COMMUTING INVOLUTIONS AND ELEMENTARY ABELIAN SUBGROUPS OF SIMPLE GROUPS

ROBERT M. GURALNICK AND GEOFFREY R. ROBINSON

Dedicated to the memory of our good friend Jan Saxl

Abstract. Motivated in part by representation theoretic questions, we prove that if G is a finite quasi-simple group, then there exists an elementary abelian subgroup of G that contains a member of each conjugacy class of involutions of G.

1. Introduction

Let G be a finite group. An involution of G is an element of order 2. An elementary abelian subgroup E of G is a called a broad subgroup if every involution of G is conjugate to an element of E. This definition is motivated in part by the fact that (using a theorem of R. Knörr [7]) an irreducible character which vanishes identically on non-identity elements of E lies in a 2-block of defect zero. This in turn allows us to prove that when G contains a broad subgroup, the number of irreducible characters of G which lie in 2-blocks of positive defect of G is at most $|C_G(t)|$ for some involution $t \in G$. Our main result (which depends upon the classification of finite simple groups) is:

Theorem 1. *Let G be a finite quasi-simple group. Then G contains a broad subgroup.*

Notice that it is immediate that a direct product of finite groups has a broad subgroup if each direct factor has a broad subgroup.

We have the following corollary, which may be of independent interest:

Corollary 2. *Let G be a finite quasi-simple group. If x and y are involutions of G, then x commutes with some conjugate of y.*

The promised application to character theory is provided by:

Corollary 3. *Let G be a finite group with no non-trivial normal subgroup of odd order. Then there is an involution $t \in F^*(G)$ such that the total number of irreducible characters of G which do not lie over 2-blocks of defect zero of $F^*(G)$ is at most $|C_G(t)|$.*

This applies in particular when G is a non-abelian simple group, and since $G = \mathrm{SL}_2(2^n)$ (for $n \geqslant 2$) has exactly 2^n irreducible characters which lie in 2-blocks of positive defect, while $|C_G(t)| = 2^n$ for each involution $t \in G$, the inequality of Corollary 3 may be sharp. If G is quasisimple and the center has even order, then there is a central element of order 2 and so the corollary is not useful.

Note that there is no direct analog of Theorem 1 for odd primes. For example if $p \geq 5$, let $S = \mathrm{SL}_n(p)$ with $4 \leq n \leq p$. Since $Z(S)$ has order prime to p, it suffices to produce an example in S. Let x be a regular unipotent element (i.e. x has a single Jordan block of size n).

Date: April 20, 2021.

The first author was partially supported by the NSF grant DMS-1901595 and a Simons Foundation Fellowship 609771. We thank Thomas Breuer for computations with sporadic groups and groups with exceptional multipliers, Ross Lawther for comments on the exceptional groups in characteristic 2 and Gunter Malle for his comments on an earlier version of the paper. We also thank the referee for their careful reading of the paper and their comments.

Note that x has order p. Then $C_S(x)/Z(S)$ is an elementary abelian p-group of rank $n-1$. It is straightforward to check that the only elements $y \in C_S(x)$ which have two Jordan blocks have Jordan blocks of sizes $(n \pm 1)/2$ if n is odd and two Jordan blocks of size $n/2$ if n is even. Thus, x does not commute with an element of order p that has Jordan blocks of size $n-1$ and 1.

For $p = 3$, we give an example where elements of order 3 are semisimple. Let $S = \mathrm{SL}_9(q)$ with $q \equiv 4 \pmod 9$. Then $Z = Z(S) = \langle z \rangle$ has order 3. Let $x \in S$ satisfy $x^3 = z$. So in $G = S/Z$, xZ is an element of order 3. Let $y \in S$ be an element of order 3 with a 7-dimensional 1-eigenspace. We claim that no conjugate of y commutes with x modulo Z. Suppose there is a conjugate y' of y commuting with x modulo Z. Then replacing y' by y, we see that $[x, y] = u \in Z$. Then y is conjugate to yu whence by considering eigenvalues, $u = 1$. So x and y commute in S. Since y has a 1-dimensional eigenspace, x must preserve this space. However, x has no eigenvalues in the base field, a contradiction.

The result also fails in general for almost simple groups for $p = 2$. Let $G = \mathrm{O}^+_{4m}(2^a)$ be the orthogonal group. There are two conjugacy classes of involutions in the socle $\Omega^+_{4m}(2^a)$, which are interchanged by an involution in G. Clearly such an outer involution cannot commute with any element of either of the two conjugacy classes interchanged.

Note that all three families of counterexamples above are also counterexamples to Corollary 2. We also remark that it is easy to check that the quaternion group Q_8 is the only extra-special 2-group which has a broad subgroup, while it is clear that for p odd, a non-abelian p-group of exponent p never has a broad elementary abelian p-subgroup.

In the next three sections, we prove Theorem 1 for the various families of quasi-simple groups. In the last two sections, we prove Corollary 3 and discuss some other character theoretic results.

2. Alternating and Sporadic Groups

We make a few preliminary remarks before starting the proof of Theorem 1. We may assume that G has no non-trivial odd order normal subgroups and in particular if G is quasisimple, we may assume that the center is a 2-group. We call an involution 2-central if it is contained in the center of a Sylow 2-subgroup of G.

If G has at most one class of non 2-central involutions, then the result holds by considering the abelian subgroup $E = \langle Z(S), x \rangle$ where S is a Sylow 2-subgroup of G and $x \in S$ is a non 2-central involution. If G has 3 conjugacy classes of involutions, C_1, C_2 and C_3 and there exist $x_i \in C_i$ with $x_1 x_2 x_3 = 1$, then the elementary abelian subgroup $\langle x_1, x_2 \rangle$ intersects each C_i. If H is a subgroup of G and H intersects every conjugacy class of involutions of G and H has a broad subgroup, then so does G.

The case of alternating groups is trivial.

Lemma 2.1. *Let $G = A_n, n \geq 5$. Let E be the maximal elementary abelian subgroup of S_n with all orbits of size 2 if n is even and all orbits but one of size 2 if n is odd. Then every involution in S_n is conjugate to an element of E by an element of A_n.*

Lemma 2.2. *Let $G = 2A_n, n \geq 5$ be the nonsplit double cover of A_n. Then G contains a broad subgroup.*

Proof. If $x \in A_n$ is an involution, then x lifts to an involution in G if and only if the number of points moved by x is a multiple of 8. Now choose a partition of $\{1, \ldots, n\}$ into subsets $X_0, X_1, \ldots, X_d$ where $|X_i| = 8$ for $i > 0$ and $|X_0| < 8$. Let E be the elementary abelian 2-group $E_1 \times \ldots \times E_d$ where E_i acts as a regular elementary abelian group of order 8 on X_i. Note that if $x \in E$, then x moves $8e$ points for some $0 \leq e \leq d$. Let $Z = Z(G) = \langle z \rangle$ and let $f : G \to G/Z$ be the natural map. Thus, if $x \in E$, $f^{-1}(x) = \{t, tz\}$ with t an involution.

Thus, $f^{-1}(E)$ is an elementary abelian 2-group containing a conjugate of every involution of G. □

All but five of the sporadic groups have at most 2 conjugacy classes of involutions and so at most one class of involutions that are not 2-central. As noted above, this implies the result. The remaining cases are $Co_2, Co_1, Fi_{22}, Fi_{23}$ and B. The first four have three classes of involutions and B has four such classes. In these cases, we just use GAP [5] to produce E. One deals with the quasi-simple sporadic groups in a similar manner. The details of the computations and more detailed explanations are given in [2, 2.3-10].

Lemma 2.3. *Let G be a quasi-simple sporadic group. Then there exists an elementary abelian subgroup E intersecting every conjugacy class of involutions in G.*

Proof. First assume that G is simple. As noted above, there are only five sporadic groups with more than 2 conjugacy classes of involutions. In each of the five cases, we produce a subgroup H for which the theorem holds and which intersects each conjugacy class of involutions (this condition can be checked using fusion tables in GAP [5]).

First set $H = HS.2 = \mathrm{Aut}(HS)$. Then H has four conjugacy classes of involutions and using [5], one sees that there is an elementary abelian subgroup of order 8 intersecting each conjugacy class of H.

In each of the five sporadic groups, we use [5] to a find a subgroup J of G intersecting all conjugacy classes of G such that J also has the desired property. If $G = Co_2$ or B, there is a subgroup $J \cong H$ intersecting each class. If $G = Co_1$, take $J = A_9 \times S_3$. If $G = Fi_{22}$ or Fi_{23}, then we can choose $J = O_2(2^{10}M_{22})$ or $O_2(2^{11}M_{23})$.

Now assume that G is quasisimple with $Z = Z(G)$ a non-trivial 2-group. There are ten groups to consider. If $G = 2M_{12}$, $2M_{22}$, $2J_2$, $2HS$, $2Ru$ or $2Suz$, there is an elementary abelian subgroup H of G/Z such that H intersects each conjugacy class of involutions in G/Z that lift to involutions in G and none that lift to elements of order 4. Thus, if $Z < K$ with $K/Z = H$, then K is elementary abelian and intersects each conjugacy class of involutions in G. If $G = 2Fi_{22}$, then all involutions lift to involutions and so just take the preimage of the elementary abelian subgroup of G/Z intersecting all the classes of involutions. If $G = 4M_{22}$, then G has only two conjugacy classes of involutions and so the result holds.

Suppose that $G = 2.Co_1$. There are 4 classes of involutions which are lifts of the classes $2A$ and $2C$ involutions in Co_1. Thus, it suffices to show that there is a elementary abelian subgroup K of Co_1 of order 4 containing $2A$ and $2C$ involutions but no element from $2B$. This follows from the fact that the $(2A, 2A, 2C)$ structure constant of Co_1 is nonzero. The preimage of K is the desired broad subgroup.

Finally suppose that $G = 2.B$. There are 5 classes of involutions in G. It suffices to show that there is an elementary abelian subgroup K of B of order 4 that contains elements from the classes $2A, 2B$, and $2D$ (but no element from $2C$). This follows from the fact that the $(2A, 2B, 2D)$ structure constant of B is nonzero. The preimage of K is the given broad subgroup. □

3. Groups of Lie type in characteristic 2

In this section q is a power of 2. We consider the finite simple groups of Lie type over $\mathbb{F}_q$. We will typically work with the simply connected group (which will have center of odd order) which is sufficient. We begin by observing that the centralizer of an involution is connected in the ambient algebraic group (it is not true that all centralizers of unipotent elements are connected).

Lemma 3.1. *Let X be a simple algebraic group over any algebraically closed field of characteristic 2. Let $g \in X$ be an involution. Let σ be a Steinberg endomorphism of X (i.e. the fixed subgroup X_σ of σ on X is finite).*

(1) $C_X(g)$ is connected.
(2) If g^X is σ-invariant, then $g^X \cap X_\sigma$ is a single conjugacy class in X_σ.

Proof. Since $Z(X)$ is finite of odd order, the result does not depend upon the isogeny type of X. So we may work with the most convenient form of the group. It follows by Lang-Steinberg, that (1) implies (2) and indeed, the converse is true as well.

If σ is the standard q-Frobenius endomorphism of X, we write $X_\sigma = X(q)$.

If G is exceptional, we just quote [10, Chapter 22]. This also follows from the result in [1] where is it shown that any involution in X_σ is conjugate to an involution in $X(2)$ and there is no fusion of classes of involutions in $X(2)$ in any $X(q)$ (and so also in X). This argument holds in the case of classical groups with one minor complication. In both [1] and [10], the classes in the case $X = \mathrm{SO}_n(k)$, n even (or in X_σ), are given in terms of conjugacy in the orthogonal group. In fact, there is only one pair of SO-classes which are not also O-classes (and only if $n = 4m$). This $\mathrm{O}(V)$-class is denoted a_{2m} in [1] and $W(2)^m$ in [10]. Aside from that pair of classes, one can argue as above (i.e. either consider the results in [1] or [10]). If we use [10], then in results about centralizers, the centralizer usually has two connected components and so is connected in $\mathrm{SO}(V)$. Consider this last case. Let $g \in X$ be in one of the classes of involutions that is not $\mathrm{O}(V)$-invariant. Then the centralizer of g in $\mathrm{O}(V)$ is contained in X. It is shown in [10] that this is connected (and so also for the other class). □

Remark 3.2. (1) We note that if X is a classical group, there is a fairly elementary proof. We just need to observe that any two involutions in $X(q)$ which are conjugate in X are already conjugate in $X(q)$. If $X = \mathrm{SL}_n(k)$, then any involution in $X(q)$ is contained in the radical of the parabolic subgroup stabilizing a subspace of dimension $\lfloor (n+1)/2 \rfloor$. Similarly, if $X = \mathrm{Sp}_{2n}(k)$, every involution acts trivially on a totally singular n-dimensional space. In both cases, the result follows by elementary linear algebra.

The argument for $\mathrm{SO}_{2n}(k)$ is slightly more complicated but follows from the fact that two involutions in $\mathrm{SO}_{2n}(k)$ which are conjugate in $\mathrm{Sp}_{2n}(k)$ are already conjugate in $\mathrm{O}_{2n}(k)$ [1, 4, 10].

(2) Also note that the connectedness of centralizers in the simple case implies the same result for any connected reductive group as well.

(3) Costantini [3] has shown that if X is a simple algebraic group in characteristic 2, then centralizers of involutions are spherical (i.e. there are only finitely many double cosets $C_X(g)\backslash X/B$ with g an involution and B a Borel subgroup) and moreover that $C_B(g)$ is connected and from that one can deduce the connectedness of $C_X(g)$. The proof does depend on the classification of involutions [1].

3.1. **Linear, Unitary and Symplectic Groups.** The case of $\mathrm{SL}_n(q)$ is obvious.

Lemma 3.3. *Let $G = \mathrm{SL}_n(q) = \mathrm{SL}(V), n \geq 2$ and set $m = \lfloor (n+1)/2 \rfloor$. Let P be the stabilizer of an m-dimensional subspace W of V. Then any involution in G is conjugate to an element acting trivially on W. In particular, if Q is the unipotent radical of the stabilizer of W, then Q is elementary abelian and every involution of G is conjugate to an element of Q.*

For symplectic and unitary groups, we use the following elementary observation.

Lemma 3.4. *Let $n \geq 2$ with $G = \mathrm{SU}_{2n}(q)$ or $\mathrm{Sp}_{2n}(q)$. Then any involution g acts trivially on a totally isotropic subspace of dimension n and so the elementary abelian subgroup Q that is the unipotent radical of the stabilizer of a totally singular subspace of dimension n intersects every conjugacy class of involutions.*

Proof. If $G = \mathrm{Sp}_{2n}(q)$, the argument is easier (and is given in [4, Lemma 4.4]). So we assume that $G = \mathrm{SU}_{2n}(q)$.

Let W be the fixed space of an involution $g \in G$. Note that $\dim W \geq n$. If W is totally singular, the result follows. Otherwise g is trivial on a nondegenerate 1-space L. Then g acts on $L^{\perp}$ and since $\dim L^{\perp} = 2n-1$, the fixed space of g has dimension at least n and so is not totally singular. Thus g leaves invariant some nondegenerate 1-space orthogonal to L and so acts trivially on a nondegenerate 2-space. The result then follows by induction. $\square$

Since every every involution of $G := \mathrm{SU}_{2n+1}(g)$ fixes a nondegenerate 1-space , it follows that a subgroup $\mathrm{SU}_{2n}(q)$ contains a conjugate of every involution of G. This yields:

Lemma 3.5. *If $G = \mathrm{SU}_{2n+1}(q)$, then G contains a broad subgroup.*

3.2. **Orthogonal Groups.** We now consider $G = \Omega^{\epsilon}_{2n}(q) = \Omega(V)$. Since $\Omega^{\epsilon}_{4}(q)$ is either isomorphic to a product of two copies of $\mathrm{SL}_2(q)$ or to $\mathrm{SL}_2(q^2)$ and $\Omega^{\epsilon}_{6}(q)$ is isomorphic to a quotient of $\mathrm{SL}_4(q)$ or $\mathrm{SU}_4(q)$, we assume that $n \geq 4$. This case is different from the other families of classical groups and we have to examine the conjugacy classes of involutions more closely.

Suppose that $n = 2m$ is even. Decompose $V = V_1 \perp \ldots \perp V_m$ as the orthogonal sum of m nondegenerate 4-dimensional spaces. If $\epsilon = +$, choose all the summands to be of $+$ type. Otherwise choose $V_1, \ldots, V_{m-1}$ of $+$ type and V_m to be of $-$ type.

Lemma 3.6. *Let E be a Sylow 2-subgroup of $\Omega(V_1) \times \ldots \times \Omega(V_m)$. Then E is a broad subgroup.*

Proof. Note that E is elementary abelian and that the normalizer of E contains elements in $\mathrm{O}(V)$ not in $\Omega(V)$. Thus it suffices to show that E intersects every $\mathrm{O}(V)$ conjugacy class of involutions contained in $\Omega(V)$. Such involutions are described in [10, Chap. 6]. The possible conjugacy classes are labelled $W(2)^e \oplus W(1)^f$ or $V(2)^2 \oplus W(2)^e \oplus W(1)^f$. They are distinguished by their Jordan form and whether (gv, v) vanishes identically for $v \in V$ with respect to the alternating form left invariant by G (the classes involving $V(2)^2$ are the ones where this function does not vanish everywhere).

Note that involutions in $\Omega^{+}_{4}(q)$ are either $W(2)$ or $V(2)^2$. Involutions in $\Omega^{-}_{4}(q)$ are in the class $V(2)^2$. If $\epsilon = +$, then it is clear any class of involutions intersects E. Similarly if $\epsilon = -$, it is clear that any involution other than $W(2)^m$ is conjugate to an element of E. However, this class of involutions in the algebraic group is not invariant under the graph automorphism (i.e. there are two Ω classes which are fused in O). Since the classes are stable under any field automorphism, it follows that this class is not present in $\Omega^{-}_{2n}(q)$. $\square$

If n is odd, decompose $V = W \perp U$ with $\dim U = 2$ and W of $+$ type (and so U has the same type as V).

Lemma 3.7. *Any involution in G is conjugate to an element of $\Omega(W)$ and so G contains a broad subgroup*

Proof. By [10, Chap. 6], any involution in G is conjugate to an element in $\Omega(W)$ and since $\Omega(W)$ contains a broad subgroup by the previous result, so does G. $\square$

3.3. **Exceptional Groups.** First observe that the groups ${}^2B_2(2^{2a+1})$, ${}^3D_4(2^a)$, ${}^2F_4(2^{2a+1})'$ or $G_2(q)$ have at most 1 non 2-central conjugacy class of involutions [10, Chap. 22] and the theorem holds as noted above. In addition, since centralizers of involutions are connected by Lemma 3.1, all classes of involutions intersect a subfield group and so one can work over the prime field (and so use the character tables).

In $F_4(q)$, the center of a Sylow 2-subgroup has order q^2 and intersects three of the four classes of involutions and so the result holds in this case as well. This can be seen deduced by noting that centralizers of representatives of elements in three classes of the classes have odd index. Alternatively, one can show that there are four classes of involutions in $\mathrm{Sp}_6(q)$ that are not fused in $F_4(q)$ and so the result for $\mathrm{Sp}_6(q)$ implies the result for $F_4(q)$.

It is easy to see that each conjugacy class of involutions in ${}^2E_6(q)$ or $E_6(q)$ intersects $F_4(q)$. For example, this can be seen by inspecting the tables in [10, Chap. 22] – indeed they exhibit the classes of unipotent elements in the exceptional groups by first working in E_8 and then determining which classes intersect the smaller groups and if they split. Alternatively, using the Jordan block structure of involutions of F_4 acting on the Lie algebra and the 26 dimensional module [8] and noting that the Lie algebra of E_6 as an F_4-module is the direct sum of the Lie algebra of F_4 and the 26-dimensional module, one can see that three of the classes in F_4 remain distinct in E_6. Thus, the result for these cases follows from the result for F_4.

In $E_7(q)$, we see that we can choose 4 commuting simple root subgroups (using the Bourbaki labelling, the roots are $\beta_2, \beta_3, \beta_5$ and β_7) and the group generated by these meets all four classes (see [1] or [8]). Each class of involutions in $E_8(q)$ intersects $E_7(q)$ (arguing as in the case of $F_4(q) < E_6(q)$). Thus, the theorem holds for $E_7(q)$ and $E_8(q)$.

3.4. **Exceptional Multipliers.** If G is a simple group of Lie type in characteristic 2, then almost always its Schur multiplier has odd order and so there is nothing more to do. There are a handful of cases where this fails. See [6, Table 6.1.3]. In each of the cases, one produces the required broad subgroup using GAP [2, 5].

4. Groups of Lie type in odd characteristic

In this section, we consider finite simple groups of Lie type over a field $\mathbb{F}_q$ with q odd. We prove a slightly stronger result which makes the proof easier. So let X be a simple algebraic group over an algebraically closed field of odd characteristic p. Let σ be a Steinberg endomorphism of X and let $H = X_\sigma$ the fixed points of σ. Then H is a finite group of Lie type over a finite field $\mathbb{F}_q$ for some q a power of p. Let $G = O^{p'}(H)$. Then G is quasi-simple unless $H = {}^2G_2(3), \mathrm{SL}_2(3)$ or $\mathrm{PGL}_2(3)$. Note that in the latter two cases G is solvable and in the first case $[H, H] \cong \mathrm{PSL}_2(8)$. We may exclude these cases.

We say that a subgroup S of H is toral if S is contained in a torus T in X. It follows that S is contained in a maximal torus of H (which is defined to be T_σ for T a σ-invariant maximal torus of X). Note that if $\phi : X \to Y$ is an isogeny of algebraic groups, then tori map to tori and the inverse image of a maximal torus is a maximal torus.

We shall prove the following:

Theorem 4.1. *Let G be a finite quasi-simple group of Lie type over a field of odd characteristic. Then there exists a toral subgroup of G which intersects every conjugacy class of involutions of G.*

If G is as in the theorem and Z is a central subgroup, then the result for G/Z implies the result for G (since as noted above toral subgroups lift to toral subgroups and any involution in G maps to an involution in G/Z). On the other hand, if we prove that there exists a toral subgroup S of G such that S intersects every conjugacy class of 2-elements $g \in G$ with $g^2 \in Z$, then SZ/Z is toral and intersects each class of involutions in G/Z. Thus, we can choose a particular form of the group and prove the result needed for that form.

If G is simply connected and split (i.e. σ is just a Frobenius endomorphism), the result is quite easy. Note that $G = X_\sigma$ in this case.

Lemma 4.2. *Let G be a finite quasi-simple simply connected split group of Lie type over the field of q elements. Let S be a maximal torus of G contained in a Borel subgroup of G. Then S intersects every conjugacy class of involutions of G.*

Proof. Let T be a maximal torus of X containing S. Every involution of X is conjugate to an element of T (indeed every semisimple element of X is conjugate to an element of T). If r is the rank of X, then S is a direct product of r copies of a cyclic group of order $q-1$ and thus S contains all involutions in T. Let $g \in G$ be an involution and note that g is conjugate in X to some element of S. Since X is simply connected, $C_X(g)$ is connected and $g^X \cap G = g^G$. Thus g is conjugate in G to an element of S. □

We can now complete the proof for the exceptional groups. The previous lemma implies the result for the simply connected groups of type $G_2(q)$, $F_4(q)$, $E_6(q)$, $E_7(q)$ and $E_8(q)$. Aside from the case of $E_7(q)$, the centers are either trivial or have order 3 and so the result holds.

We note that in the simply connected group $E_7(q)$, there are maximal tori that are direct products of seven cyclic groups of order $q-1$ and also of order $q+1$ [9, Section 5]. Arguing as above, one of these maximal tori contains a conjugate of any element of order 4 in G and so of any element whose square is central.

This leaves only the cases of ${}^2G_2(3^{2k+1}), k \geq 1$, ${}^3D_4(q)$ and ${}^2E_6(q)$. In the first two cases, there is only one class of involutions and the result follows since any semisimple element is contained in some maximal torus. In the case of ${}^2E_6(q)$ (and since the center has odd order, it suffices to consider the simply connected case), there is a maximal torus that is the direct product of six copies of the cyclic group of order $q+1$ [9, Section 5]. This contains all involutions of a maximal torus of the algebraic group and we argue as above.

We next consider the classical groups. We will work with the form of the group that acts on the natural module V.

We first consider $\mathrm{SL}_n(q)$. If n is odd, the center has odd order and so the result follows by Lemma 4.2. We next handle the case that n is even.

Lemma 4.3. *Let $G = \mathrm{SL}_{2m}(q) \leq \mathrm{GL}_{2m}(q) = L$. Then there exists a toral subgroup A of L such that A contains a conjugate of any element of G whose square is central.*

Proof. Note that semisimple elements in G which are conjugate in L are already conjugate in G. Let Z be the Sylow 2-subgroup of the center of G with z a generator. Consider the subgroup $B = B_1 \times \ldots \times B_m$ of L with each $B_i \cong \mathrm{GL}_2(q)$, acting on a direct sum of m two dimensional spaces. Let A_i be a cyclic subgroup of B_i of order q^2-1 and set $A = A_1 \times \ldots \times A_m$. Note that A contains an element w with $w^2 = z$ (by considering the two dimensional case). Suppose that $y^2 = z^i$ with $y \in G$. If i is odd, then there is an odd power of y with square z and so y is conjugate to a power of w. If $i = 2j$, then yz^{-j} is an involution in G. It is easy to see that an involution in G is conjugate to an element of A (since each eigenspace is even dimensional). Thus, A contains a conjugate of every element of G whose square is central. Clearly A is toral and so the result holds. □

As we noted above, this implies that Theorem 1 holds for any quotient of SL.

The same proof holds for $G = \mathrm{SU}_{2m}(q), m \geq 2$ and so the main result for any quotient of $\mathrm{SU}_{2m}(q)$. If $G = \mathrm{SU}_n(q)$ with n odd, then $Z(G)$ has odd order and we see that there is a toral subgroup that is a direct product of $n-1$ copies of a cyclic group of order $q+1$ which contains all involutions in a maximal torus of the algebraic group and the result follows as above. Thus, we have proved:

Lemma 4.4. *Let $G = \mathrm{SU}_n(q), n > 2$. Then Theorem 1 holds for any quotient of G.*

Lemma 4.5. *Theorem 1 holds for any quotient of $G = \mathrm{Sp}_{2n}(q)$.*

Proof. First suppose that $G = \mathrm{Sp}_{2n}(q)$ with $q \equiv 1 \pmod 4$. Then the split torus S contains all elements of order dividing 4 in the maximal torus T containing it in the algebraic group. Thus every element of order dividing 4 in G is conjugate to an element of S. Since G is simply connected, two elements of S which are conjugate in the algebraic group are already conjugate G, whence the results holds for $\mathrm{Sp}_{2n}(q)$ and its central quotient. If $q \equiv 3 \pmod 4$, there is a maximal torus of G that is the direct product of n copies of the cyclic group of order $q+1$ which again contains all elements of order dividing 4 in a maximal torus of the algebraic group and the result follows similarly. □

Finally we consider the quasi-simple groups related to orthogonal groups in dimension at least 7. We will prove the appropriate result for the groups $G = \Omega_n^{\epsilon}(q) \leq L = \mathrm{SO}_n^{\epsilon}(q)$. As noted above, this suffices to prove the result in general.

Lemma 4.6. *Theorem 1 holds for any quotient of* $\mathrm{Spin}_n^{\epsilon}(q)$ *for* $n \geq 7$.

Proof. First suppose that $n = 2m+1$ is odd. Then $\mathrm{SO}_n(q) = \mathrm{SO}(V)$ has trivial center and the simple group $\Omega_n(q)$ consists of the elements with spinor norm 1 and has index 2. Decompose $V = W \perp W^{\perp}$ with W a hyperplane such that the central element in $\mathrm{SO}(W)$ has spinor norm 1. Now decompose $W = W_1 \perp \ldots \perp W_m$ as an orthogonal sum of m nondegenerate 2-spaces with at least one summand of each type. If g is an involution in $\Omega_n(q)$, then g is conjugate to an element of the maximal torus $S = \mathrm{SO}(W_1) \times \ldots \times \mathrm{SO}(W_m)$. If the dimension of the trivial eigenspace of g is greater than 1, this is clear since the class of g (for g an involution even in $\mathrm{SO}(V)$) is determined by the dimension and type of its fixed space. If the fixed space of g is 1-dimensional and g has spinor norm 1, then the -1 eigenspace of g has the same type as W and so g is conjugate to the element acting as -1 on W. Thus, $S \cap \Omega_n(q)$ is a toral subgroup intersecting each conjugacy class of involutions and the result holds.

Next consider the case that $n = 4m+2, m \geq 2$. First consider the case that $L = \mathrm{SO}_n^{\epsilon}(q) = \mathrm{SO}(V)$ with $q \equiv \epsilon 1 \pmod 4$. Note that $Z(L) = Z(G)$ has order 2 in this case. Decompose $V = V_1 \perp \ldots \perp V_{2m+1}$ where the V_i are 2-dimensional spaces of the same type as V. Let $S = \mathrm{SO}(V_1) \times \ldots \times \mathrm{SO}(V_{2m+1})$. Then S is a maximal torus of $\mathrm{SO}(V)$. It is easy to see that any involution of spinor norm 1 is conjugate to an element of S. Moreover, if $x \in G$ and $x^2 = -I$, then x is conjugate to an element of S (reduce to the two dimensional case).

Thus, $S \cap \Omega(V)$ intersects any conjugacy of elements of G whose square is central. This proves the theorem for $\Omega(V)$ and its simple quotient and so the result holds.

Suppose that $q \equiv \epsilon 3 \pmod 4$. In this case the involution in $Z(L)$ has spinor norm -1 and so $\Omega(V)$ has trivial center and is the simple group. Decompose $V = V_1 \perp \ldots \perp V_{2m+1}$ so that there are at least 2 summands of each type. Let $S = \mathrm{SO}(V_1) \times \ldots \times \mathrm{SO}(V_{2m+1})$. Then S intersects every conjugacy class of involutions of $\mathrm{SO}(V)$ and the result holds.

Finally consider the case that $n = 4m, m \geq 2$. Suppose that $L = \mathrm{SO}_n^-(q) = \mathrm{SO}(V)$. Note that in this case $-I$ has spinor norm -1 and so $\Omega_n^-(q)$ is simple. Decompose $V = V_1 \perp \ldots \perp V_{2m}$ into an orthogonal sum of $2m$ nondegenerate 2-dimensional spaces (note both types must occur in this decomposition). It is clear that any involution in $\Omega(V)$ is conjugate to an element of $S = \mathrm{SO}(V_1) \times \ldots \times \mathrm{SO}(V_{2m})$ and the result holds.

Finally suppose that $L = \mathrm{SO}_n^+(q)$. Decompose $V = V_1 \perp \ldots \perp V_{2m}$ with each V_i of dimension 2 and all of the same type. If $q \equiv 1 \pmod 4$, take the type of V_i to be $+$ and $-$ otherwise. In this case the central involution of each $\mathrm{SO}(V_i)$ has spinor norm 1 and so the central involution in L also has spinor norm 1. Set $S = \mathrm{SO}(V_1) \times \ldots \times \mathrm{SO}(V_{2m})$, a direct product of $2m$ cyclic groups of order $q \pm 1$ (and each cyclic group has order a multiple of 4). If $x \in G$ and $x^2 = -I$, then x is conjugate to an element of S and any involution of spinor norm 1 is also conjugate to an element of S and the result follows. □

The proof of Theorem 1 is now complete.

5. Proof of Corollary 3

As mentioned in the introduction, Corollary 2.11 of R. Knörr [7] tells us that when p is a prime and G is a finite group of order divisible by p, then the irreducible character

χ of G lies in a p-block of defect zero of G (hence vanishes on all elements of G of order divisible by p) if and only if χ vanishes on all elements of order p in G. Hence when G has an elementary abelian subgroup E which meets every conjugacy class of elements of order p of G, the irreducible character χ lies in a p-block of defect zero of G if and only if χ vanishes identically on $E^{\#}$, the set of non-identity elements of E.

We may conclude, using Theorem 1 of [11], that if G has such an elementary abelian p-subgroup E, then $\sum_{a \in E^{\#}} |\chi(a)|^2 \geqslant |E| - 1$ whenever χ lies in a p-block of positive defect of G.

Using the orthogonality relations, we deduce that if G has k_+ irreducible characters lying in p-blocks of positive defect, we have

$$\sum_{a \in E^{\#}} |C_G(a)| \geqslant k_+(|E| - 1).$$

In particular, we have $k_+ \leqslant |C_G(a)|$ for some $a \in E^{\#}$.

More generally, let G be a finite group, and $N \lhd G$. We will first prove that if N has an elementary abelian p-subgroup E which meets every conjugacy class of elements of order p of N, then there is an element x of order p in N such that at most $|C_G(x)|$ irreducible characters of G lie in p-blocks which do not cover p-blocks of defect zero of N.

We first need a slight extension of the above result of Knörr.

Lemma 5.1. *Let G be a finite group and N be a normal subgroup of G. Let B be a p-block of G with defect group D such that $D \cap N \neq 1$. Then for any irreducible character $\chi \in B$, there is an element $x \in N$ of order p with $\chi(x) \neq 0$.*

Proof. Let (R, K, F) be a p-modular system for G. We note that $H = N_G(D \cap N) \geqslant N_G(D)$ so by Brauer's First Main Theorem, there is a unique Brauer correspondent block for B in $N_G(D \cap N)$, say B'. Let $\sigma = \sum_{\{n \in N : n^p = 1\}} n$, which is an element of $Z(RG)$. Here ω_χ denotes the linear character of $Z(RG)$ associated to the irreducible character χ and $J(R)$ is the unique maximal ideal of the complete dvr R.

We claim that $\omega_\chi(\sigma) \in J(R)$, so that $\omega_\chi(\sigma - 1_G) \notin J(R)$, and in particular, there must be some non-identity element $x \in N$ of order p with $\chi(x) \neq 0$.

Now, using the Brauer homomorphism, there is an irreducible character $\mu \in B'$ (which may be assumed to have $D \cap N$ in its kernel) such that $\omega_\chi(\sigma) \equiv \omega_\mu(\sigma^*) \pmod{J(R)}$, where $\sigma^* = \sum_{\{n \in C_G(D \cap N) : n^p = 1\}} n$.

However, let $Z = \Omega_1(Z(D \cap N))$, and let Z^+ be the sum of its elements in RG. It is clear that $\sigma^* = Z^+ T$ for some element T of $RC_G(D \cap N)$ which is itself a sum of certain elements of order dividing p. Notice that T commutes with Z^+. It follows that σ^* has nilpotent image in $Z(FN_G(D \cap N))$, so that $\omega_\mu(\sigma^*) \in J(R)$, which suffices to complete the proof. □

We conclude from the lemma (and Clifford's Theorem) that the irreducible character χ of G lies over characters in p-blocks of positive defect of N if and only if $\chi(x) \neq 0$ for some element x of order p in N.

In particular, if E is a broad elementary abelian p-subgroup of N, then no irreducible character χ of G which lies over irreducible characters in p-blocks of positive defect of N can vanish identically on $E^{\#}$. We may then conclude as above that there is an element x of order p in N such that the total number of irreducible characters of G which do not vanish identically on p-singular elements of N is at most $|C_G(x)|$.

Recall that $O(G)$ is the maximal odd order normal subgroup of G. Finally, we turn our attention to the case $p = 2$, $O(G) = 1$ and $N = F^*(G)$. If $O_2(G) \neq 1$, let $Z = \Omega_1(Z(O_2(G))) \neq 1$. Then by Clifford's Theorem, whenever χ is an irreducible character of G, $\mathrm{Res}^G_Z(\chi)$ is not a multiple of the regular character, so that χ does not vanish identically on $Z^{\#}$. Hence, as before, we have $\sum_{z \in Z^{\#}} |\chi(z)|^2 \geqslant |Z| - 1$, and we have $k(G) \leqslant |C_G(z)|$ for some z of order 2 in Z, where (as usual), $k(G)$ denotes the number of complex irreducible characters of G.

Suppose then that $O_2(G) = 1$. Then $F^*(G)$ is a direct product of non-abelian simple groups, and $F^*(G)$ has a broad elementary 2-subgroup, say E, by Theorem 1 and the remarks following. Now the arguments above tell us that there is some element $t \in E^{\#}$ such that the number of irreducible characters of G which do not vanish identically on 2-singular elements of $F^*(G)$ is at most $|C_G(t)|$, and the proof of Corollary 3 is complete.

Note that Corollary 3 shows that the number of irreducible characters of G which do not vanish identically on 2-singular elements of $F^*(G)$ is bounded above by the order of a 2-local subgroup of G which is the normalizer of a non-trivial 2-subgroup of $F^*(G)$. We remark that if equality holds in Corollary 3, then every irreducible character of G which does not vanish at t takes value ± 1 at t, and that each such character has odd degree, so lies in a 2-block of full defect of G (and has height zero in that block).

6. Further character-theoretic applications

One of our motivations for asking the question answered by Corollary 2 is the following:

Lemma 6.1. *Let G be a finite group, and let t, u be involutions of G such that t does not commute with any G-conjugate of u. Let $C = C_G(t)$ and $D = C_G(u)$. Then there is a non-trivial irreducible character μ in the principal* 2*-block of G such that $\mu(t)\mu(u) \neq 0$ and $\mu(1) \leqslant ([C : O(C)] - 1)(\sqrt{[D : O(D)] - 1})$.*

Proof. We first note that u is not expressible as the product of two conjugates of t. More generally, the product of two conjugates of t never lies in the 2-section of u, for if $t^x t^y$ has 2-part u^z, then t^x and t^y both invert the involution u^z, contrary to hypothesis.

By the usual character-theoretic formula for the coefficient of g in the product of two class sums, we see that the class function

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)^2 \chi}{\chi(1)}$$

vanishes identically on the 2-section of u in G.

By a well-known consequence of Brauer's Second Main Theorem, the class function

$$\sum_{\chi \in B} \frac{\chi(t)^2 \chi}{\chi(1)}$$

also vanishes identically on the 2-section of u in G, where B is the principal 2-block of G. It follows easily that

$$\sum_{1 \neq \chi \in B} \frac{\chi(t)^2 |\chi(u)|}{\chi(1)} \geqslant 1.$$

Choose a non-trivial irreducible character $\mu \in B$ with $\mu(t)\mu(u) \neq 0$ and with $r(u) = \frac{|\mu(u)|}{\mu(1)}$ maximal. Then

$$\sum_{1 \neq \chi \in B} \chi(t)^2 \geqslant \frac{1}{r(u)}.$$

By Brauer's Second and Third Main Theorem, we have

$$\sum_{\chi \in B} \chi(t)^2 = \sum_{\theta \in b} \theta(1)^2,$$

where b is the principal 2-block of $C = C_G(t)$. Since each irreducible character θ of b has $O(C)$ in its kernel, we deduce that

$$\sum_{1\neq\chi\in B} \chi(t)^2 \leqslant [C : O(C)] - 1.$$

A similar argument with u certainly allows us to conclude that $|\mu(u)| \leqslant \sqrt{[D : O(D)] - 1}$. Hence we may conclude that

$$\mu(1) \leqslant ([C : O(C)] - 1)(\sqrt{[D : O(D)] - 1}),$$

and the result follows. □

In view of Corollary 2, this result may not be applied as it stands to finite simple groups, but we have seen that the hypotheses may be satisfied within almost simple groups, so we mention:

Corollary 6.2. *Let G be an almost simple group with $F^*(G) = S$, and let t be an involution of $G\backslash S$ and u be an involution of S which commutes with no conjugate of t. Then the principal 2-block of S contains a t-stable non-trivial irreducible character of degree at most $([C : O(C)] - 1)(\sqrt{[D : O(D)] - 1})$, where $C = C_S(t)$ and $D = C_S(u)$.*

Proof. We might as well work within $\langle t\rangle S$, so we suppose that $G = \langle t\rangle S$. We may argue in a similar fashion to the previous result. Now the principal 2-block of G contains two linear characters, 1 and λ, say, and we also have $\lambda(t)^2\lambda(u) = 1$. This time, we find that

$$\sum_{\chi\in B:\chi(1)>1} \frac{\chi(t)^2|\chi(u)|}{\chi(1)} \geqslant 2,$$

where B is again the principal 2-block of G. However, the irreducible characters $\chi \in B$ with $\chi(t)\chi(u) \neq 0$ come in pairs, both members of which lie over the same t-stable irreducible character of the principal 2-block of S (if χ is one such, so is $\lambda\chi \neq \chi$, and note that $\chi(t)^2\chi(u)$ is unchanged on replacing χ by $\lambda\chi$). Also, $C_G(t) = \langle t\rangle \times C_S(t)$, so the result follows in a fashion similar to the previous corollary. □

References

[1] M. Aschbacher and G. Seitz, Involutions in Chevalley groups over fields of even order, Nagoya Math. J. 63 (1976), 1–91.

[2] T. Breuer, `https://urldefense.com/v3/__http://www.math.rwth-aachen.de/*Thomas.Breuer/ctbllib/doc/chap2_mj.html*X7AD5E36B7D44C507__;fiM!!LIr3w8kk_Xxm!9FyxtBR62DLbgSaALoeqxKzN5fQqo8yGp4x_86c5w7qJ-w6OkWODg8DhxKBDKHk$`

[3] M. Costantini, A classification of unipotent spherical conjugacy classes in bad characteristic, Trans. Amer. Math. Soc. 364 (2011), 1997–2019.

[4] J. Fulman, R. Guralnick and D. Stanton, Asymptotics of the number of involutions in finite classical groups, J. Group Theory 20 (2017), 871–902.

[5] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1; 2021. (https://www.gap-system.org)

[6] D. Gorenstein, R. Lyons and R. Solomon, The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups. Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.

[7] R. Knörr, Virtually irreducible lattices, Proc. London Math. Soc. 59 (1989), 99-132.

[8] R. Lawther, Jordan block sizes of unipotent elements in exceptional algebraic groups, Comm. Algebra 23 (1995), 4125–4156.

[9] M. Liebeck, J. Saxl and G. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, Proc. London Math. Soc. 65 (1992), 297–325.

[10] M. Liebeck and G. Seitz, Unipotent and nilpotent classes in simple algebraic groups and Lie algebras, Mathematical Surveys and Monographs, 180. American Mathematical Society, Providence, RI, 2012.

[11] G.R. Robinson, More bounds on norms of generalized characters with applications to p-local bounds and blocks, Bull. London Math. Soc. 37 (2005), 555–565.

R.M. Guralnick, Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA

Email address: guralnic@usc.edu

G. R. Robinson, Department of Mathematics, King's College, Aberdeen, AB24 3FX, UK

Email address: g.r.robinson@abdn.ac.uk