2$, $(p = 3)$.
Subgroups of $\overline{H}$ containing $\overline{S}$ and which generate $\overline{H}$:

$$GU(6,2), \qquad U_4(2) \times GU(3,2).$$

(16) $\overline{H} \cong PSp(6,3)$, $|\overline{H}| = 2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$, $|Out(\overline{H})| = 2$, $(p = 2)$.
Maximal subgroups of $\overline{H}$ invariant under $\overline{S}$:

$$2(Alt(4) \times U_4(2)), \qquad 2^{2+6} : 3^3 : Sym(3).$$

(19) $\overline{H} \cong Sp(8,2)$, $|\overline{H}| = 2^{16} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17$, $|Out(\overline{H})| = 1$, $(p = 3$ or $5)$.
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 5$:

$$D_4(2), \qquad Sp(4,4) : 2.$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p=3$:

$$D_4(2), \qquad Sym(3)\times Sp(6,2).$$

(20) $\overline{H}\cong PSp(8,3)$, $|\overline{H}|=2^{14}\cdot 3^{16}\cdot 5^2\cdot 7\cdot 13\cdot 41$, $|Out(\overline{H})|=2$, ($p=2$ or 5).
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p=5$:

$$(Sp(4,3)\circ Sp(4,3))2, \qquad PSp(4,9):2.$$

Maximal subgroups of $\overline{H}$ invariant under $\overline{S}$ if $p=2$:

$$(Sp(4,3)\circ Sp(4,3))2, \qquad \overline{M},$$

where $\overline{M}$ is the image in $\overline{H}$ of a subgroup of $Sp(8,3)$ of the form $SL(2,3)\wr Sym(4)$.

(21) $\overline{H}\cong \Omega_7(3)$, $|\overline{H}|=2^9\cdot 3^9\cdot 5\cdot 7\cdot 13$, $|Out(\overline{H})|=2$, ($p=2$).
Maximal subgroups of $\overline{H}$ invariant under $\overline{S}$:

$$2U_4(3):2, \qquad 2^6:Alt(7).$$

(22) $\overline{H}\cong \Omega_8^+(2)$, $|\overline{H}|=2^{12}\cdot 3^5\cdot 5^2\cdot 7$, $|Out(\overline{H})|=6$, ($p=3$ or 5).
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p=5$:

$$(Alt(5)\times Alt(5)):2^2 \quad \text{in three different ways.}$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p=3$ and $S\leq H$:

$$(3\times U_4(2)):2, \qquad 3^4:2^3.Sym(4).$$

Maximal subgroups of $\overline{H}^*$ containing $\overline{S}$ if $p=3$ and $S\not\leq H$:

$$3^{1+4}_+:GL(2,3), \qquad (3^4:2^3.Sym(4)).3.$$

(23) $\overline{H}\cong \Omega_8^-(2)$, $|\overline{H}|=2^{12}\cdot 3^4\cdot 5\cdot 7\cdot 17$, $|Out(\overline{H})|=2$, ($p=3$).
Maximal subgroups of $\overline{H}$ containing $\overline{S}$:

$$2^6:U_4(2), \qquad Sp(6,2).$$

(24) $\overline{H}\cong {}^3D_4(2)$, $|\overline{H}|=2^{12}\cdot 3^4\cdot 7^2\cdot 13$, $|Out(\overline{H})|=3$, ($p=3$ or 7).
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p=7$:

$$(7\times L_3(2)):2, \qquad 7^2:SL(2,3).$$

There is a unique maximal subgroup of $\overline{H}^*$ containing $\overline{S}$ if $p = 3$. This case will be treated below.

(25) $\overline{H} \cong G_2(3)$, $|\overline{H}| = 2^6 \cdot 3^6 \cdot 7 \cdot 13$, $|Out(\overline{H})| = 2$, $(p = 2)$.
Maximal subgroups of $\overline{H}$ invariant under $\overline{S}$:

$$(2^3)L_3(2), \qquad 2_+^{1+4} : 3^2.2.$$

(26) $\overline{H} \cong G_2(4)$, $|\overline{H}| = 2^{12} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$, $|Out(\overline{H})| = 2$, $(p = 3$ or $5)$.
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 5$:

$$U_3(4) : 2, \qquad Alt(5) \times Alt(5).$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 3$:

$$SL(3, 4) : 2, \qquad J_2.$$

(27) $\overline{H} \cong F_4(2)$, $|\overline{H}| = 2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17$, $|Out(\overline{H})| = 2$, $(p = 3$, 5, or $7)$.
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 7$:

$$^3D_4(2), \quad \text{in two different ways.}$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 5$:

$$^2F_4(2), \qquad Sp(8, 2).$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 3$:

$$Aut(D_4(2)), \qquad L_4(3) : 2.$$

(28) $\overline{H} \cong (^2F_4(2))'$, $|\overline{H}| = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$, $|Out(\overline{H})| = 2$, $(p = 3$ or $5)$.
Maximal subgroups containing $\overline{S}$ if $p = 5$:

$$L_2(25), \qquad 5^2 : 4Alt(4).$$

Maximal subgroups containing $\overline{S}$ if $p = 3$:

$$L_3(3) : 2 \quad \text{in two different ways.}$$

(29) $\overline{H} \cong Sz(8)$, $|\overline{H}| = 2^6 \cdot 5 \cdot 7 \cdot 13$, $|Out(\overline{H})| = 3$. This case contradicts (2).

(30) $\overline{H} \cong {}^2E_6(2)$, $|\overline{H}| = 2^{36} \cdot 3^9 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$, $|Out(\overline{H})| = 6$, ($p = 3$, 5, or 7).
Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 7$:

$$F_4(2), \quad \text{in three different ways.}$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 5$:

$$F_4(2), \quad \text{in three different ways.}$$

Maximal subgroups of $\overline{H}$ containing $\overline{S}$ if $p = 3$ and $S \leq H$:

$$Fi_{22} \quad \text{in three different ways.}$$

Maximal subgroups of $\overline{H}^*$ containing $\overline{S}$ if $p = 3$ and $S \not\leq H$.

$$3^6 : U_4(2) : 2, \qquad 3^{1+6}.2^{3+6}.(Sym(3) \times 3).3.$$

It now remains to take up the four exceptional cases: $\overline{H} \cong L_3(4)$, ${}^3D_4(2)$, $L_3(3)$, and $L_3(4)$.

Suppose first that $\overline{H} \cong L_3(4)$, of order $2^6 \cdot 3^2 \cdot 5 \cdot 7$. Then $p = 3$, by (2). Then $Z(H)$ is a 2-group, the 3-rank of G is 2, and so $|A| \leq 9$. We claim that four conjugates of A suffice to generate HA if $|A| = 3$, and that three conjugates suffice if $|A| = 9$. Indeed, suppose that $A \cap H \neq 1$, and let $1 \neq a \in A \cap H$. Then two conjugates of a generate a subgroup K of H with $Z(H)K/Z(H) \cong L_3(2)$, and $A \cap K$ is a Sylow 3-subgroup of $N_G(K)$. Here $Z(H)K$ is maximal in H, so the claim holds in this case. On the other hand, suppose that $A \cap H = 1$, and set $X = C_H(A)$. Referring to the ATLAS, we find that $Z(H)X/Z(H) \cong SL(2,4)$ or $Fr(21)$. Let B be a Sylow 3-subgroup of $C_G(A)$. Then A is conjugate to every cyclic subgroup of B not contained in X, and so there are conjugates A_1 and A_2 of A such that $Z(H)\langle A_1, A_2\rangle = Z(H)XA$. It is left to the reader to demonstrate that two conjugates of XA suffice to generate HA (or to find a different argument) and thus to prove the claim. We conclude that $|V| \leq 3^8$.

If $S \leq H$ then there are two different maximal subgroups M_1 and M_2 of H containing S (with $\overline{M}_1 \cong U_3(2)$ and with $\overline{M}_2 \cong M_{10}$), contrary to (1). Thus $S \not\leq H$. There then exists a subgroup Y of G with $Y \cong Fr(21) \times 3$. Let b be a non-identity element of $O_3(Y)$ and x a non-identity element of $O_7(Y)$. Then $dim([V, x]) = 6$, and $[V, x, b] = 0$, so $|V/C_V(b)| \leq 9$. But, as we have seen, b is conjugate to an element of Y not contained in $\langle b\rangle$, and in this way we violate 2.2. Thus, $H/Z(H) \not\cong L_3(4)$.

Suppose next that $\overline{H} \cong {}^3D_4(2)$ and that $p = 3$. It so happens that $Z(H) = 1$, so $\overline{G} = G$. There are exactly two classes of elements of order 3 in H. To be consistent with ATLAS notation, we label a pair of fixed representatives of these two classes by $3A$ and

$3B$, where $N_H(3A) \cong Sym(3) \times L_2(8)$, and where $N_H(3B)$ is of the form $3^{1+2}_+)GL(2,3)$. Set $L = E(C_H(3A))$. We may assume that $[3A, 3B] = 1$, and then $3B \in E(C_H(3A))$ since $3A$ is not contained in a cyclic group of order 9. Let t be an involution in $N_H(3A)$ with $[t, L] = 1$. Then $C_H(t)$ is a maximal parabolic subgroup of H, of the form $2^{1+8}_+ : L_2(8)$. As two conjugates of $3B$ suffice to generate L, it follows that three conjugates of $3B$ suffice to generate $C_H(t)$, and then four conjugates suffice to generate H. On the other hand, we observe that $3A$ is not central in a Sylow 3-subgroup of H, and hence $3A$ is not weakly closed in a Sylow 3- subgroup of $N_H(3A)$. Thus, there is a conjugate of $3A$ which is "diagonal" in $\langle 3A \rangle \times L$, and so $C_H(3A)$ is generated by two conjugates of $3A$. Then four conjugates of $3A$ suffice to generate a subgroup of H containing $C_H(t)$. As $C_H(t)$ contains no conjugate of $3A$, it follows that four conjugates of $3A$ suffice to generate H. Thus, we have shown that for any element $x \in H$ of order 3, four conjugates of x suffice to generate H.

No involution-centralizer in H contains a copy of $\mathbb{Z}_3 \times \mathbb{Z}_3$, and then it follows from the given structure of $N_H(3B)$ that the 3-rank of H is two, and the 3-rank of $Aut(H)$ is then at most three. In particular, we have $|A| \leq 27$, and so $|V/C_V(A)| \leq 3^6$. We now appeal to 10.4, where we find that $dim(V) \geq 24$. It follows that four conjugates of A do not suffice to generate HA, and therefore $A \cap H = 1$. Thus $|A| = 3$, $|V/C_V(A)| \leq 9$, and twelve conjugates of A do not suffice to generate HA. But A is not weakly closed in S, and therefore eight conjugates of A suffice to generate HA. Thus, we have a contradiction, and $H \ncong {}^3D_4(2)$.

Suppose next that $\overline{H} \cong L_3(3)$. Then $Z(G) = 1$, $|G/H| \leq 2$, and by (2) we have $p = 2$. A Sylow 2-subgroup of $Aut(H)$ is a direct product of a semidihedral with $\mathbb{Z}_2$, so the 2-rank of A is at most 3. By [MS1], G contains no quadratic fours groups, and then no element of A is a 2-transvection on V, by 5.6. Also, as A contains no quadratic fours group we have $C_V(a) \neq C_V(A)$ for any $a \in A^{\#}$. As $|A|^{3/2} \geq |V/C_V(A)|$, by Hypothesis $4'$, we conclude that $|A| = 8$, that $|V/C_V(A)| = 16$, and that $|V/C_V(a)| = 8$ for all $a \in A^{\#}$. Let $a \in A - H$. Then $C_H(a) \cong GL(2,3)$, and since $|[V,a]| = 8$ we have $[V, a, Z(C_H(a))] = 0$. Thus A contains a quadratic fours group, and we have a contradiction in this case.

Finally, suppose that $\overline{H} \cong L_4(3)$. Then $p = 2$, as seen in (5). As $Z(H)$ is a 2-group, we then have $Z(H) = 1$ and $H \cong L_4(4)$. A Sylow 2 subgroup of $Aut(H)$ is contained in a unique maximal subgroup of $Aut(G)$, of the form $2 \times (GL(2,3) \circ GL(2,3))2$, so we have $|A| \leq 32$. As in the preceding paragraph, G contains no quadratic fours groups, so $|V/C_V(a)| \geq 8$ and $C_V(a) \neq C_V(A)$ for any $a \in A^{\#}$, and we have $|A| \geq 8$. In particular, we then have $A \cap H \neq 1$.

There are exactly two conjugacy classes of involutions in H, with representatives $2A$ and $2B$, and where $C_H(2A)$ and $C_H(2B)$ have the form $(4 \times L_2(9)) : 2$ and $(SL(2,3) \circ SL(2,3)) : 2^2$, respectively. Moreover, an element of $C_H(2B)$ interchanges the two subnormal $SL(2,3)$- subgroups of $C_H(2B)$. (The involution $2B$ lifts to an involution in $SL(4,3)$, while $2A$ lifts to an element of order 4.) Let $1 \neq a \in A \cap H$, and set $K = C_H(a)$. As H contains no quadratic fours groups, it follows that a is the unique involution in $C_K([V,a])$, and hence $dim([V,a]) \geq 4$. As $|A|^{3/2} \geq |V/C_V(A)| > |V/C_V(a)|$, we then have $|A| = 16$ or 32.

Suppose $|A| = 16$. Then $|V/C_V(A)| \leq 2^6$, and so $|V/C_V(a)| \leq 2^5$. We have $dim(V) \geq 26$, by 10.4(2), so it follows that H cannot be generated by five conjugates of a. Suppose that a is of type $2B$, and let L_1 and L_2 be two copies of $L_3(3)$ in H such that $\langle L_1, L_2 \rangle = H$, with $L_1 \cap L_2 \cong GL(2,3)$. Then $L_1 \cap L_2$ is generated by three conjugates of a, and since $L_1 \cap L_2$ is maximal in each L_i it follows that five conujugates of a suffice to generate H. On the other hand, suppose that a is of type $2A$. Then K lifts in $SL(4,4)$ to a group of the form $(8 \circ SL(2,9)) : 2$, so $O^2(K)$ contains a conjugate of a, and then three conjugates of a suffice to generate $O^2(K)$. We have $O^2(K) \leq L$, where $L \cong PSp(4,3)$, and $N_L(O^2(K))$ is the unique maximal subgroup of L containing $O^2(K)$. It follows that four conjugates of a suffice to generate L. As $N_H(L)$ is the unique maximal subgroup of H containing L, it follows that five conjugates of a generate H.

We conclude that $|A| = 32$. Here $|V/C_V(A)| \leq 2^7$, so $|V/C_V(a)| \leq 2^6$. Then HA is not generated by A together with three conjugates of a. Further, we now have $HA = G \cong Aut(H)$, so we may choose $a \in G - H$ so that $H\langle a \rangle \cong PGL(4,3)$, and so that a inverts an element x of order 13 in H. Then three conjugates of a generate a subgroup N of G of the form $3^3 : 13 : 2$, while a conjugate of A contains an element b which induces a transpose-inverse automorphism of H, and such that $\langle O_3(N), O_3(N)^b \rangle = H$. Thus, we have a contradiction in this case, and the lemma is proved. □

Having disposed of so many individual groups in 10.7, we may now start in on the general case. To this end, the following elementary lemma will be helpful.

10.8 Lemma. *Let $1 \leq n_1 \leq n_2 < \cdots \leq n_k$ be a non-decreasing sequence of natural numbers, and let $q > 1$. Set $N = \sum_{i=1}^k n_i$. Then $\prod_{i=1}^k (q^{n_i} + (-1)^i) < q^N$.*

Proof. Let k be the least integer for which the lemma fails. Let ℓ be the largest even integer smaller than k. Then $\ell \geq 0$ and one has $\prod_{i=1}^{\ell} (q^{n_i} + (-1)^i) < q^M$ where $N = \sum_{i=1}^{\ell} n_i$. The reader is invited to supply the last step in the induction. □

10.9 Lemma. *Let G_0 be a group such that $F^*(G_0)$ is a quasisimple group of Lie type in characteristic r different from p. Assume also that $O_p(G_0) = 1$ and that $G_0 = F^*(G_0)A$ where A is an elementary abelian p-group. Set $X = F^*(G_0)/Z(F^*(G_0))$. Finally, assume that r does not divide $|Z(F^*(G_0))|$. Then one of the following holds.*

(1) *$X \cong PSL(n,q)$ or $PSU(n,q)$, and $|G_0| \leq 2p \cdot q^{n^2-1}$.*

(2) *$X \cong PSp(2n,q)$, $n \geq 2$, and $|G_0| \leq 2p \cdot q^{n(2n+1)}$.*

(3) *$X \cong P\Omega(2n+1,q)$, $n \geq 3$, and $|G_0| \leq 2p \cdot q^{n(2n+1)}$.*

(4) *$X \cong P\Omega^{\epsilon}_{2n}(q)$, $n \geq 4$, and $|G_0| \leq 3p \cdot q^{n(2n-1)}$.*

(5) *$X \cong {}^3D_4(q)$ and $|G_0| \leq pq^{28}$.*

(6) *$X \cong E_6(q)$ or ${}^2E_6(q)$, and $|G_0| \leq 2pq^{78}$.*

(7) *$X \cong E_7(q)$ and $|G_0| \leq pq^{133}$.*

(8) *$X \cong E_8(q)$ and $|G_0| \leq pq^{248}$.*

(9) *$X \cong F_4(q)$ and $|G_0| \leq 2pq^{52}$.*

(10) *$X \cong {}^2F_4(q)$ and $|G_0| \leq pq^{26}$.*

(11) *$X \cong G_2(q)$ and $|G_0| \leq pq^{14}$.*

(12) *$X \cong {}^2G_2(q)$ and $|G_0| \leq q^7$.*

(13) *$X \cong Sz(q)$ and $|G_0| \leq pq^5$.*

Moreover, in (1) through (13), the factor p appearing in the estimate for $|G|$ is present only if q is a p^{th} power.

Proof. Let $L = L(q)$ be a Chevalley group (i.e. a non-twisted group of Lie type) of universal type. Then $|L|$ is a polynomial in q, of the form $q^M \prod_{i=1}^k (q^{n_i}-1)$, and so we have $|L| \leq q^{M+N}$, where $N = \sum i = 1^k n_i$, and where, as it happens, $M+N$ is the dimension of the adjoint module for L. We may of course take the sequence of natural numbers $n_1, n_2, \cdots n_k$ to be non-decreasing. Now assume that L is not of type D_n, $n \geq 4$, and let ${}^2L(q)$ be a Steinberg Variation of L. Then $|{}^2L(q)| = q^M \prod_{i=1}^k (q^{n_i} + (-1)^i)$, and so also $|{}^2L(q)| < q^{M+N}$ by 10.5. Suppose that $L ={}^2 D_4(q)$, of order $q^{n(n-1)}(q^n+1) \prod_{i=1}^{n-1}(q^{2i}-1)$. Then $|L| < q^{n(2n-1)}$, as follows from an obvious variation on 10.5. Also, we have

$$|{}^3D_4(q)| = q^{12}(q^8+q^4+1)(q^6-1)(q^2-1) = q^{12}(q^{12}-1)(q^6-1)/(q^2+1),$$

and so $|{}^3D_4(q)| < q^{30}/(q^2+1) < q^{28}$. So, in all these cases, $|L| < |U|$ where U is the adjoint module for the untwisted version of L. Here we refer to Table 16.1 in [A1] for the group orders, and to [J] for the dimensions of the adjoint modules. From these references, the reader may check that if L is a Suzuki-Ree group then $|L| < \sqrt{|U|}$ where U is the adjoint module for the untwisted antecedent of L.

We are given $G_0 = F^*(G_0)A$ where A is an elementary abelian p-group. Without loss of generality, we have $A \cap F^*(G) = 1$. Let A_1 be the largest subgroup of A which induces inner-diagonal automorphisms on X, and A_2 the largest subgroup of A which induces inner-diagonal-graph automorphisms of X. Then $|A/A_2| \leq p$, since the group of field automorphisms of X is cyclic. Also, $|A_2/A_1| = 1$ if X is a twisted group or if the Dynkin diagram for X admits no symmetries. Otherwise we have $|A_2/A_1| \leq 3$, with equality only if $p = 3$ and X is of type D_4. We have $|A_1| \leq p$, and if $|A_1| = p$ then p divides the order of $Z(L)$ where L is the universal version of X. Since $O_p(G) = 1$, $|A_1|$ is then "absorbed" by the estimate, given in the preceding paragraph, for $|L|$. In this way, we obtain (1) through (13). □

10.10 Lemma. *Assume Hypothesis 10.1. Then $\overline{H}$ is not isomorphic to $PSp(4,q)$ for any q.*

Proof. Set $G_0 = HA$. Then $|G_0| \leq q^{11}$, as follows from 10.9. Suppose first that q is even, so that p is odd. Then 10.4 yields $dim(V) \geq q(q-1)^2/2$. As $|A|^2 \geq |V/C_V(A)|$ we have also $|\overline{G}_0| \geq |V|$, by Theorem 2.3 of [CD1], and thus

$$22log_p(q) > q(q-1)^2/2.$$

This inequality evidently fails if $q \geq 8$, so we have $q = 2$ or 4. The case $q = 2$ has already been eliminated in 10.5, so $\overline{H} \cong Sp(4,4)$. Then $|\overline{H}| = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17$, and $Out(\overline{H})$ is a 2-group. The criteria (a) and (b) in the proof of 10.7 then reduce the problem to finding a pair of distinct maximal subgroups of $\overline{H}$ containing $\overline{S}$, in the case that $p = 3$ or that $p = 5$. According to the ATLAS, there are in fact two different maximal subgroups of $\overline{H}$ of the form $(SL(2,4) \times SL(2,4)) : 2$, and so we conclude that q is odd.

Now 10.4 yields

$$22log_p(q) > (q-1)^2/2. \tag{1}$$

Suppose that $p = 2$. Then Hypothesis $4'$ yields $|A|^{3/2} \geq |V/C_V(A)|$, and so (1) improves to

$$33log_2(q) > (q-1)^2. \tag{2}$$

This yields $q \leq 11$. Here $Z(H)$ is a 2-group, so $Z(H) = 1$ and $H = \overline{H}$. There is an S-invariant maximal subgroup L of H of the form $(SL(2,q) \circ SL(2,q)) : 2$, where the components of L are interchanged by an involution in L. If q is congruent to 3 or 5 mod 8 then there is also a maximal S-invariant subgroup M of H of the form $2^4 : Alt(5)$ (and which may be described as the set-wise stabilizer of an orthonormal basis in the $\Omega_5(q)$-module for H). Thus, we are reduced to the cases where $q = 7$ or 9.

Denote by L^* the normalizer in $Aut(H)$ of L. If $q = 7$ then $L^* = L\langle d\rangle$ where d is an involution which induces a diagonal automorphism on each of the components of L. If $q = 9$ then $L^* = L\langle d, \alpha\rangle$, where d is as just described and where α induces a field automorphism on each component of L. It follows that the 2-rank of S is 4 if $q = 7$, and at most 5 if $q = 9$. In particular, we have $|A| \leq 32$, and $|A| \leq 16$ if $q = 7$.

By 5.6, G contains no quadratic fours groups, and so 5.5 implies that $|A| \geq 8$ and that $C_V(A) \neq C_V(a)$ for any $a \in A^{\#}$. As $|A|^{3/2} \geq |V/C_V(A)|$ we have $|V/C_V(A)| \leq 2^7$, and $|V/C_V(A)| \leq 2^6$ if $q = 5$. Then $|[V,a]| \leq 2^6$ (and $|[V,a]| \leq 2^5$ if $q = 5$) for any

$a \in A^{\#}$. Suppose that $A \cap H$ contains an involution a with $C_H(a) = L$. As A contains no quadratic fours groups, $L/\langle a \rangle$ acts faithfully on $[V, a]$, whereas $[V, a]$ is too small to support such an action. Thus $A \cap Z(L) = 1$. There are only two conjugacy classes of subgroups of order 2 in H, and one of these lifts to a class of cyclic subgroups of order 4 in $SP(4, q)$. It follows from this that $|A \cap H| \leq 4$. Thus $|A| \leq 16$, and $|A| = 8$ if $q = 7$. Fix an involution $a \in A \cap H$. Then $|V/C_V(a)| \leq 32$, and $|V/C_V(a)| \leq 8$ if $q = 7$. On the other hand, 8.4 yields $dim(V) \geq 24$ if $q = 7$, and $dim(V) \geq 40$ if $q = 9$. As $C_V(H) = 0$ it follows that H cannot be generated by eight conjugates of a. We leave to the reader the task of verifying the absurdity of this outcome. □

We may now complete the proof of Theorem 10.2. Thus, assume Hypothesis 10.1. In view of 10.3, 10.5, 10.6, and 10.9, we may assume that $\overline{H}$ is not isomorphic to $L_2(q)$, or to any of the groups in the list $\mathcal{L}$ given by 10.6. Among the groups in $\mathcal{L}$ one finds all the groups of Lie type (other than those which are isomorphic to $L_2(q)$) which have an exceptional Schur multiplier. Having excluded these groups, it follows that H is a homomorphic image of the universal version, in the Lie-theoretic sense, of $\overline{H}$.

Set $G_0 = HA$. By Hypothesis 10.1 we have $|A|^2 \geq |V/C_V(A)|$, and then Theorem 2.3 of [CD1] implies that $|G_0|^2 \geq |V|$. An upper bound for G_0 is given by 10.8, while a lower bound for $dim(V)$ is given by 10.4. The proof of 10.2 now reduces to a systematic comparison of $log_p(|G_0|^2)$ with $dim(V)$.

Suppose first that $\overline{H} \cong L_n(q)$, $n \geq 3$. Then $|G_0| \leq 2pq^{n^2-1}$, and the factor p is required only if q is a p^{th} power. Thus $|G_0| \leq q^{n^2}$. By 10.4 we then have

$$(1) \qquad 2n^2 log_p(q) > (q^n - 1)/(q - 1) - n.$$

Suppose that $q = 2$. Then $p \geq 3$, and so $2log_p(q) < 1.5$. Then (1) yields $1.5n^2 > 2^n - n - 1$, and then $n \leq 5$. Thus $\overline{H} \in \mathcal{L}$ in this case, and thus $q \geq 3$. From (1) we have

$$2n^2 q + n > q^{n-1},$$

and then

$$(2) \qquad 2n^2 + n > q^{n-2}.$$

We observe that (2) is false if $q \geq 3$ and $n \geq 6$. As $q > 2$, it follows that (2) holds only if $n \leq 5$. For $n = 3$ one checks that (1) is false for $q \geq 7$, and for $n = 4$ we find that (1) is false if $q \geq 5$. Also, (1) fails to hold if $n = 5$ and $q \geq 3$. Thus, $\overline{H} \in \mathcal{L}$.

Suppose next that $\overline{H} \cong U_n(q)$, $n \geq 3$. As in the preceding case, we find $|G_0| \leq q^{n^2}$. Referring to 10.8, we then have

$$(3) \qquad 2n^2 log_p(q) > \begin{cases} (q^n - q)/(q + 1) & \text{if } n \text{ is odd, and} \\ (q^n - 1)/(q + 1) & \text{if } n \text{ is even.} \end{cases}$$

Suppose $q = 2$. Then we replace (3) by the estimate

$$(4) \qquad 2n^2 log_3(2) > (2^n - 2)/3.$$

If $n = 8$ then the left side of (4) is less than 81 and the right side is bigger than 84, so (4) fails in this case. Taking the derivative of each side of (4) with respect to n, we observe that

$$4nlog_3(2) < (ln(2))2^n$$

for all $n \geq 8$, and so (4) holds only if $n \leq 7$. Thus $\overline{H} \in \mathcal{L}$ if $q = 2$, and so $q \geq 3$.

Suppose $n = 3$. We may take $p = 2$ in (3), and obtain $18log_2(q) > (q^3 - q)/4$, which is false if $q = 7$. Taking derivatives with respect to q we find that $18/(ln(2)q) < (3q^2 - 1)/4$ for $n \geq 7$, so $q \leq 5$ if $n = 3$. Now suppose that $n = 4$. Then (3) yields $32log_2(q) > (q^4 - 1)/4$, which is false if $q = 5$. We leave it to the reader to perform the derivative test which establishes that (3) is false if $n = 4$ and $q \geq 5$. We also leave to the reader the task of verifying that if $n = 5$ then $q = 2$. Thus, in all these cases we have $\overline{H} \in \mathcal{L}$.

We now have $n \geq 6$, and we obtain

$$2n^2 log_p(q) > q(q^{n-1} - 1)/(q + 1)$$

from (3). Then also

$$2n^2 > (q^{n-1} - 1)/(q + 1) > (q^{n-1} - 1)/2(q - 1) > q^{n-2}/2,$$

and so $4n^2 > q^{n-2}$. This result fails to hold if $q = 4$ and $n = 6$, and it is a trivial matter to check that q^{n-2} grows more rapidly than $4n^2$ as a function of q and n, independently, for $q \geq 4$ and for $n \geq 6$. One also checks directly that (3) fails to hold if $n = 6$ and $q = 3$. This completes the proof that $\overline{H} \in \mathcal{L}$ if $\overline{H} \cong U_n(q)$.

Suppose next that $\overline{H} \cong PSp(2n, q)$, $n \geq 3$ (the case $n = 2$ having been dealt with in 10.9). Then 10.8 yields $|G_0| < q^{2n^2+n+1}$, and then with 10.4 we have

$$(5) \qquad 2(2n^2 + n + 1)log_p(q) > \begin{cases} (q^n - 1)/2 & \text{if } q \text{ is odd, and} \\ q(q^n - 1)(q^{n-1} - 1)/2(q + 1) & \text{if } q \text{ is even.} \end{cases}$$

If $p = 2$ then there is more than one maximal subgroup of G containing S, by Theorem A in [A1]. Thus $p \geq 3$.

Suppose $n = 3$, and then suppose that q is even. Then (5) yields $44 > (q^3 - 1)(q - 1)/2$, which is false if $q \geq 4$. On the other hand, suppose that q is odd. Then (5) yields $44log_p(q) > (q^3 - 1)/2$, which is false if $q \geq 7$. If $q = 5$ then q is not a p^{th} power, and then $|G_0| < 5^{10}$. One then checks that $40log_3(5) < 60 < (5^3 - 1)/2$. We conclude that $q = 2$ if $n = 3$.

Suppose $n = 4$. Then $q \geq 3$, by 10.6, and (5) then reduces us to the case $q = 3$. The only prime greater than 3 whose square divides $|PSp(8, 3)|$ is 5, so 2.2 yields $p = 5$. Then S is contained in a pair of subgroups L_1 and L_2 of H, with $L_1 \cong PSp(4, 3) \circ PSp(4, 3)$ and with $L_2 \cong PSp(4, 9)$, such that $H = \langle L_1, L_2 \rangle$. Thus $n \geq 5$.

Suppose that $n = 5$. If $q = 2$ then (5) yields $228log_p(2) > 155$, which is false for $p = 3$ (as one checks on one's pocket calculator) and which is therefore false for all p since $p \neq 2$. Then also (5) fails to hold for all even q, when $n = 5$. If instead q is odd then (5) yields $228log_p(q) > q^5 - 2$, and one quickly verifies that this is false for $q = 3$ (where $p \geq 5$) and then for all odd q and p.

Suppose $q = 2$. Then (5) yields

$$2(2n^2 + n + 1)log_3(2) > (2^n - 1)(2^{n-1} - 1)/3,$$

which fails to hold for $n \geq 6$. Thus, $q > 2$. In general, (5) yields

$$2(2n^2 + n + 1) > (q^n - 1)/2log_p(q) > (q^n - 1)/q > q^{n-1} - 1.$$

This fails for $n = 6$ and $q = 3$, and since $q^{n-1} - 1$ grows more rapidly than $2(2n^2+n+1)$ as a function of n, we have thereby eliminated all of the groups $PSp(2n, q)$ as possibilities for $\overline{H}$, with the exception of $Sp(6, 2)$.

Suppose next that $\overline{H} \cong P\Omega_{2n+1}(q)$, q odd, $n \geq 3$. Then 10.8 and 10.4 yield

(6)
$$2(2n^2 + n + 1)log_p(q) > \begin{cases} (q^{2n} - 1)/(q^2 - 1) - n & \text{if } q \neq 3, \text{ and} \\ (3^{2n} - 1)/8 - (3^n - 1)/2 & \text{if } q = 3. \end{cases}$$

Supppose $q \neq 3$. If $n = 3$ then (6) yields $44log_2(q) > q^4 + q^2 - 2$, which fails to hold for any odd q. Also, in the case $n = 4$ we have $78log_2(q) > q^6 + q^4 + q^2 - 3$, which also fails for odd q. In general, (6) yields

$$2(2n^2 + n + 1) > (q^{2n-2} - 1)/(q^2 - 1)log_p(q) - n/log_p(q) > q^{2n-4}/log_p(q) - n,$$

and so $4n^2+3n+2 > q^{2n-5}$. This fails for $n \geq 5$ and all odd q, so we have a contradiction in the case $q \neq 3$. On the other hand, if $q = 3$ then $log_p(q) < 2$, and so (6) implies that $4(2n^2 + n + 1) > 3^{2n-2} - 3^{n-2} > 3^{2n-3}$. This fails for $n \geq 4$, and then since $\Omega_7(3) \in \mathcal{L}$ we have a contradiction.

Suppose next that $\overline{H} \cong P\Omega^+_{2n}(q)$, $n \geq 4$. Then 10.8 and 10.4 yield

(7)
$$2(2n^2 - n + 2)log_p(q) > \begin{cases} q(q^{2n-2} - 1)/(q^2 - 1) + q^{n-1} - n & q \neq 2, 3, \text{ and} \\ q(q^{2n-2} - 1)/(q^2 - 1) - (q^{n-1} - 1)/(q - 1) - 7\delta_{2,q} & q \text{ even.} \end{cases}$$

Suppose that $q \neq 2$ or 3. As $log_p(q) < q$ we then have

$$2(2n^2 - n + 2) + n > q^{2n-4} + q^{n-2},$$

This fails to hold if $n = 4$ and $q = 4$, and then also if $n \geq 4$ and $q \geq 4$. Thus, $q = 2$ or 3. As $log_p(q) < q$, (7) yields

$$2(2n^2 - n + 2) > q^{2n-4} - q^{n-3} - 7\delta 2, q/q > q^{2n-5} - 4.$$

These inequalities fail if $n = 6$ and $q = 2$, and then also if $n \geq 6$ and $q \geq 2$. They also fail if $n = 5$ and $q = 3$. As $\Omega^+_8(2) \in \mathcal{L}$, we are then reduced to the case $n = 4$ and $q = 3$, and to the case $n = 5$ and $q = 2$. One may then check directly from (7) that neither of these cases may occur.

Suppose next that $\overline{H} \cong P\Omega^{-}_{2n}(q)$, $n \geq 4$. Then 10.8 and 10.4 yield

$$2(2n^2 - n + 2)log_p(q) > q(q^{2n-2} - 1)/(q^2 - 1) - q^{n-1} + 2. \tag{8}$$

Then $2(2n^2 - n + 2) > q^{2n-4} - q^{n-2}$, and this fails if $n \geq 6$, or if $q \geq 3$. As $P\Omega^{-}_{8}(2) \in \mathcal{L}$, we are reduced to the case where $n = 5$ and $q = 2$, and in this case one checks directly that (8) fails to hold.

It remains to consider the exceptional groups and the groups ${}^3D_4(q)$. The estimates that we obtain from 10.4 and 10.8 are as follows.

${}^3D_4(q)$: $58log_p(q) > q^3(q^2 - 1)$.

$E_6(q)$ or ${}^2E_6(q)$: $158log_p(q) > q^9(q^2 - 1)$.

$E_7(q)$: $268log_p(q) > q^{15}(q^2 - 1)$.

$E_8(q)$: $498log_p(q) > q^{27}(q^2 - 1)$.

$F_4(q)$: $106log_p(q) > q^6(q^2 - 1)$ if q is odd, or $q^7(q^3 - 1)(q - 1)/2$ if q is even.

${}^2F_4(q)$: $54log_p(q) > \sqrt{q/2}(q^4)(q - 1)$.

$G_2(q)$ $(q \geq 3)$: $30log_p(q) > q(q^2 - 1)$.

${}^2G_2(q)$ ($q \geq 27$ an odd power of 3): $14log_p(q) > q(q - 1)$.

$Sz(q)$ ($q \geq 8$ an odd power of 2): $12log_p(q) > \sqrt{q/2}(q - 1)$.

In the case of $Sz(q)$ we may take $q \geq 32$, as $Sz(8) \in \mathcal{L}$. None of the above inequalities holds for $q = 5$, and then none holds for $q \geq 5$. For $p = 3$, only the inequality for $G_2(3)$ is valid, and for $q = 2$, only the inequalities for ${}^3D_4(2)$ and ${}^2F_4(2)$ are valid. All three of these groups are in $\mathcal{L}$, so we have a final contradiction at this point, proving Theorem 10.2.

Section 11: Theorems 1 through 6

We ask the reader to recall the definitions of $\mathcal{Q}(Y, V)$, $q(Y, V)$ and $\mathcal{Q}^*(Y, V)$, from the Introduction. Recall also that, for any group G, a *component* of G is a subnormal quasisimple subgroup of G, and that $E(G)$ is the product of all the componentsof G.

11.1 Lemma. *Let p a prime, G a group whose order is divisible by p, and let S be a Sylow p-subgroup of G. Assume that $O_p(G) = 1$ and that S is contained in a unique maximal subgroup of G. Set $H = O^p(G)$ and set $\overline{G} = G/\Phi(G)$. Then one of the following holds.*

(i) *H is an r-group for some prime $r \neq p$, and S acts irreducibly on $H/\Phi(H)$.*

(ii) *$\overline{H}$ is a direct product of non-abelian simple groups, permuted transitively by $\overline{S}$. Moreover, for any component $\overline{L}$ of $\overline{G}$, $N_{\overline{S}}(\overline{L})$ is contained in a unique maximal subgroup of $N_{\overline{S}}(\overline{L})\overline{L}$.*

Moreover, if there exists a faithful $\mathbb{F}_pG$-module V with $q(S,V) \leq 2$ then, in case (ii), we have $H = E(G)$.

Proof. Denote by M be the unique maximal subgroup of G containing S, and set $F = \cap\{M^g\}_{g\in G}$. Then $G = N_G(S \cap F)F$. As $O_p(G) = 1$ and $G \neq M$ it follows that $S \cap F = 1$, and so F is a p'-group. Let M^* be any maximal subgroup of G. If $F \not\leq M^*$ then $G = FM^*$, so $S^g \leq M^*$ for some $g \in G$, and this implies that M^* is conjugate to M. Thus $F \leq M^*$, and $F = \Phi(G)$. Now let N be the inverse image in G of a minimal normal subgroup of $\overline{G}$. Then $NS = G$, and so $N = H$. Suppose that N is a p'-group. For any prime divisor r of $|N|$ there then exists an S-invariant Sylow r-subgroup of N, and it follows that N is an r-group. Uniqueness of M then implies that S acts irreducibly on $N/\Phi(N)$, and so (i) holds in this case. On the other hand, suppose that N is not a p'-group. Here $\overline{N}$ is not a p-group, as $N \neq F$, so $\overline{N}$ is a direct product of simple groups.

Suppose that (ii) is false. We may then assume without loss of generality that $F = 1$. The uniqueness of M implies that S acts transitively on the set of components of N. Fix a component L of N, and suppose that there exist distinct maximal subgroups X_1 and X_2 of $N_S(L)L$ containing $N_S(L)$. Set $X_i^* = \langle S^{X_i}\rangle$. Then X_i^* is a proper subgroup of G, and $\langle X_1^*, X_2^*\rangle = G$. As this contradicts the uniqueness of M, (ii) is proved.

Suppose now that G is non-solvable, and that $[\Phi(G), H] \neq 1$. Setting $Q = \Phi(G)$, we then have $Q = F(G) = F^*(G)$. Suppose also that there is a faithful $\mathbb{F}_pG$-module V with $q(G,V) \leq 2$, and set $q = q(S,V)$. Without loss of generality, we may assume that V is irreducible for G. Denote by $\mathcal{A}$ the set of elements A of $\mathcal{Q}^*(S,V)$ of minimal order, and set $G_0 = \langle\mathcal{A}\rangle$. Then $H \leq G_0$. Let $\mathcal{K}$ the set of subgroups of Q given by 4.6, and set $D = [Q, G_0]$. Every member of $\mathcal{K}$ has a solvable automorphism group, so if H fixes every member of $\mathcal{K}$ we obtain $[D,H] = 1$. But in that case we have $[Q,H,H] = 1$, and then $[Q, O^{p'}(H)] = 1$, and so $H = 1$. We conclude that H acts non-trivially on $\mathcal{K}$, and then 4.6(d) implies that $|A| = p$ for any $A \in \mathcal{A}$.

We have $p \leq 3$, as follows from 4.1. Suppose first that $p = 2$, and let $K \in \mathcal{K}$. By the definition of $\mathcal{K}$ (at the start of the proof of 4.6) there then exists $A \in \mathcal{A}$ with $K = [K, A]$. Then 4.6(f) says that every element of $\mathcal{K}$ is A-invariant. But $H \leq \langle A^G\rangle$, so it follows that, in fact, H acts trivially on $\mathcal{K}$. Thus, we have a contradiction if $p = 2$.

Suppose that $p = 3$. Fix $A \in \mathcal{A}$, and set $L = \langle A^H\rangle$. Then $L = \langle A^L\rangle$ and $F^*(L) = F(L)$. There then exists an irreducible L-submodule U of V such that $[F(L), L]$ acts non-trivially on U. Setting $\overline{L} = L/C_L(U)$, we then have $F^*(\overline{L}) = F(\overline{L})$, and we have $\overline{A} \cong A$ as $|A| = 3$. Set $\overline{Y} = [F(\overline{L}), \overline{A}]$. Then [C2, Theorem A] implies that $F(\overline{L})$ is a 2-group of symplectic type, that $\overline{Y}$ is a quaternion group, and that U is an irreducible module for $F(\overline{L})$. Further, if the width of a largest extraspecial subgroup $\overline{X}$ of $F(\overline{L})$ is n, then U is a direct sum of 2^{n-1} natural $SL(2,3)$-modules for $\overline{YA}$ if $\overline{X} = F(\overline{L})$, and a direct sum of 2^n such modules if $\overline{X} \neq F(\overline{L})$. As $q(G,V) \leq 2$, $\overline{A}$ is generated by a 2-transvection, so we conclude that $n \leq 2$, and that $\overline{X} = F(\overline{L})$ if $n = 2$. As $\overline{L}$

is non-solvable, it follows that $n = 2$, $F(\overline{L}) \cong Q_8 \circ D_8$, and $\overline{L}/F(\overline{L}) \cong Alt(5)$. Here $\overline{L}/F(\overline{L})$ is incident with a component of G/Q, so outcome (ii), above, implies that $\overline{A}$ is contained in a unique maximal subgroup of $\overline{L}/F(\overline{L})$. But such is not the case, and we have a contradiction at this point. Thus, the final statement in the lemma holds for all p. □

11.2 Proposition. *Let G be a group with $O_p(G) = 1$ and let V be a faithful $\mathbb{F}_pG$-module. Let $A \in \mathcal{Q}(S, V)$, let K be a component of G, put $E = \langle K^A \rangle$, and assume that $K \neq E$. Then $p = 2$, and one of the following holds:*

(i) *$|A/C_A(E)| = 2$, or*

(ii) *$E \cong \Omega_4^+(2^n)$ for some n, $n \geq 2$, and $[V, E]$ is a direct sum of natural $O_4^+(2^n)$-modules for EA.*

Proof. Without loss, $G = \langle K, A \rangle$ and $C_A(E) = 1$. Let $\Omega = \{K_1, \cdots, K_t\}$ be the set of components of G, with $K = K_1$. Suppose first that $|A| = p$, and let $1 \neq a \in A$. Then $t = p$, and for each prime factor q of $|K|$ there is an A-invariant Sylow q-subgroup Q of E with $[Q, A] \neq 1$. If p is odd then Theorem 3.8.1 in [G] says that QA involves $SL(2, p)$, and so $p = 3$ and $q = 2$. But then K is a $\{2, 3\}$-group, and hence K is solvable by a theorem of Burnside. Thus $p = 2$, and (i) holds. On the other hand, if $|A| > p$, then Theorem 2 of [C1] yields (ii). □

11.3 Lemma. *Assume Hypothesis 4, and let $A \in \mathcal{Q}_*(S, V)$. Suppose further that there exists a component X of G not normalized by A. Set $K = \langle X^A \rangle$, and let $K^S = \{K_1, \cdots, K_r\}$. Set $V_i = [V, K_i]$, $1 \leq i \leq r$. Then the following hold:*

(i) *$p = 2$, $H = K_1 \times \cdots \times K_r$, and $V = C_V(H) \oplus V_1 \oplus \cdots \oplus V_r$, where $K_i \cong \Omega_4^+(2^n)$, and V_i is a natural orthogonal module for K_i.*

(ii) *Each K_i is invariant under $\langle \mathcal{Q}(S, V) \rangle$, and $K_iA/C_{K_iA}(K_i) \cong O_4^+(2^n)$.*

Proof. Set $U = [V, K]$, and let A_0 be a complement to $C_A(K)$ in A. As $q(A, V) \leq 2$, 3.4 implies that $q(A_0, U) \leq 2$. Suppose that $|A_0| > 2$. Then 11.2 yields $p = 2$, $K \cong \Omega_4^+(2^n)$, and $V = C_V(K) \oplus U$, where U is a direct sum of natural orthogonal modules for KA_0. Set $q = 2^n$, and let U_0 be an irreducible KA_0-submodule of U. Then $|U_0| = q^4$, and $|A_0| \leq 2q$. Further, no element of $A_0 \cap K$ induces a transvection on U_0 over $\mathbb{F}_q$, and so $|U_0/C_{U_0}(A_0)| \geq q^2$. Thus $|A_0|^2 \leq 4|U_0/C_{U_0}(A_0)|$, and if $U \neq U_0$ it follows that $|A_0|^2 \leq 4|U/C_U(A_0)|^{1/2}$. But if $U \neq U_0$ we have $4|U/C_U(A_0)|^{1/2} < |U/C_U(A_0)|$, and so $q(A, V) > 2$. We therefore conclude that $U = U_0$. We have $H = \langle X^S \rangle$, by 11.2, so $H = \langle K^S \rangle$. Let $\{K_1, \cdots, K_r\}$ be the set of conjugates of K in G, and put $V_i = [V, K_i]$. Then $[U_i, K_j] = 0$ for $i \neq j$, and so (i) holds. Part (ii) follows from 11.2.

Suppose next that $|A_0| = 2$, and let a be the involution in A_0. Then $|U/C_U(a)| \leq 4$. As $O_2(G) = 1$, there is a Sylow 2-subgroup T of K of the form $R \times R^a$, where R is a Sylow 2-subgroup of X, and R has 2-rank at least 2. Then $C_R(a)$ has 2-rank at least 2, and so $C_R(a)$ contains an involution b such that $[U, a, b] = 0$. Setting $A_1 = \langle a, b \rangle$, we then have $[U, A_1, A_1] = 0$, and so 11.2 implies that $K \cong \Omega_4^+(2^n)$ and that U is a direct sum of natural orthogonal modules for KA_0. As in the preceding paragraph, let U_0 be an irreducible KA_0-submodule of U. As $2^n \geq 4$, we then have $|A_0|^2 \leq |U_0/C_{U_0}(A_0)|$, and hence $U = U_0$. Now (i) and (ii) follow, as above. □

We may now assemble the proofs of Theorems 1 through 6.

Theorem 1. *Assume Hypothesis 4. Then there exists a subgroup K of H, unique up to conjugation, such that, upon setting $U = [V, K]$, the following conditions hold.*

(a) *$H = K_1 \times \cdots \times K_r$ where $\{K_1, \cdots, K_r\} = K^S$.*

(b) *We have $[V, K_i, K_j] = 0$ whenever $i \neq j$.*

(c) *One of the following holds:*

(i) *$K \cong O^p(SL(2, p^n))$, $n \geq 1$, and $U/C_U(K)$ is a natural $SL(2, p^n)$-module for K, or a direct sum of two natural modules for K.*

(ii) *$K \cong O^p(O_4^\epsilon(p^n))$, $n \geq 1$, $\epsilon = \pm 1$, and U is a natural orthogonal module for K.*

(iii) *$K \cong O^p(SU(3, p^n))$ and U is a natural module for K.*

(iv) *$p = 2$, $K \cong O^2(Sz(2^n))$, and U is a natural module for K.*

(v) *$p = 2$, $A \leq C_G(K)K$, $K \cong SL(3, 2^n)$ (resp. $O^2(Sp(4, 2^n))$) and U is the direct sum of a natural and a dual module (resp. a natural and a contragredient module) for K. Moreover, there exists $g \in N_S(K)$ such that g interchanges, by conjugation, the two maximal subgroups of K containing $S \cap K$, and if $K \cong O^2(Sp(4, 2^n))$ then A is conjugate to $Z(S)$.*

(vi) *$p = 2$, $K \cong Alt(2^n + 1)$, $n \geq 3$, and U is a natural module for K, or a direct sum of two natural modules for K.*

(vii) *$p = 2$, $K \cong Alt(9)$, and U is a spin module for K, of dimenson 8 over $\mathbb{F}_2$.*

viii *$p = 3$, $K \cong SL(2, 5)$, and U is a natural $SL(2, 9)$-module for K.*

Moreover, if K is not invariant under $\mathcal{Q}^*(S, V)$ then $p = 2$, $K \cong \mathbb{Z}_3$, $|U| = 4$, and $q(S, V) = 2$.

Proof. If G is solvable then the theorem follows from 11.1 and 4.6. So assume that G is non-solvable. Then 11.1 yields $H = E(G)$. Let $A \in \mathcal{Q}(S, V)$. If there is a component X of G such that X is not A-invariant, then the theorem follows from 11.3. So assume that X is A-invariant. If $X \cong SL(2, p^n)$, $[V, X]$ is a direct sum of two natural modules for X, and there exists a unique conjugate Y of X such that $[X, Y] = 1$ and $[V, X, Y] \neq 0$, set $K = XY$, and otherwise set $K = X$. Let $\{K_1, \cdots, K_r\}$ be the set of conjugates of K under S. By 11.1 we then have $H = K_1 \cdots K_r$. Set $V_i = [V, K_i]$, and set $U = [V, K]$.

As $O_p(G) = 1$ we may assume that A and X have been chosen so that $[X, A] \neq 1$. Choose a complement A_0 to $C_A(K)$ in A. Then $q(A_0, U) \leq 2$, by 3.4. If $K = X$ set $A_1 = A_0$, and otherwise take A_1 to be a complement in A_0 to $C_{A_0}(X)$. Then also $q(A_1, [V, X]) \leq 2$. If $p = 3$, $X \cong SL(2, 5)$, and $[V, X]$ is a natural $SL(2, 9)$-module for X then $K = X$ and the theorem holds (with (c)(viii)), so we may assume that this special case does not obtain. Then 5.5 implies that $X/Z(X)$ is a group of Lie type in characteristic p, or that $p = 2$ and X is an alternating group $Alt(2^n + 1)$. If $X/Z(X)$ is of Lie type in characteristic p then 5.9 says that the pair $(X, [V, X])$ is described by 6.10 or by 7.5, while if $X \cong Alt(2^n + 1)$ then 5.7 provides a description of $(X, [V, X])$. In particular, if $[V,X]$ is reducible, and is not a direct sum of two non-isomorphic irreducible submodules, then $X \cong SL(2,p^n)$ or $Alt(2^n+1)$ and X is a direct sum of two natural modules for X. It follows that if $End_X([V,X])$ contains a subgroup isomorphic to X, then $[V,X]$ is a direct sum of two isomorphic irreducible modules, and if W is an irreducible submodule of $[V,X]$ then the dimension of W over $End_X(W)$ is equal to 2. This is the case only if $X \cong SL(2,p^n)$ and $[V,X]$ is a direct sum of two natural modules.

Suppose that $[V,X,Y] \neq 0$ for some conjugate Y of X with $Y \neq X$. Then the preceding discussion yields $XY \cong \Omega_4^+(p^n)$, $[V,X]$ is a natural orthogonal module for XY, and X and Y are the only conjugates of X which act non-trivially on $[V,X]$. By definition, we then have $K = XY$ and $U = [V,X]$. The theorem follows in this case (with (c)(ii)), so we may assume henceforth that $[V,X,Y] = 0$ for any conjugate of X distinct from X. Then also $K = X$.

If $K/Z(K)$ is a group of Lie type in characteristic p, the theorem now follows from 6.10 and 7.5. Thus, we are reduced to the case where $p = 2$ and $K \cong Alt(2^n+1)$. Since $Alt(5)$ is a group of Lie type in characteristic 2, we may assume that $n \geq 3$. The theorem then follows from 5.7 (with either part (vi) or part (vii) of (c) obtaining). □

In order to prove Theorems 2 and 3, let the hypotheses be as in Theorem 1, and fix $A \in \mathcal{Q}^*(S,V)$. Suppose that $q^*(A,V) < 2$, and let K and U be as in Theorem 1, with $[K,A] \neq 1$. Let A_0 be a complement in A to $C_A(K)$. Then $q(A_0,U) < 2$ by 3.4, and so we do not have the case given by (c)(viii) in Theorem 1. Thus, K is of Lie type in characteristic p, or $p = 2$ and $K \cong Alt(2^n+1)$ with $n \geq 3$.

Suppose that K is quasisimple. If the Lie rank of $K/Z(K)$ is 1 then 6.10 implies that $H \cong SL(2,p^n)$, or that $p = 2$ and $H \cong \Omega_4^-(2^n)$ or $Alt(5)$, with U a natural module for K in each of these cases. Moreover, if $H \cong Omega_4^-(2^n)$ then 6.10 says that $KA/C_{KA}(K) \cong O_4^-(2^n)$. Thus, Theorem 2 holds in these cases. If the Lie rank of $K/Z(K)$ is greater than 1 then 5.9 and 7.5 yield $p = 2$ and $K \cong SL(3,2^n)$, and Theorem 2 holds in this case. Now suppose that $K \cong Alt(2^n+1)$, $n \geq 3$. Then 5.7 applies. In particular, the condition $q(A_0,U) < 2$ excludes the case where $n = 3$ and U is a spin module for K, and excludes also the case where U is a direct sum of two natural modules for K. Thus, U is a natural module for K, and we have Theorem 2 in this case.

Now assume that K is not quasisimple, and that K is non-solvable. Then Theorem 1 yields $K \cong \Omega_4^+(p^n)$. Suppose that A fixes each of the components of K. As $q(A_0,U) < 2$ it is then easy to see that $|A| > p$, and so $A_0 \cap C_G(K)K \neq 1$. Quadratic action then forces $A_0 \leq C_G(K)K$, and we again appeal to the quadratic action of A_0, to conclude that $|A_0| \leq p^n$. But $dim_{\mathbb{F}_{p^n}}(C_U(a)) \leq 2$ for any $a \in A_0^{\#}$, so $q(A_0,U) \geq 2$ in this case. We therefore conclude that $p = 2$ and that A_0 interchanges the two components of K. Then 11.2 yields $KA/C_{KA}(K) \cong O_4^+(2^n)$. This is outcome (ii) of Theorem 2.

Suppose finally that K is solvable. If K is not A-invariant then Theorem 1 yields $K \cong \mathbb{Z}_3$ and $|U| = 4$, and this result is contained in outcome (i) of Theorem 2. So assume that K is A-invariant. As $q(A,V) < 2$, 4.5(a) implies that $|U| = p^2$, and that $K \cong O^p(SL(2,p))$ ($p = 2$ or 3). We have thus eliminated all the cases in Theorem 1 which do not remain in the statement of Theorem 2, and thus Theorem 2 is proved.

Now suppose that $q(S,V) \leq 1$. If K is solvable then Theorem 3 follows from 4.5(b), so assume that K is non-solvable. We have $q(A_0, U) \leq 1$, so 7.5 implies that K is not isomorphic to $SL(3, 2^n)$ with $p = 2$. If $p = 2$ and $K \cong \Omega_4^+(2^n)$, $n \geq 2$, then Theorem 2 yields $|A_0| = 2^{n+1}$ and $|U/C_U(A_0)| = 2^{2n}$, and so $q(A_0, U) > 1$ in this case. If $p = 2$ and $K \cong Alt(2^n + 1)$, $n \geq 3$, then 5.7 implies that A_0 is generated by a set of commuting transvections on the natural module U, so that $KA/C_{KA}(K) \cong Sym(2^n+1)$ and $q(A_0, U) = 1$. Then $1 = q(A, V) = q(S, V)$, and $\langle A^H \rangle$ is isomorphic to a direct product of copies of $Sym(2^n + 1)$. Then also $\langle A^G \rangle$ is the point-wise stabilizer in G of $\{K_1, \cdots, K_r\}$, and is a direct product of copies of $Sym(2^n + 1)$. Thus, Theorem 3 holds in this case. Finally, the last case given by Theorem 2 is that in which $K \cong SL(2, p^n)$ and U is a natural module for K. Again, we have $q(A_0, U) \leq 1$, and it follows that A_0 is incident with a Sylow p-subgroup of $KA/C_{KA}(K)$ and that $q(A_0, U) = 1$. We then obtain $q(S, V) = 1$, and $\langle A^G \rangle = H$. This completes the proof of Theorem 3.

Theorem 4. *Assume Hypothesis 3, and assume that H is a quasisimple group of Lie type in characteristic p. Let A be an $F2$-offender on V. Then one of the following holds.*

(a) *$H \cong SL(2, p^n)$ and one of the following holds.*
  (i) *V is a natural $SL(2, p^n)$-module for H.*
  (ii) *V has an H- submodule U such that both U and V/U are natural $SL(2, p^n)$-modules for H.*
  (iii) *n is even and V is a natural $\Omega_4^-(p^{n/2})$-module for H.*

(b) *$H \cong SU(3, p^n)$ and V is a natural module for H.*

(c) *$p = 2$, $H \cong Sz(2^n)$, and V is a natural module for H.*

(d) *$p = 2$, $H \cong SL(3, 2^n)$ (resp. $O^2(Sp(4, 2^n))$) and V is the direct sum of a natural and a dual module (resp. a natural and a contragredient module) for H. Moreover, there exists $g \in N_S(K)$ such that g interchanges, by conjugation, the two maximal subgroups of H containing $S \cap H$. If A is a quadratic $F2$-offender then $A \leq H$, and if also $H \cong Sp(4, 2^n)$ then A is conjugate to $Z(S)$.*

Proof. Immediate from 5.9, 6.8, 6.9, and 7.5. □

Theorem 5. *Assume Hypothesis $4'$, and assume that $H/Z(H)$ is isomorphic to $Alt(n)$, $n \geq 5$. If $p = 2$ assume that n is odd. Then one of the following holds.*

(i) *$p = 2$, $H \cong Alt(n)$, $n \geq 5$, and V is a natural module for H.*

(ii) *$p = 2$, $H \cong Alt(n)$, $n = 5, 7$, or 9, and V is a spin module for H (of dimension 4, 4, or 8, respectively). Moreover, if $n = 9$ then A is the direct product of two quadratic fours groups in H.*

(iii) *$|A| = p = 3$, $G \cong Alt(n)$, $n \neq 6$, and V is a natural module for G. Moreover, A is generated by a 3-cycle.*

(iv) *$|A| = p = 3$, $H \cong SL(2, 5)$, and V is isomorphic to the natural $SL(2, 9)$-module for H.*

(v) *$p = 3$, $H \cong Alt(9)$, $|A| = 27$, and V is a spin module for H (of dimension 8 over $\mathbb{F}_3$). Moreover, we have $|A|^2 = |V/C_V(A)|$.*

Proof. If p is odd then 8.3 yields one of the outcomes (iii) through (v) above. So assume that $p = 2$ (and hence also that n is odd). Suppose that there is more than one non-trivial irreducible constituent for HA in V. As $q(A, V) \leq 3/2$, there there then exists a non-trivial irreducible constituent U for HA in V such that $q(A, U) \leq 3/4$. By the Timmesfeld Replacement Theorem there then exists $B \in \mathcal{Q}(S, U)$ with $q(B, U) \leq 3/4$, and this is contrary to 5.7. Thus, there is a unique non-trivial constituent in V for HA, and then V is irreducible for HA, and hence also for G, by 1.2.

If $n = 5$ then $H \cong L_2(4)$, and we obtain (i) or (ii) from Theorem 4. So we may assume that $n \geq 7$. By 9.1 there then exists a fours group F in G with $A \cap F \neq 1$ and with $[V, F, F] = 0$. Assuming that V is not a natural module for G, it then follows from [MS2, Theorem 4] that V is a spin module for HF. Let a be a non-identity element of $A \cap F$, and identify H with $Alt(n)$. After conjugation, we have $F = \langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle$, and F is the unique quadratic fours group in G containing a. Denote by k the greatest integer in $n/3$. Then H contains a subgroup E generated by k pairwise disjoint 3-cycles. For any 3-cycle x in H we have $C_V(x) = 0$, so the dimension of V over $\mathbb{F}_2$ is a multiple of 2^k. In particular, if $dim(V) < 8$ then $n = 7$, and we have (ii). So we may assume that $dim(V) \geq 8$ (and that $n \geq 9$).

As a inverts a 3-cycle, we have also $dim(V) = 2dim(C_V(a))$. Then $|V/C_V(a)| \geq 16$, and then since $|A|^{3/2} \geq |V/C_V(A)| \geq |V/C_V(a)|$ we have $|A| \geq 8$. If $C_V(a) = C_V(A)$, and then every fours group in A which contains a is quadratic, contrary to the uniqueness of F. We therefore conclude that $C_V(a) \neq C_V(A)$, and this yields $|A| \geq 16$.

Let K be the component in $C_H(a)$, and let A_0 be a complement to $C_A(K)$ in A. Then $|A_0| \geq 4$. For any 3-cycle y in K we have $C_{[V,a]}(y) = 0$, so $[V, a] = [V, a, K]$, and Theorem 4 in [MS2] implies that every irreducible constituent for K in $[V, a]$ is a spin module. As A_0 acts quadratically on $[V, a]$, by hypothesis, we conclude that $|A_0| = 4$. Then $F \leq A$, we may take A_0 to be a quadratic fours group contained in K, and we have $A = F \times A_0$. Now $|A|^{3/2} = 64$, and since $C_V(a) \neq C_V(A)$ we have $dim(C_V(a)) \leq 5$. Then $dim(C_V(a)) = 4$, and the faithful action of K on $C_V(a)$ yields $n = 9$ or 11. Now $dim(V) = 8$, and since 11 is not a divisor of $|L_8(2)|$ we have $n = 9$, and (ii) holds. □

Theorem 6. *Assume Hypothesis $4'$, and assume that S is contained in a unique maximal subgroup of G. Assume also that $H/Z(H)$ is a quasisimple group of Lie type in characteristic different from p, or a sporadic group, and that there exists no isomorphism of $H/Z(H)$ with a group of Lie type in characteristic p. Then $|A| = p = 3$, $G \cong Sp(6, 2)$, V has dimension 7 over $\mathbb{F}_3$, and $|A|^2 = |V/C_V(A)|$.*

Proof. Immediate from 2.2 and 10.2. □

References

[A1] M. Aschbacher, *On finite groups of Lie type and odd characteristic.*

[A2] ———, *$GF(2)$-representations of finite groups*, Amer. Jour. of Math. **104 4** (1982), 683-771.

[A3] ———, *Finite Group Theory*, Cambridge University Press Cambridge, 1986.

[A4] ———, *Overgroups of Sylow subgroups in sporadic groups*, Memoirs Amer. Math. Soc. **60 343** (1986), 1-235.

[AS] M. Aschbacher and S. Smith, *Quasithin groups*, (In preparation).

[B] H. Bender, *On groups with abelian Sylow 2-subgroups*, Math. Zeit. **117** (1970), 164-176.

[C1] A. Chermak, *An elementary proof of the $\mathcal{P}(G, V)$-theorem in arbitrary characteristic*, Jour. of group theory **2** (1999), 1-13.

[C2] ———, *Quadratic pairs without components*, (preprint).

[C3] ———, *Quadratic pairs*, (preprint).

[CD] A. Chermak and A. L. Delgado, *A measuring argument for finitte groups*, Proc. Amer. Math. Soc. **107** **4** (1989), 907-914.

[Chev] Claude Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras*, Springer Verlag, 1991.

[CCNPW] Conway, Curtis, Norton, Parker, Wilson, *ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.

[DS] A. L. Delgado and B. Stellmacher, *Weak (B, N)-pairs of rank* 2, in Groups and Graphs: New Results and Methods (Goldschmidt, Delgado, and Stellmacher, eds.), Birkhäuser, Basel, 1985.

[G] Daniel Gorenstein, *Finite Groups*, Second Edition, Chelsea, New York, 1980.

[GLS3] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, American Math. Soc., 1994.

[HH] Phillip Hall and Graham Higman, *The p-length of a p-soluble group and reduction theorems for Burnside's problem*, Proc. London Math. Soc. **6** (1956), 1-42.

[J] N. Jacobson, *Lie Algebras*, Dover, 1979.

[K] William Kantor, *Some exceptional* 2*-adic buildings*, J. Algebra **92** (1985), 208–223.

[LPR] W. Lempken C. Parker and P. Rowley, *Minimal parabolic systems for the symmetric and alternating groups*, preprint.

[M] Ulrich Meierfrankenfeld, *A characterization of the Spin-module for* $2 \cdot A_n$.

[MS1] Ulrich Meierfrankenfeld and Gernot Stroth, *On quadratic $GF(2)$-modules for Chevalley groups over fields of odd order*, Arch. Math. **55** (1990), 105-110.

[MS2] ———, *Quadratic $GF(2)$-modules for sporadic simple groups and alternating groups*, Comm. in Algebra **18** **7** (1990), 2099-2139.

[N] R. Niles, *Pushing-up in finite groups*, J. of Algebra **57** (1979), 26-63.

[Sa] B. Salzberg, *Another look at Thompson's quadratic pairs*, J. Algebra **45** (1977), no. 2, 334–342.

[St1] R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33-56.

[St2] ———, *Lectures on Chevalley Groups*, Notes by J. Faulkner and R. Wilson, Mimeographed notes, Yale University Mathematics Department, 1968.

[Stel] Bernd Stellmacher, *On the* 2*-local structure of finite groups*, in Groups, Combinatorics, and Geometry (Liebeck and Saxl, eds.), London Math. Soc. Lecture Notes 165, Cambridge University Press, 1992.

[T] F. Timmesfeld, *A remark on Thompson's replacement lemma*, Arch. Math. **38** (1982), 491-495.

[W] J. Walter, *The characterization of finite groups with abelian Sylow* 2*-subgroups*, Ann. of Math. **89** (1969), 405-514.

[Z] K. Zsigmondy, *Zur Theorie Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265-284.