

PRODUCTS OF CONJUGACY CLASSES AND FIXED POINT SPACES

ROBERT GURALNICK AND GUNTER MALLE

ABSTRACT. We prove several results on products of conjugacy classes in finite simple groups. The first result is that for any finite nonabelian simple groups, there exists a triple of conjugate elements with product 1 which generate the group. This result and other ideas are used to solve a 1966 conjecture of Peter Neumann about the existence of elements in an irreducible linear group with small fixed space. We also show that there always exist two conjugacy classes in a finite nonabelian simple group whose product contains every nontrivial element of the group. We use this to show that every element in a nonabelian finite simple group can be written as a product of two r th powers for any prime power r (in particular, a product of two squares answering a conjecture of Larsen, Shalev and Tiep).

1. INTRODUCTION

Our first main result is the following:

Theorem 1.1. *Let G be a finite nonabelian simple group. There exists a conjugacy class C of G such that:*

- (1) *there is a triple of elements in C which have product 1 and generate G , and*
- (2) *there exist $x, y \in C$ that generate G such that xy is conjugate to x^2 unless G is a projective two-dimensional special linear group $L_2(q)$ with q even or $q = 7$.*

The exceptions in (2) are true exceptions. Indeed, we will see that any group satisfying Theorem 1.1(2) can have no irreducible two-dimensional representations.

We show that this has the following consequence.

Corollary 1.2. *Let G be a finite nonabelian simple group. Then there exists $g \in G$ with the following property. Whenever k is an algebraically closed field, and V a finite-dimensional kG -module without composition factors of dimension at most 2, then every eigenspace of g on V has dimension at most $(1/3) \dim V$.*

Note that the hypothesis that V has no two-dimensional composition factors is vacuous if the characteristic of k is not 2. For our intended subsequent application it is critical that the $g \in G$ that we choose does not depend on V . We also prove a variant of the previous corollary for direct products of finite simple groups.

If V is a G -module, let $C_V(g)$ denote the fixed space for $g \in G$. We use the previous result together with some recent results of the first author and Maróti [26] as well as an improvement in the solvable case to answer a conjecture of P. Neumann [45]:

Date: May 19, 2010; revised April 13, 2011.

1991 Mathematics Subject Classification. Primary 20C15, 20C20, 20D05.

The first author was partially supported by NSF grants DMS 0653873 and 1001962.

Theorem 1.3. *Let G be a nontrivial irreducible subgroup of $\mathrm{GL}(V)$, where V is a finite-dimensional vector space. There exists $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

This is Theorem 5.10. See Remark 5.9 for a short history of this problem. The example $G = \mathrm{SO}_3(k)$ on its natural module shows that $1/3$ is best possible. However, if the dimension of V is large enough, it seems likely that the bound of $1/3$ can be improved. Indeed, we prove (Theorem 6.1) that if $\epsilon > 0$, G is finite simple and V is an irreducible $\mathbb{C}G$ -module of sufficiently large dimension, then there exist $g \in G$ with all eigenspaces of dimension at most $\epsilon \dim V$. On the other hand we give examples for suitable nonsimple groups G of irreducible $\mathbb{C}G$ -modules V of arbitrarily large dimension such that $\dim C_V(g) \geq (1/9) \dim V$ for all $g \in G$ and even with V primitive and $\dim C_V(g) > (1/50) \dim V$ for all $g \in G$; see Examples 6.4 and 6.5.

We also extend some results of Malle–Saxl–Weigel [44] and Larsen–Shalev–Tiep [36] to prove another result about products of conjugacy classes.

Theorem 1.4. *Let G be a finite nonabelian simple group. There exist conjugacy classes C_1, C_2 in G with $G = C_1 C_2 \cup \{1\}$. Moreover, aside from $G = \mathrm{L}_2(q)$, $q = 7$ or 17 , we can assume that each C_i consists of elements of order prime to 6.*

This immediately implies that any element in a finite nonabelian simple group is the product of two m th powers for m a power of 6 (answering a conjecture of Larsen–Shalev–Tiep [36] for squares; the result on squares has also been obtained independently by Liebeck, O’Brien, Shalev and Tiep by other methods). Combining our methods with the main result of Chernousov–Ellers–Gordeev [7], we obtain:

Corollary 1.5. *Let G be a finite nonabelian simple group. Let m be either a prime power or a power of 6. Then every element of G is a product of two m th powers.*

The main result of [36] is a similar (but asymptotic) result for arbitrary words.

There is a related conjecture of Thompson that in fact $G = CC$ for some class C . Thompson’s conjecture is known to hold in many cases. See Ellers–Gordeev [12]. We show that if G is a finite simple group of Lie type of rank 1, then a very strong version of Thompson’s conjecture holds (see Theorem 7.1 for a precise statement). This shows that a version of the previous corollary holds for most words for the rank 1 groups. See Theorem 7.2 for a very strong result for the Suzuki and Ree groups.

Next, we extend some results of Breuer–Guralnick–Kantor [5] about the generation of finite simple groups. The proof depends upon knowledge of maximal subgroups as well as the ideas from the proof of Theorem 1.4.

An easy consequence (see Corollary 8.2) answers a question of Jayce Getz [19] in regard to an application to nonsolvable base change for automorphic representations of GL_2 :

Theorem 1.6. *Let S be a finite nonabelian simple group other than $\mathrm{O}_8^+(2)$. There exists a conjugacy class C of S consisting of elements whose order is prime to 6 such that if $1 \neq s \in S$, then $S = \langle g, s \rangle$ for some $g \in C$.*

The results in [5] show there is a conjugacy class C as above (but the elements in C may not have order prime to 6). It is proved there that the probability that a random element of C generates with s is typically large. If $S = \mathrm{O}_8^+(2)$, then one can take C to

consist of elements of order 15 (and so with no exceptions we can take C to be a class of elements of odd order).

We also show how our methods can be used to answer a conjecture of Bauer–Catanese–Grunewald [2, 3] regarding Beauville structures (this is related to the existence of certain free actions of a finite group acting on a product of two smooth projective curves; see [16] for background). The conjecture is that all nonabelian simple groups other than \mathfrak{A}_5 admit an unmixed Beauville structure. It has recently been proved by Garion–Larsen–Lubotzky [17] to hold at least asymptotically. In particular, we prove Theorem 8.6 that the groups $E_8(q)$ admit an unmixed Beauville-structure. In a sequel [25], we use our methods to solve the conjecture in the affirmative.

We now describe some of the main ingredients in the proofs of our main results. There usually are two parts: first, we need to show that triples of elements from specified conjugacy classes C_i and with product 1 exist in a given group G . There is a well-known character formula which counts the number of such triples, involving values of the complex irreducible characters of G on the C_i . In our situation, we choose the C_i such that only a few irreducible characters vanish simultaneously on all three classes. Then we may estimate the structure constant using Deligne–Lusztig theory, or for some small rank groups compute it from known character tables.

Secondly, we need to argue that some of these triples do generate G . So we will choose conjugacy classes C_i whose elements are contained in only a few maximal subgroups of G , and for which the character formula allows us to estimate the structure constant to be larger than the possible contributions from maximal subgroups. The most delicate case occurs in Theorem 1.1 where there is only one class to be chosen.

The paper is organized as follows. In Section 2, which may be of independent interest, we classify the maximal subgroups of the simple groups of Lie type containing certain elements with large irreducible submodules. In Section 3, we prove Theorem 1.1 for groups of Lie type. In Section 4, we complete the proof of that result for alternating and sporadic groups.

In Section 5, we prove Neumann’s conjecture, Theorem 1.3. In Section 6, we show a much stronger (asymptotic) version of the theorem for finite simple groups in characteristic zero. We also give examples to show that there are large dimensional examples (in all characteristics) where all fixed spaces are large. In Section 7, we prove Theorem 1.4 and Corollary 1.5. We also derive stronger results for the low rank groups of Lie type and a very strong result for the image of word maps for Suzuki and Ree groups. In the final section, we prove Theorem 1.6 and some corollaries including the application needed for nonsolvable base change for GL_2 . The final result is a proof that $E_8(q)$ admits a Beauville structure for all q .

We will use standard notation for the finite simple groups: for the exceptional groups (and their twisted analogs) we use the Lie notation; for the simple classical groups, we prefer to use the notation L , U , S and O^ϵ for the (projective special) linear, unitary, symplectic and orthogonal groups.

2. ZSIGMONDY PRIMES

Here we collect some results on subgroups of groups of Lie type containing large Zsigmondy prime divisors. If q is a prime power and $e > 2$ is a positive integer, we let $\Phi_e^*(q)$ be the largest divisor of $q^e - 1$ that is relatively prime to $q^m - 1$ for all $1 \leq m < e$. Note that every prime divisor of $\Phi_e^*(q)$ is congruent to 1 modulo e . By Zsigmondy's theorem, $\Phi_e^*(q) > 1$ unless $n = 6$ and $q = 2$ (and indeed, this is true for $e = 2$ as well unless q is a Mersenne prime). In particular, aside from that case, $\Phi_e^*(q) \geq e + 1$.

Hering [29] showed that usually $\Phi_e^*(q)$ is reasonably large (see Bamberg–Penttila [1, Lemma 6.1] for the version we are stating below and see Feit [13] as well).

Lemma 2.1. *Let q be a power of the prime p and $e > 2$ an integer.*

- (a) *If $\Phi_e^*(q) = 1$, then $q = 2$ and $e = 6$.*
- (b) *If $\Phi_e^*(q) = e + 1$, then $q = p$ and $q^e = 2^4, 2^{10}, 2^{12}, 2^{18}, 3^4, 3^6$ or 5^6 .*
- (c) *If $\Phi_e^*(q) = 2e + 1$, then either $q = 2$ and $e = 3, 8$, or 20 , or $q = 4$ and $e = 3$ or 6 .*

The main result of [28] was the classification of all subgroups of $\mathrm{GL}_n(q)$ whose order is divisible by some prime divisor of $\Phi_e^*(q)$ with $e > n/2$. The list becomes much shorter if we insist that this prime divisor is larger than $2e + 1$. The previous lemma indicates that almost always such a prime divisor exists.

Theorem 2.2. *Let $G = \mathrm{GL}(V) = \mathrm{GL}_n(q)$ where $q = p^a$ with p prime. Assume that $n > 2$. Let r either be a Zsigmondy prime divisor of $q^e - 1$ with $e > n/2$ and $r > 2e + 1$ or a product of two (not necessarily distinct) Zsigmondy prime divisors of $q^e - 1$. Suppose that H is an irreducible subgroup of G containing an element of order r . Then one of the following holds:*

- (1) *H contains $\mathrm{SL}(V)$, $\mathrm{SU}(V)$, $\Omega^{(\pm)}(V)$ or $\mathrm{Sp}(V)$;*
- (2) *H preserves an extension field structure on V (of degree f dividing $\mathrm{gcd}(n, e)$);*
- (3) *H normalizes $\mathrm{GL}_n(p^b)$ for some b properly dividing a ; or*
- (4) *H normalizes the subgroup H_0 given in Table 1.*

Proof. Under our assumptions, q has order greater than $n/2$ modulo r . The main result of [28] is that Examples 2.1–2.9 are all possibilities. We go through them one at a time.

The groups in Example 2.1 are those in cases (1) and (3). Example 2.2 gives only reducible groups. Examples 2.3 and 2.5 are excluded by the hypothesis that $r > 2e + 1$. Example 2.4 is case (2).

The rest of the possibilities are nearly simple groups. All the examples in [28] other than those in Table 1 are eliminated by the hypotheses. \square

Note that the condition on r is precisely that $r > 2e + 1$. If $r = 2e + 1$, there is a relatively short list of extra possibilities but for $r = e + 1$ there are many more examples.

We make this explicit in the following sections. Moreover, we will work with each of the classical groups and pick a specific e (depending upon the type of group and the dimension).

We also use the results of Hiss–Malle [30] and the Atlas [8] to help verify what subgroups embed in each classical group we consider.

TABLE 1. Subgroups with large Zsigmondy primes

| n | e | H_0 | condition | classical overgroup |
|-----|-----|--------------|----------------|--------------------------------|
| 4 | 4 | ${}^2B_2(q)$ | $q = 2^{2k+1}$ | Sp_4 |
| 6 | 6 | $G_2(q)$ | $p = 2$ | Sp_6 |
| 7 | 6 | $G_2(q)$ | $p \neq 2$ | O_7 |
| | | ${}^2G_2(q)$ | $q = 3^{2k+1}$ | O_7 |
| | | $U_3(q)$ | $p = 3$ | O_7 |
| 8 | 6 | $U_3(q)$ | $p \neq 3$ | O_8 |
| | | $SL_2(q^3)$ | always | Sp_8 (O_8 if q is even) |
| | | $Spin_7(q)$ | always | O_8 |
| 9 | 6 | $SL_3(q^2)$ | $q \neq 2$ | SL_9 |

2.1. **The special linear groups $SL_n(q)$.** Set $q = p^a$ and let $G = SL_n(q)$. We record the following results, which are immediate consequences of the results above and in [28].

Lemma 2.3. *Let $G = SL_n(q)$, $n > 2$, and set $e = n$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that $r > 2e + 1$ and that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. Then the only possible maximal subgroups containing an element of C are:*

- (1) the normalizer of $SU_n(q^{1/2})$ (if n is odd and q is a square);
- (2) the normalizer of $\Omega_n^-(q)$ (if n is even and q is odd);
- (3) the normalizer of $Sp_n(q)$ (if n is even); and
- (4) the normalizer of $GL_{n/f}(q^f) \cap G$ for f a prime divisor of n .

Moreover, such a class exists unless (n, q) is one of $(6, 2)$, $(4, 2)$, $(10, 2)$, $(12, 2)$, $(18, 2)$, $(4, 3)$, $(6, 3)$, $(6, 5)$, $(3, 2)$, $(8, 2)$, $(20, 2)$, $(3, 4)$ or $(6, 4)$.

Lemma 2.4. *Let $G = SL_n(q)$, $n > 3$, and set $e = n - 1$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that $r > 2e + 1$ and that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. Then the only possible maximal subgroups containing an element of C are:*

- (1) the normalizer of $SU_n(q^{1/2})$ (if n is even and q is a square);
- (2) the normalizer of $\Omega_n(q)$ (if nq is odd); and
- (3) the stabilizer of a 1-space or of a hyperplane.

Moreover, such a class exists unless possibly (n, q) is one of $(7, 2)$, $(5, 2)$, $(11, 2)$, $(13, 2)$, $(19, 2)$, $(5, 3)$, $(7, 3)$, $(7, 5)$, $(4, 2)$, $(9, 2)$, $(21, 2)$, $(4, 4)$ or $(7, 4)$.

The only $SL_n(q)$, $n > 2$, where neither of the previous lemmas applies are $SL_3(2)$, $SL_3(4)$ and $SL_4(2) \cong \mathfrak{A}_8$.

2.2. **The special unitary groups $SU_n(q)$.** The following two results are easy consequences of earlier results. Let $q = p^a$.

If n is odd, then we take $e = 2n$ and so the only special cases are when $\Phi_e^*(q) = 2n + 1$ or $4n + 1$, that is, (n, q) is one of $(5, 2)$, $(9, 2)$, $(3, 3)$, $(3, 4)$, or $(3, 5)$ by Lemma 2.1. In these cases we use [30] and [28] to check the possibilities. This gives:

Lemma 2.5. *Let $G = \mathrm{SU}_n(q)$, $n > 2$ and n odd, $(n, q) \neq (3, 2)$. Set $e = 2n$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. If M is a maximal subgroup of G containing an element of order r , then one of the following holds:*

- (1) M is the normalizer of $G \cap \mathrm{GU}_{n/f}(q^f)$, f an odd prime divisor of n ;
- (2) $(n, q) = (5, 2)$, C consists of elements of order 11 and M is the normalizer of $\mathrm{L}_2(11)$;
- (3) $(n, q) = (9, 2)$, C consists of elements of order 19, and M is the normalizer of J_3 ;
- (4) $(n, q) = (3, 3)$, C consists of elements of order 7, and $M = \mathrm{L}_2(7)$; or
- (5) $(n, q) = (3, 5)$, C consists of elements of order 7, and M is the normalizer of \mathfrak{A}_7 (3 classes fused in the automorphism group).

Similarly, if n is even, we take $e = 2(n - 1)$ and so the only problematic cases are when $\Phi_e^*(q) = 2n - 1$, $4n - 3$ or 1, so (n, q) is one of $(4, 2)$, $(6, 2)$, $(10, 2)$, $(4, 3)$, $(4, 4)$ or $(4, 5)$. Since $\Phi_6^*(2) = 1$, we have to exclude the case $(4, 2)$.

Lemma 2.6. *Let $G = \mathrm{SU}_n(q)$ with $n > 2$, n even, $(n, q) \neq (4, 2)$. Set $e = 2(n - 1)$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. If M is a maximal subgroup of G containing an element of order r , then one of the following occurs:*

- (1) M is the stabilizer of a nondegenerate 1-space;
- (2) $(n, q) = (6, 2)$, C is a class of elements of order 11 and $M = M_{22}$ (3 classes);
- (3) $(n, q) = (4, 3)$, C is a class of elements of order 7, and $M = 4_2.\mathrm{L}_3(4)$ (2 classes) or $M = \mathfrak{A}_7$ (4 classes); or
- (4) $(n, q) = (4, 5)$, C is a class of elements of order 7, and $M = \mathfrak{A}_7$ (2 classes fused in $\mathrm{GU}_4(5)$).

Finally, we deal with $\mathrm{SU}_4(2)$. The maximal subgroups containing elements of order 5 are \mathfrak{S}_6 and $2^4.\mathfrak{A}_5$ (see [8]).

2.3. The odd-dimensional orthogonal groups $\Omega_{2n+1}(q)$.

Lemma 2.7. *Let $G = \Omega_{2n+1}(q)$, $q = p^a$, $n > 2$ and q odd. Let $e = 2n$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that $r > 2e + 1$ and that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. Let M be a maximal subgroup of G intersecting C . Then one of the following holds:*

- (1) M is the stabilizer of a nondegenerate 1-space;
- (2) $n = 3$, M is the normalizer of $G_2(q)$;
- (3) $n = p = 3$, M is the normalizer of $\mathrm{U}_3(q)$; or
- (4) $n = 3$, $q = 3^{2a+1}$ and M is the normalizer of a Ree group ${}^2G_2(q)$.

Moreover, such a class exists unless $(2n+1, q)$ is either $(7, 3)$ or $(7, 5)$. In those two cases, the additional possibilities are given in Table 2.

The entries in Table 2 can be proved using [8], resp. [30].

2.4. The symplectic groups $\mathrm{Sp}_{2n}(q)$. Applying the previous results gives:

TABLE 2. Further maximal subgroups of $\Omega_{2n+1}(q)$, $n \geq 3$

| $(2n+1, q)$ | M | # classes | r |
|-------------|---|------------|-----|
| $(7, 3)$ | $\mathfrak{S}_9, 2^6.\mathfrak{A}_7, \text{Sp}_6(2)$ | 2, 1, 2 | 7 |
| $(7, 5)$ | $\mathfrak{A}_8, 2^6.\mathfrak{A}_7, \text{Sp}_6(2), \text{U}_3(3).2$ | 2, 1, 2, 2 | 7 |

Lemma 2.8. *Let $G = \text{Sp}_{2n}(q)$, $q = p^a$, $n \geq 2$ with $(n, q) \neq (2, 2)$, and set $e = 2n$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that $r > 2e + 1$ and that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. Let M be a maximal subgroup of G intersecting C . Then one of the following holds:*

- (1) M is the normalizer of $\text{Sp}_{2n/f}(q^f)$ for f a prime divisor of n ;
- (2) nq is odd and M is the normalizer of $\text{SU}_n(q)$;
- (3) q is even and $M = \Omega_{2n}^-(q)$;
- (4) $n = 3$, q is even, and M is the normalizer of $G_2(q)$; or
- (5) $n = 2$, $q = 2^{2a+1}$, and M is the normalizer of a Suzuki group ${}^2B_2(q)$.

Moreover, such a class exists unless $(2n, q)$ is as in Table 3. In those remaining cases, the additional possibilities (for $r \mid \Phi_e(q)$) are listed in the table.

The entries in Table 3 follow by the results of [28, 30]. We excluded $\text{Sp}_4(2) \cong \mathfrak{S}_6$.

TABLE 3. Further maximal subgroups of $\text{Sp}_{2n}(q)$

| $(2n, q)$ | M | r | Remarks |
|-----------|-------------------------------------|-----|-------------------|
| $(4, 3)$ | $2^{1+4}.\mathfrak{A}_5$ | 5 | $\text{U}_4(2)$ |
| $(6, 2)$ | $2^6.\text{L}_3(2), \mathfrak{S}_8$ | 7 | $\Phi_6^*(2) = 1$ |
| $(6, 3)$ | $2.\text{L}_2(13)$ (2 classes) | 7 | |
| $(6, 4)$ | $\text{L}_2(13)$ | 13 | |
| $(6, 5)$ | $2.J_2, \text{U}_3(3)$ | 7 | |
| $(8, 2)$ | $\text{L}_2(17)$ | 17 | |
| $(10, 2)$ | none | 11 | |
| $(12, 2)$ | $\mathfrak{A}_{14}, \text{L}_2(25)$ | 13 | |
| $(18, 2)$ | none | 19 | |
| $(20, 2)$ | $\text{L}_2(41)$ | 41 | |

2.5. **The orthogonal groups of plus type $\Omega_{2n}^+(q)$.** Applying the previous results gives:

Lemma 2.9. *Let $G = \Omega_{2n}^+(q)$, $q = p^a$, $n > 3$, and set $e = 2n - 2$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that $r > 2e + 1$ and that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. Let M be a maximal subgroup of G intersecting C . Then one of the following holds:*

- (1) M is the stabilizer of a nondegenerate subspace of dimension 1 or 2;
- (2) nq is odd and M is the normalizer of $\Omega_n(q^2)$;

- (3) n is even, and M is the normalizer of $\mathrm{SU}_n(q)$; or
(4) $n = 4$ and M is the normalizer of $\mathrm{U}_3(q)$ (for $p \neq 3$) or $\mathrm{Spin}_7(q)$.

Moreover, such a class exists unless $(2n, q)$ is as in Table 4, where additional maximal subgroups arise as given.

TABLE 4. Further maximal subgroups of $\Omega_{2n}^+(q)$, $n \geq 4$

| $(2n, q)$ | M | # classes | r | Remarks |
|-----------|---|------------|-----|-------------------|
| $(8, 2)$ | $\mathfrak{A}_9, 2^6 : \mathfrak{A}_8$ | 3, 3 | 7 | $\Phi_6^*(2) = 1$ |
| $(8, 3)$ | $2.\mathrm{O}_8^+(2)$ | 4 | 7 | |
| $(8, 4)$ | none | | 13 | |
| $(8, 5)$ | $2.^2B_2(8), \mathfrak{A}_{10}, 2.\mathfrak{A}_{10}, 2.\mathrm{O}_8^+(2)$ | 8, 4, 8, 4 | 7 | |
| $(10, 2)$ | none | | 17 | |
| $(12, 2)$ | none | | 11 | |
| $(14, 2)$ | $\mathfrak{A}_{16}, \mathrm{L}_2(13), G_2(3).2$ | 1, 2, 2 | 13 | |
| $(20, 2)$ | $\mathrm{L}_2(19), J_1$ | 1, 1 | 19 | |
| $(22, 2)$ | none | | 41 | |

For the 8-dimensional groups we have used the results of Kleidman [33]. For $\Omega_{14}^+(2)$ there are two classes of $\mathrm{L}_2(13)$: first of all there are two different (not even quasi-equivalent) 14-dimensional representations and so at least two classes (and exactly two in the full orthogonal group). Note that both representations extend to $\mathrm{PGL}_2(13)$, which does sit in the full $\mathrm{GO}_{14}^+(2)$ but not in the simple group. (The easiest way to see this is that there is an element of order 4 normalizing the 13 in $\mathrm{PGL}_2(13)$, it permutes freely the 12 nontrivial eigenvalues of the element of order 13 and on the 2-dimensional fixed space it acts trivially since it commutes with the element of order 3 which is semisimple regular on that 2-space. Thus, it has 5 Jordan blocks, but unipotent elements are in the simple algebraic group if and only if they have an even number of Jordan blocks.) So there are two classes.

For $G_2(3)$, there is one class in the full orthogonal group $\mathrm{GO}_{14}^+(2)$ (since there is only one such representation) and it extends to $G_2(3).2$. The centralizer of an outer involution $x \in G_2(3).2$ (which is unique up to conjugacy) is $\mathrm{L}_2(8).3$. Since x commutes with an element y of order 9 that has precisely two eigenvalues of order 3, it must be trivial on the 2-dimensional space where $y^3 = 1$, and so it has at least 2 trivial Jordan blocks. If it had $t < 6$ Jordan blocks, then the reductive part of its centralizer (in $\mathrm{GL}_{14}(2)$) would be a direct product of a torus and $\mathrm{GL}_t(2)$ and so $\mathrm{L}_2(8).3$ would embed in $\mathrm{GL}_5(2)$, but the smallest faithful representation of $\mathrm{L}_2(8).3$ is 6-dimensional. So x has 6 nontrivial Jordan blocks and thus lies in $\Omega_{14}^+(2)$.

2.6. The twisted orthogonal groups $\Omega_{2n}^-(q)$. Applying the previous results gives:

Lemma 2.10. *Let $G = \Omega_{2n}^-(q)$, $q = p^a$, $n > 3$, and set $e = 2n$. Let C be a conjugacy class of elements of order r dividing $\Phi_e^*(q)$. Assume that $r > 2e + 1$ and that r is divisible by some prime divisor of $\Phi_{ae}^*(p)$. Let M be a maximal subgroup of G intersecting C . Then one of the following holds:*

- (1) M is the normalizer of $\Omega_{2n/f}^-(q^f)$ for f a prime divisor of n ; or
- (2) n is odd and M is the normalizer of $SU_n(q)$.

Moreover, such a class exists unless $(2n, q)$ is as in Table 5, where additional maximal subgroups arise as given.

TABLE 5. Further maximal subgroups of $\Omega_{2n}^-(q)$, $n \geq 4$

| $(2n, q)$ | M | r |
|-----------|--------------------------------------|-----|
| $(8, 2)$ | none | 17 |
| $(10, 2)$ | \mathfrak{A}_{12} | 11 |
| $(12, 2)$ | $\mathfrak{A}_{13}, L_2(13), L_3(3)$ | 13 |
| $(18, 2)$ | \mathfrak{A}_{20} | 19 |
| $(20, 2)$ | none | 41 |

2.7. The exceptional groups. We end this section by completing a result of Weigel [50] on maximal subgroups of exceptional groups of Lie type containing certain maximal tori.

Proposition 2.11. *Let G be a simple exceptional group of Lie type. Then there exists a cyclic subgroup $T \leq G$ such that $|T|$, $|N_G(T) : T|$ and the conjugacy classes of maximal overgroups $M \geq T$ in G are as given in Table 6.*

TABLE 6. Cyclic subgroups and maximal overgroups in exceptional groups

| G | $ T $ | $ A_G(T) $ | $M \geq T$ | further maximals |
|--------------------------------|------------------------------|------------|-------------------------------|--------------------------------------|
| ${}^2B_2(q^2)$, $q^2 \geq 8$ | Φ'_8 | 4 | $N_G(T)$ | — |
| ${}^2G_2(q^2)$, $q^2 \geq 27$ | Φ'_{12} | 6 | $N_G(T)$ | — |
| $G_2(q)$, $3 q + \epsilon$ | $q^2 + \epsilon q + 1$ | 6 | $SL_3(q).2$ | $L_2(13)$ ($q = 4$) |
| $G_2(q)$, $3 q$ | $q^2 + q + 1$ | 6 | $SL_3(q).2$ ($2 \times$) | $L_2(13)$ ($q = 3$) |
| ${}^3D_4(q)$ | $q^4 - q^2 + 1$ | 4 | $N_G(T)$ | — |
| ${}^2F_4(q^2)$, $q^2 \geq 8$ | Φ'_{24} | 12 | $N_G(T)$ | — |
| $F_4(q)$, $2 \nmid q$ | $q^4 - q^2 + 1$ | 12 | ${}^3D_4(q).3$ | |
| $F_4(q)$, $2 q$ | $q^4 - q^2 + 1$ | 12 | ${}^3D_4(q).3$ ($2 \times$) | ${}^2F_4(2), L_4(3).2_2$ ($q = 2$) |
| $E_6(q)$ | $\Phi_9/(3, q - 1)$ | 9 | $SL_3(q^3).3$ | — |
| ${}^2E_6(q)$ | $\Phi_{18}/(3, q + 1)$ | 9 | $SU_3(q^3).3$ | — |
| $E_7(q)$ | $\Phi_2\Phi_{18}/(2, q - 1)$ | 18 | ${}^2E_6(q)_{sc}.D_{q+1}$ | — |
| $E_8(q)$ | Φ_{30} | 30 | $N_G(T)$ | — |

Here, $A_G(T) := N_G(T)/C_G(T)$, $\Phi'_8 = q^2 + \sqrt{2}q + 1$, $\Phi'_{12} = q^2 + \sqrt{3}q + 1$, $\Phi'_{24} = q^4 + \sqrt{2}q^3 + q^2 + \sqrt{2}q + 1$.

The entry “($2 \times$)” signifies that there are two conjugacy classes of the indicated maximal subgroups.

Proof. The existence of cyclic tori of G of the given orders follows from the general theory of tori in finite reductive groups; see for example [6, §3.3]. In all cases T is (the image in G of) a self-centralizing maximal torus (of the corresponding finite reductive group of simply-connected type), and the order of the automizer $A_G(T) = N_G(T)/C_G(T)$ can be calculated from the Weyl group; see [6, Prop. 3.3.6].

The lattice of overgroups of T up to conjugation can be found in the work of Weigel [50, Sect. 4], except for

$$G \in \{G_2(q), F_4(2), F_4(3), {}^2E_6(2), {}^2E_6(3), E_7(2), E_7(3)\}.$$

The maximal subgroups of $G_2(q)$ were determined by Kleidman [34, Thm. A] and Cooperstein [9, Thm. 2.3]: for $q \geq 5$ the only maximal subgroups containing T are one class of $SU_3(q).2$ if $q \equiv 1 \pmod{3}$, respectively one or two classes of $SL_3(q).2$ else. For $G_2(3)$ and $G_2(4)$ there is one further class of maximal subgroups $L_2(13)$. The maximal subgroups of $F_4(2)$ and of ${}^2E_6(2)$ are printed in the Atlas [8]. According to the arguments given in [50, Sect. 4(f)], the only further overgroup of T in $F_4(3)$ could be a group with derived group isomorphic to $SU_3(9)$. But the latter group contains elements of order 80, while the centralizer of a 5-element in $F_4(3)$, of shape $C_{10}Sp_4(3)$ has no element of order 16 (see [8]). (This fact was pointed out to us by Frank Lübeck. Alternatively, one can show that the 25-dimensional module would have to split as $24 \oplus 1$ for such a subgroup, whence $SU_3(9)$ would have to be contained in the stabilizer ${}^3D_4(3).3$ of that 1-space.) It is shown in [40, Thm. 5.1] that no further overgroups of T arise in ${}^2E_6(3)$.

Now assume that $G = E_7(q)$ with $q = 2, 3$. If $q = 3$, then we take the cyclic maximal torus T of order 4×703 . If $q = 2$, T is cyclic of order 3×57 (by [6, Prop. 3.2.2]).

We claim that there is a unique maximal subgroup M of G containing T (with $M = {}^2E_6(q)_{sc}.D_{q+1}$). The proof is very similar in spirit to Weigel's proof and is based on various results of Liebeck and Seitz and others on the maximal subgroups of the exceptional Chevalley groups. See [38] for a summary of these results and various references.

Let H be a maximal subgroup of G containing T other than M . By [38, Thm. 3], H is an almost simple group. Let S denote its socle. It follows by [38, Table 2] that S must be a Chevalley group in the same characteristic as G . Moreover, by [38, Thm. 7], it follows that the (untwisted) rank of S is at most 3. Inspection of the groups of rank at most 3 defined over fields of size a power of q shows as in [50] that the only possibility is that $S = U_3(q^3)$. If $q = 3$, we can eliminate the latter case, since the automorphism group of S contains no elements of order $|T|$.

So assume that $q = 2$ and $F^*(H) = S = U_3(8)$. We will show that the normalizer of any subgroup of $E_7(2)$ isomorphic to S and containing an element x of order 19 in T is contained in M . Let V be the irreducible \mathbb{F}_2G -module of dimension 56. Let $T_0 = \langle x \rangle$ be the subgroup of T of order 19. Note that T_0 has a 2-dimensional fixed space on V , and so the fixed space of T_0 is the same as that of $M_0 = F^*(M)$. Since M acts transitively on those 3 points, it follows that the stabilizer of the vectors are the three subgroups of the form $M_0.2 < M$. Looking at the Brauer character table for $\mathbb{F}_2U_3(8)$ -modules and knowing that the element of order 19 has Brauer character -1 , it follows that if S exists, then V has three \mathbb{F}_2S -composition factors: one of dimension 54 and two trivial modules. Since V is self-dual, this implies that S has fixed points on V , whence $S \leq M$. If S has a 1-dimensional fixed space, then the normalizer of S also fixes this vector, whence is also

contained in M . If S has a 2-dimensional fixed space, then H is contained in the stabilizer of the 2-space and so again $H \leq M$. \square

Note that we proved a bit more for $E_7(2)$: even the cyclic subgroup of order 57 of T is only contained in one maximal subgroup of $E_7(2)$. We also note that Ryba [46] proved that $U_3(8).6$ in fact does embed in $E_7(2)$. It follows that in fact $U_3(8).6$ embeds in ${}^2E_6(q)_{sc}.D_{q+1}$.

3. GROUPS OF LIE TYPE

This section is devoted to the proof of Theorem 1.1 for finite simple groups of Lie type. We first give a sketch of the approach to be followed. Let G be a finite group, C a conjugacy class of G . If $a \in \mathbb{Z}$, let C^a be the conjugacy class $\{x^a | x \in C\}$. Then, for $a \in \mathbb{Z}$ and fixed $x \in C$ the number of pairs

$$n_a(C) := |\{(y, z) \in C \times C^a \mid xyz = 1\}|$$

in G is given by the well-known character formula

$$n_a(C) = \frac{|C|^2}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(C)^2 \chi(C^a)}{\chi(1)},$$

where the sum ranges over the complex irreducible characters of G and $\chi(C)$ denotes the value of χ on elements of C (see, for example, [43, Thm. I.5.8]).

Often, for G almost simple and C a large conjugacy class, the main contribution to this structure constant is by the terms coming from the linear characters of G . In our situation, the class C will be contained in the derived group G' , so all linear characters take value 1 on elements of C and C^a . Set $d := |G/G'|$, the number of linear characters of G . We'll write

$$\epsilon_a(C) := \frac{1}{d} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(C)^2 \chi(C^a)}{\chi(1)} - 1 = \frac{1}{d} \sum_{\chi(1) \neq 1} \frac{\chi(C)^2 \chi(C^a)}{\chi(1)},$$

so that

$$n_a(C) = d \frac{|C|^2}{|G|} (1 + \epsilon_a(C)) = d \frac{|G|}{|C_G(x)|^2} \cdot (1 + \epsilon_a(C))$$

for $x \in C$. So to show that there exist triples we need to prove that $|\epsilon_a(C)| < 1$. This can either be done using results from Deligne–Lusztig theory, or, for many small rank groups, using the known generic character tables which are available in the **Chevie**-package [18].

To prove generation, assume that H is a maximal subgroup of G containing x , and $C_H := C \cap H$. Then there are at most $|C_H|$ pairs of elements $y \in C_H$, $z \in H$, such that $xyz = 1$. So we will choose a conjugacy class C of elements whose order is divisible by a Zsigmondy prime as considered in the previous section, so which are contained in few maximal subgroups of G , and for which the value of $n_a(C)$ can be estimated from below by the character formula to be larger than the possible contributions from maximal subgroups.

3.1. Some character theory. We first recall some results on character values in finite groups of Lie type. Let \mathbf{G} be a connected reductive algebraic group over the algebraic closure of a finite field and $F : \mathbf{G} \rightarrow \mathbf{G}$ a Frobenius map, with finite group of fixed points $G = \mathbf{G}^F$. For \mathbf{T} an F -stable maximal torus of \mathbf{G} , with $T := \mathbf{T}^F$, and $\theta \in \text{Irr}(T)$ we denote by $R_{T,\theta}$ the corresponding Deligne–Lusztig character.

Lemma 3.1. *Let $x \in G$ be a semisimple element. Then we have:*

- (a) *If $R_{T,\theta}(x) \neq 0$, then $x \in T^g$ for some $g \in G$.*
- (b) *If x is regular, lying in the (unique) maximal torus T , then $R_{T,\theta}(x) = \pm \theta_T^G(x)$.*

Proof. Part (a) is clear from the character formula [6, Prop. 7.5.3]. For the second part, note that if x is regular, then it lies in a unique F -stable maximal torus, so $C_{\mathbf{G}}(x)^\circ = \mathbf{T}$. The Steinberg character St then takes value ± 1 on x by [6, Thm. 6.4.7], so the claim follows by the fact that $\text{St} \cdot R_{T,\theta} = \theta_T^G$ [6, Prop. 7.5.4]. \square

Let's translate this to the setting of Lusztig series of characters. For this let \mathbf{G}^* be a group in duality with \mathbf{G} , with corresponding Frobenius map $F^* : \mathbf{G}^* \rightarrow \mathbf{G}^*$ and group of fixed points $G^* := \mathbf{G}^{*F^*}$ (see [6, §4.3]). There is a bijective correspondence between G -conjugacy classes of pairs (T, θ) in G as above and G^* -classes of pairs (T^*, s) , where $T^* \leq G^*$ is a maximal torus in duality with T and $s \in T^*$ is semisimple (see [11, Prop. 13.13]). We will also write $R_{T^*,s}$ for $R_{T,\theta}$ if (T^*, s) corresponds to (T, θ) in this way. Then the Lusztig series $\mathcal{E}(G, s)$ is by definition the set of constituents of $R_{T^*,s}$ for T^* running over maximal tori of G^* containing s . Lusztig has shown that the $\mathcal{E}(G, s)$, with s running over semisimple elements of G^* modulo conjugation, form a partition of $\text{Irr}(G)$. With these definitions we have:

Lemma 3.2. *Let $x \in G$ be semisimple and $\chi \in \text{Irr}(G)$ with $\chi(x) \neq 0$. Then there exists a maximal torus $T \ni x$ of G and $s \in T^* \leq G^*$ such that $\chi \in \mathcal{E}(G, s)$.*

Proof. By the result of Lusztig, there is some $s \in G^*$ with $\chi \in \mathcal{E}(G, s)$. Since $\chi(x) \neq 0$ and the characteristic functions of semisimple classes are uniform, there exists a maximal torus $T^* \leq G^*$ with $s \in T^*$ such that $R_{T^*,s}(x) \neq 0$, so $R_{T,\theta}(x) \neq 0$ for some $\theta \in \text{Irr}(T)$. By Lemma 3.1, this implies that x lies in some conjugate of T . \square

Let's assume for what follows that \mathbf{G} has connected center, so that centralizers of semisimple elements in \mathbf{G}^* are connected (see [6, Thm. 4.5.9]). Let $W(s)$ denote the Weyl group of the centralizer $C_{\mathbf{G}^*}(s)$ of s in \mathbf{G}^* . The semisimple character of G corresponding to s is defined (up to sign) by

$$\chi_s := \frac{1}{|W(s)|} \sum_{w \in W(s)} \epsilon_w R_{T_w^*,s}$$

(with certain signs ϵ_w ; see [11, Def. 14.40]), where T_w^* denotes a maximal torus of $C_{\mathbf{G}^*}(s)$ (hence of G^*) parametrized by w in the sense of [6, Prop. 3.3.3]. By [6, Thm. 8.4.8] the degree of χ_s is given by

$$\chi_s(1) = |G^* : C_{G^*}(s)|_{p'},$$

the part of the index of $C_{G^*}(s)$ prime to the characteristic p of \mathbf{G} . The character χ_s is irreducible (see [11, Prop. 14.43]). We let $W(\theta) := N_G(\mathbf{T}, \theta)/T$ denote the stabilizer of θ in $W(T) := N_G(\mathbf{T})/T$.

Proposition 3.3. *Let $x \in G$ be regular, lying in the (unique) maximal torus T of G parametrized by $v \in W$. Let (T^*, s) correspond to (T, θ) , and assume that the intersection of the F -conjugacy class of v in W with $W(s)$ is a single F -conjugacy class in $W(s)$. Then*

$$\chi_s(x) = \pm \sum_{w \in W(T)/W(\theta)} \theta(x^w),$$

where the sum runs over a set of coset representatives of $W(\theta)$ in $W(T)$. In particular, $|\chi_s(x)| \leq |C_W(Fv) : C_{W(s)}(Fv)|$.

Proof. By assumption T is parametrized by the F -conjugacy class of $v \in W$. Since $x \in T$ is regular, by the definition of χ_s and Lemma 3.1 we have

$$\chi_s(x) = \frac{1}{|W(s)|} \sum_{w \sim v} \epsilon_v \theta_T^G(x),$$

where the sum extends over those $w \in W(s)$ for which T_w is G -conjugate to T , that is, the F -conjugates of v in $W(s)$. By assumption there are exactly $|W(s) : C_{W(s)}(Fv)|$ such conjugates, so

$$\chi_s(x) = \pm \frac{1}{|C_{W(s)}(Fv)|} \theta_T^G(x).$$

In order to evaluate $\theta_T^G(x)$ observe that for $g \in G$ we have $x^g \in T$ if and only if $x \in {}^gT$, that is, if $g \in N_G(T)$. Moreover $N_G(T) = N_G(\mathbf{T})$ since T contains the regular element x . Thus

$$\theta_T^G(x) = \frac{1}{|T|} \sum_{g \in N_G(\mathbf{T})} \theta(x^g) = \frac{1}{|T|} \sum_{g \in N_G(\mathbf{T})} {}^g\theta(x).$$

Then, with $W(T) = N_G(\mathbf{T})/T$ and $W(\theta) = N_G(\mathbf{T}, \theta)/T$ we have

$$\theta_T^G(x) = |W(\theta)| \sum_{w \in W(T)/W(\theta)} {}^w\theta(x) = |W(\theta)| \sum_{w \in W(T)/W(\theta)} \theta(x^w).$$

Since (T, θ) corresponds to (T^*, s) we have $W(\theta) \cong N_{G^*}(\mathbf{T}^*, s)/T^* \cong C_{W(s)}(Fv)$ (see [11, proof of Prop. 14.43]), so

$$\chi_s(x) = \pm \frac{1}{|C_{W(s)}(Fv)|} |W(\theta)| \sum_{w \in W(T)/W(\theta)} \theta(x^w) = \pm \sum_{w \in W(T)/W(\theta)} \theta(x^w).$$

□

Apart from these results from Deligne–Lusztig theory we also use the following result on blocks with cyclic defect groups: let B be a block with cyclic defect group P generated by x , say. Then the character values $\chi(x)$, for all nonexceptional characters χ in B , are the same up to sign.

3.2. The exceptional groups. We first consider the simple exceptional groups of Lie type. We postpone the treatment of the classical groups ${}^2G_2(3)' = L_2(8)$ and $G_2(2)' = U_3(3)$ until the next subsection, as well as the Tits group ${}^2F_4(2)'$, which will be considered in Section 4.

We show that not all triples of elements from a class of generators of the cyclic subgroup T as in Table 6 can lie in proper subgroups. For the five families of exceptional groups

of small rank, the character tables are known, so that lower bounds for the structure constant $n_a(C)$ can easily be obtained. Using Proposition 2.11 we can also estimate the contribution from maximal subgroups containing T from above. From this one gets:

Proposition 3.4. *Theorem 1.1 holds for the simple exceptional groups of Lie type ${}^2B_2(q^2)$, ${}^2G_2(q^2)$, $G_2(q)$, ${}^3D_4(q)$ and ${}^2F_4(q^2)$, with C containing generators of a cyclic subgroup $T \leq G$ as in Table 6.*

Proof. The character tables of all five families of groups are known explicitly and contained for example in the GAP-package Chevie [18]. With this system it is possible to compute structure constants generically, that is, for all prime powers q (in a fixed congruence class modulo 12) at the same time. For $G = {}^2B_2(q^2)$ one obtains with Chevie

$$n_a(C) = \frac{|G|}{|T|^2} \left(1 + \frac{4q^5 + 11\sqrt{2}q^4 + 6q^3 - 2q + \sqrt{2}}{\sqrt{2}(q^2 + \sqrt{2}q + 1)} \right) \geq \frac{|G|}{|T|^2}.$$

By Proposition 2.11 the only maximal subgroup M of G containing T is the normalizer $N_G(T)$, which contributes at most $|C_H| = |C \cap H| = 4$ triples.

Similarly, for $G = {}^2G_2(q^2)$ one finds that

$$n_a(C) \geq \frac{|G|}{|T|^2}.$$

The only maximal subgroup containing T , the normalizer $N_G(T)$, contains at most 6 of these triples.

For $G = G_2(q)$ one finds that for either congruence,

$$n_a(C) \geq \frac{1}{3}q^{10}.$$

For $q \geq 5$ the possible number of triples from the subgroups $SL_3^{\epsilon}(q).2$ is too small. For $G_2(3)$ we have $n_1(C) = 25456$, $n_{-2}(C) = 26185$, while the two classes of maximal subgroups $SL_3(3).2$ contain at most 133 triples each and the maximal subgroup $L_2(13)$ contains no more than 15 triples with fixed first component. Similarly, for $G_2(4)$ we have $n_1(C) = 1495561$, $n_{-2}(C) = 1499657$, while the maximal subgroups of type $SU_3(4).2$ and $L_2(13)$ contain at most $1380 + 15$ triples.

From the known character table of $G = {}^3D_4(q)$ one computes that

$$n_a(C) = |T|(q^{12} - 4q^6 + 1)(q^2 + 1)^2.$$

The only maximal subgroup containing T is the normalizer $N_G(T)$, contributing 4 triples.

From the known character table of $G = {}^2F_4(q^2)$ one finds that $n_a(C) \geq q^{42}$ when $q^2 \geq 8$. Again, the only maximal subgroup containing T is the normalizer $N_G(T)$, accounting for 12 triples. \square

For the larger exceptional groups, neither the character table nor the list of maximal subgroups is completely known. In order to estimate the structure constant $n_a(C)$ we use results from Deligne–Lusztig theory as explained above.

Proposition 3.5. *Theorem 1.1 holds for the simple exceptional groups of Lie type $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$ with C containing generators of a cyclic subgroup T as in Table 6.*

Proof. First let $G = F_4(q)$. By Lemma 3.2 the only characters not vanishing on an element $x \in C$ are those in the Lusztig series $\mathcal{E}(G, s)$, where s is a semisimple element lying in the dual torus $T^* \leq G^*$ (up to conjugation). As T is the centralizer of any of its nonidentity elements, the same is true for T^* . Thus all nonidentity elements $s \in T^*$ are regular, and $\mathcal{E}(G, s)$ consists of a single irreducible and thus semisimple Deligne-Lusztig character χ_s (up to sign).

The elements of $\mathcal{E}(G, 1)$ are by definition the unipotent characters of G . Using the character formula [6, Prop. 7.5.4] or the theory of blocks with cyclic defect group for a prime dividing $|T|$, one finds that $\chi(x) \in \{0, \pm 1\}$ for all unipotent characters $\chi \in \mathcal{E}(G, 1)$, with $\chi(x) \equiv \chi(1) \pmod{|T|}$. Explicit computation using the degrees of unipotent characters, given in [6, 13.9] for example, shows that the contribution of these $\chi \neq 1_G$ to $\epsilon_a(C)$ is positive.

Next, the character formula in Proposition 3.3 shows that for $s \in T^*$ a regular element $\chi_s(x)$ is a sum of $|N_G(T) : T| = 12$ roots of unity, hence of absolute value at most 12. There are $(|T| - 1)/12$ such semisimple characters, each of degree $|G : T|_{q'}$, so they contribute at most $12^2|T|^2/|G|_{q'}$ to $|\epsilon_a(C)|$. Thus $n_a(C) \geq |G|/|T|^2(1 - 12^2|T|^2/|G|_{q'})$.

By Table 6 the only maximal subgroups H containing x are one or two classes of triality groups ${}^3D_4(q).3$, when $q \geq 3$. Since any such subgroup contains the full normalizer of T , T is contained in a unique group in each class, and moreover the intersection $C_H = C \cap H$ is a single conjugacy class of H , whence $|C_H| = |H : T|$. Thus each of the two classes of triality subgroups contributes at most $|H : T|$ triples, which is smaller than $n_a(C)$. For $F_4(2)$, the maximal subgroups above $N_G(T)$ contain less than 10^8 triples, while $n_a(C) > 10^{13}$.

For $E_6(q)$ we compute the structure constant $n_a(C)$ in the group $G = E_6(q)_{\text{ad}}$ of adjoint type, which contains the simple group as a normal subgroup of index $d = \gcd(3, q - 1)$. Here, the dual group is of type $E_6(q)_{\text{sc}}$, and the semisimple elements in the dual torus T^* are either central, or regular. The regular elements parametrize irreducible Deligne-Lusztig characters, whose contribution to $|\epsilon_a(C)|$ is thus bounded above by $81|T|^2/|G|_{q'}$ by Proposition 3.3, while the d central elements parametrize the d Lusztig series consisting of the various characters of G having the same restrictions to $E_6(q)$ as unipotent characters. Explicit computation gives that their contribution to $|\epsilon_a(C)|$ is less than $q^{56}/|G : T|$.

By Proposition 2.11 the only maximal subgroup H containing T is of type $\text{SL}_3(q^3).3$. This subgroup contains at most $|H| < 3q^{24}$ triples.

The argument for $G = {}^2E_6(q)_{\text{ad}}$ is completely analogous to the one in the untwisted case. Here, the contribution from the unipotent characters to $|\epsilon_a(C)|$ is less than $2q^{56}/|G : T|$. The only maximal subgroup containing T is of type $\text{SU}_3(q^3).3$, by Proposition 2.11, and we may conclude as before.

For $G = E_7(q)_{\text{ad}}$, the torus T^* does contain nonregular noncentral elements. We use the results of Lübeck [39, §5.9] on smallest character degrees. Let $x \in G' = E_7(q)$ be an element of order $\Phi_2(q)\Phi_{18}(q)/d$, where $d = \gcd(2, q - 1)$. The nontrivial character of G of smallest degree is the unipotent character $\phi_{7,1}$. It lies in the principal p -block for any Zsigmondy prime divisor p of $\Phi_{18}(q)$, so takes value ± 1 on x (in fact, value -1). There are just d characters of this degree, and the next smallest character degree is larger than

q^{26} . By the orthogonality relations for characters,

$$\sum_{\chi \in \text{Irr}(G)} |\chi(x)|^2 = |C_G(x)| = (q+1)(q^6 - q^3 + 1) < q^8$$

(in particular, $|\chi(x)| < q^4$ for any irreducible character χ). So all the characters of degree at least q^{26} contribute less than $q^{12}/q^{26} = q^{-14}$ to $\epsilon_a(C)$. The only maximal subgroup containing our element x is $M = {}^2E_6(q).D_{q+1}$, contributing at most $|M| < q^{80}$ triples.

For $G = E_8(q)$, arguing as for $F_4(q)$ above we see that the nonunipotent characters contribute at most $900|T|^2/|G|_{q'} \leq |\epsilon_a(C)|$, while the unipotent characters different from 1_G contribute at most $q^{211}/|G : T|$.

On the other hand the normalizer $N_G(T)$ contains no more than 30 triples. \square

3.3. The classical groups. We now turn to the simple classical groups of Lie type. Let G_{ad} be a group of adjoint type such that $G' = [G_{\text{ad}}, G_{\text{ad}}]$ is our given simple group. This is the group of fixed points under a Frobenius endomorphism of a simple algebraic group with connected center, so in particular the results of Section 3.1 are applicable. We'll choose the class $C \subset G'$ of an element x whose order is divisible by a Zsigmondy prime as in Section 2.2, such that its centralizer is a maximal torus of G_{ad} . Note that the number of conjugates of a maximal subgroup containing such an element can grow with both the field size and the rank. However, note that the automizer of the maximal torus T containing x acts semiregularly on the nontrivial powers of x . It follows that every nontrivial eigenspace of x on an irreducible V has dimension at most $\dim V/[N_G(T) : T]$.

TABLE 7. Maximal tori in classical groups

| G | $ T $ | $ A_G(T) $ | ref. |
|-------------------------------------|------------------------|------------|------------|
| $\text{PGL}_n(q)$, $n \geq 3$ odd | $(q^n - 1)/(q - 1)$ | n | Lemma 2.3 |
| $\text{PGL}_n(q)$, $n \geq 4$ even | $q^{n-1} - 1$ | $n - 1$ | Lemma 2.4 |
| $\text{PGU}_n(q)$, $n \geq 3$ odd | $(q^n + 1)/(q + 1)$ | n | Lemma 2.5 |
| $\text{PGU}_n(q)$, $n \geq 4$ even | $q^{n-1} + 1$ | $n - 1$ | Lemma 2.6 |
| $\text{PCO}_{2n+1}(q)$ | $q^n + 1$ | $2n$ | Lemma 2.7 |
| $\text{PCSp}_{2n}(q)$ | $q^n + 1$ | $2n$ | Lemma 2.8 |
| $\text{PCO}_{2n}^{\circ+}(q)$ | $(q^{n-1} + 1)(q + 1)$ | $2n - 2$ | Lemma 2.9 |
| $\text{PCO}_{2n}^{\circ-}(q)$ | $q^n + 1$ | n | Lemma 2.10 |

We consider the various types case by case.

Proposition 3.6. *Theorem 1.1 holds for the groups $\text{O}_{2n}^-(q)$, $n \geq 4$, with C containing elements of order $\Phi_{2n}^*(q)$.*

Proof. We estimate the structure constants $n_a(C)$ in the group $G := \text{PCO}_{2n}^{\circ-}(q)$. Since the class C is contained in the derived subgroup $G' = \text{O}_{2n}^-(q)$, this will prove the claim. Note that elements of C are regular since their order is divisible by a Zsigmondy prime for $q^{2n} - 1$. Thus, by Lemma 3.2 the irreducible characters of G not vanishing on an element $x \in C$ lie in Lusztig series $\mathcal{E}(G, s)$ for semisimple elements s in the dual group

$G^* = \text{Spin}_{2n}^-(q)$ whose centralizer order is divisible by $\Phi_{2n}(q)$. These are precisely the elements in tori $T^* \leq G^*$ of order $q^n + 1$; the latter correspond to the F -class of an element v of the Weyl group W of G with cyclic centralizer of order n .

The elements of $\mathcal{E}(G, s)$, with s central in G^* , are the extensions to G of the unipotent characters of G' . Those which do not vanish on x take value ± 1 on x . Furthermore, since $|N_G(T) : T| = n$, there are exactly $n - 1$ nonprincipal unipotent characters of G' not vanishing on C ; as all unipotent characters extend to G , there are $d(n - 1)$ nonlinear characters of G to consider for $\epsilon_a(C)$, with $d = |G : G'| = \gcd(4, q^n + 1)$. Since the minimal nontrivial character degree of G equals $b := (q^n + 1)(q^{n-1} - q)/(q^2 - 1)$ by Tiep–Zaleskii [49, Thm. 1.1], the contribution of nonlinear characters in $\mathcal{E}(G, s)$, $s \in Z(G^*)$, to $|\epsilon_a(C)|$ is at most

$$(n - 1) \frac{1}{b} = \frac{(n - 1)(q^2 - 1)}{(q^n + 1)(q^{n-1} - q)}.$$

The noncentral elements in T^* have centralizer $Z_r := \text{GU}_{n/r}(q^r)$ for some divisor r of n such that n/r is odd. Let s_r denote an element with centralizer Z_r . Then $C_W(v) \cong W(T) \cong C_n$, $W(s) = \mathfrak{S}_{n/r}$, and $C_{W(s)}(v) \cong N_{Z_r}(T)/T \cong C_{n/r}$, so by Proposition 3.3 we have $|\chi_{s_r}(x)| \leq r$. By [15, §9] the n/r characters in $\mathcal{E}(G, s_r)$ not vanishing on x lie in the same p -block as χ_{s_r} , for all Zsigmondy prime divisors p of $\Phi_{2n}(q)$. In particular, their value on x has the same absolute value as $\chi_{s_r}(x)$, and similarly for the value on x^a . Finally, up to conjugation there are at most q^r/r elements in T^* with centralizer $\text{GU}_{n/r}(q^r)$, so the characters in Lusztig series for noncentral elements of G^* contribute at most

$$\sum_{r|n} \frac{nq^r r^3}{r^2 |G : Z_r|_{q^r}} = \sum_{r|n} \frac{nrq^r}{|G : Z_r|_{q^r}}$$

to $\epsilon_a(C)$. Using these estimates an easy calculation now shows that $\epsilon_a(C) < 0.5$ for all $n \geq 4$, $q \geq 2$, so that $n_a(C) \geq |C|^2/(2|G|)$.

The maximal subgroups of G containing an element $x \in C$ were listed in Lemma 2.10. For the two generic classes, viz. $H_1 = N_G(\text{SU}_n(q))$ (for n odd) and $H_r = N_G(\text{GO}_{2n/r}^-(q^r))$ (for r an odd prime divisor of n), we have $|G : H_1| \geq q^5(q^n + 1)$, and $|G : H_r| \geq q^{18}(q^n + 1)$, whence $\sum_{r=1}^n (q^n + 1)/|G : H_r| < 1/2$. So at most

$$\sum_{r=1}^n |H_r : T| = \frac{|G|}{|T|^2} \sum_{r=1}^n \frac{|T|}{|G : H_r|} < \frac{1}{2} \frac{|G|}{|T|^2} = |C|^2/2|G| \leq n_a(C)$$

triples are contained in these proper subgroups. For the groups $\text{O}_{10}^-(2)$, $\text{O}_{12}^-(2)$ in Table 5, an explicit calculation produces generating triples as claimed. For $\text{O}_{20}^-(2)$ the index of the subgroup \mathfrak{A}_{20} is too large. \square

Proposition 3.7. *Theorem 1.1 holds for the groups $\text{O}_{2n+1}(q)$, $n \geq 3$, q odd, with C containing elements of order $\Phi_{2n}^*(q)$.*

Proof. As in the previous proof we first estimate the structure constant $n_a(C)$ in the group $G := \text{SO}_{2n+1}(q)$ of adjoint type. Let $x \in C$ and let T be its centralizer in G , a maximal torus of order $|T| = q^n + 1$, parametrized by $v \in W$ with cyclic centralizer of order $2n$ and C the class of a generator of $T \cap G'$. As in the proof of the previous result we see that the extensions to G of unipotent characters of G' which do not vanish on x

take the values ± 1 on x . Furthermore, $|N_G(T) : T| = 2n$, so there are exactly $2(2n - 1)$ nonlinear such characters. The minimal degree of a nontrivial unipotent character of G equals $b = (q^n - 1)(q^n - q)/(2(q + 1))$ by [49, Prop. 5.1], so the contribution of characters from $\mathcal{E}(G, s)$ with $s \in Z(G^*)$ to $|\epsilon_a(C)|$ is at most

$$(2n - 1) \frac{1}{b} = \frac{(2n - 1)2(q + 1)}{(q^n - 1)(q^n - q)}.$$

The noncentral elements in the torus T^* in the dual group $G^* = \mathrm{Sp}_{2n}(q)$ have centralizer $Z_r := \mathrm{GU}_{n/r}(q^r)$, with $r|n$ such that n/r is odd. Then $C_W(v) \cong W(T) \cong C_{2n}$, $W(s) = \mathfrak{S}_{n/r}$, and $C_{W(s)}(v) \cong N_{Z_r}(T)/T \cong C_{n/r}$, so by Proposition 3.3 we have $|\chi_{s_r}(x)| \leq 2r$. Arguing as for $\mathrm{PCO}_{2n}^{\circ-}(q)$ we see that the nonunipotent characters contribute at most

$$\sum_{r|n} \frac{nq^r(2r)^3}{r^2|G : Z_r|_{q'}} = \sum_{r|n} \frac{8nrq^r}{|G : Z_r|_{q'}}$$

to $|\epsilon_a(C)|$. Again, it ensues that $n_a(C) \geq |C|^2/(2|G|)$ (recall that $q > 2$ since q is odd).

We now estimate the contribution from maximal subgroups. The maximal subgroups containing elements of order divisible by $\Phi_{2n}^*(q)$ were described in Lemma 2.7. The stabilizers of nondegenerate 1-spaces $H := N_G(\mathrm{SO}_{2n}^-(q))$ have index $|G : H| > q^2(q^n + 1)$, and for $n = 3$, $G_2(q)$ has index $q^3(q^4 - 1)$ and $\mathrm{U}_3(q)$ has index $q^6(q^3 - 1)(q^4 - 1)$, and for both groups there are $q + 1$ distinct conjugates above x . Thus, the trivial estimate that there are at most $|H|$ triples in H shows that not all triples can lie inside these proper subgroups. The Ree groups ${}^2G_2(q)$ do not possess elements of order $\Phi_6^*(q)$ for $q \geq 27$. For $\mathrm{O}_7(3)$ and $\mathrm{O}_7(5)$, explicit computation yields that there exist generating triples consisting of elements of order 7. \square

Proposition 3.8. *Theorem 1.1 holds for the groups $\mathrm{S}_{2n}(q)$, $n \geq 2$, $(n, q) \neq (2, 2)$, with C containing elements of order $\Phi_{2n}^*(q)$, respectively of order 7 when $(n, q) = (3, 2)$.*

Proof. The claim for $\mathrm{S}_6(2)$ can be checked by computer, so now assume that $(n, q) \neq (3, 2)$. Then all elements $x \in C$ are regular with centralizer a cyclic torus T of order $q^n + 1$ in the adjoint type group $G := \mathrm{PCSp}_{2n}(q)$. As in the previous proof, using [49, Prop. 5.1] we obtain that the nonlinear unipotent characters of G' contribute at most

$$\mathrm{gcd}(2, q - 1) \frac{(2n - 1)2(q + 1)}{(q^n - 1)(q^n - q)}$$

to $|\epsilon_a(C)|$ in G . The nontrivial elements in the dual torus of order $q^n + 1$ of $G^* = \mathrm{Spin}_{2n+1}(q)$ have centralizers of types $\mathrm{Spin}_{2n}^-(q)$ (when $q^n \equiv 3 \pmod{4}$) and $\mathrm{GU}_{n/r}(q^r)$ for $r|n$ with n/r odd. The semisimple elements with centralizer of types $\mathrm{Spin}_{2n}^-(q)$ lead to the Weil character of G of degree $q^n - 1$, which takes value -2 on x . Via Jordan decomposition the characters in this Lusztig series $\mathcal{E}(G, s)$ are in bijection with the unipotent characters of $\mathrm{Spin}_{2n}^-(q)$; thus the second smallest degree in $\mathcal{E}(G, s)$ equals $b|G^* : \mathrm{Spin}_{2n}^-(q)|_{q'} = b(q^n - 1)$ with $b = (q^n + 1)(q^{n-1} - q)/(q^2 - 1)$ by [49, Thm. 1.1]. Since $|\mathcal{E}(G, s)| = n$ these characters contribute at most

$$\frac{1}{q^n - 1} + \frac{(n - 1)(q^2 - 1)}{(q^n + 1)(q^{n-1} - q)(q^n - 1)}$$

to $|\epsilon_a(C)|$ (and only when $q^n \equiv 3 \pmod{4}$).

As in the previous proof, the characters parametrized by semisimple elements with centralizer $Z_r := \mathrm{GU}_{n/r}(q)$ contribute at most

$$\sum_{r|n} \frac{8nrq^r}{|G : Z_r|_{q'}}.$$

For $n \geq 3$ and $(n, q) \neq (3, 2)$ this shows that $|\epsilon_a(C)| < 0.5$. Explicit computation of the structure constant in $\mathrm{PCSp}_4(q)$ with Chevie shows that here $|\epsilon_a(C)| < 0.5$ for $q \geq 3$ as well.

The maximal subgroups of G containing elements of order divisible by $\Phi_{2n}^*(q)$ are given in Lemma 2.8 and Table 3. The index of $H_1 := N_G(\mathrm{SU}_n(q))$, for n odd, is at least $q^5(q^n + 1)$, the index of $H_r := N_G(\mathrm{Sp}_{2n/r}(q^r))$ is at least $q^{10}(q^n + 1)$ for $n \geq 4$, respectively $q^2(q^2 - 1)$ for $n = r = 2$. The index of $G_2(q)$ for $n = 3$ equals $q^3(q^4 - 1)$, and there are $q + 1$ distinct conjugates containing x . The structure constant $n_a(C)$ in $H = \mathrm{SO}_{2n}^-(q)$ was investigated in Proposition 3.6; it is less than $2|H|/|T|^2$. By explicit computation in GAP, the groups $\mathrm{Sp}_{2n}(q)$ listed in Table 3 different from $\mathrm{Sp}_{20}(2)$ possess generating triples of the stated form. For $\mathrm{Sp}_{20}(2)$ the structure constant in the exceptional subgroup $\mathrm{L}_2(41)$ is too small. The subgroups ${}^2\mathrm{B}_2(q)$ of $\mathrm{Sp}_4(q)$ in Lemma 2.8(5) do not possess elements of order $\Phi_{2n}^*(q)$ for $q \neq 2$. \square

The excluded group $\mathrm{S}_4(2)$ has derived group the alternating group \mathfrak{A}_6 , which will be considered in Lemma 4.4.

To deal with the even-dimensional split orthogonal groups we need to understand the elements in a certain maximal torus of the dual group.

Lemma 3.9. *Let $n \geq 4$, T a maximal torus of $G = \mathrm{Spin}_{2n}^+(q)$ of order $(q^{n-1} + 1)(q + 1)$. Then for $s \in T \setminus Z(G)$ either $C_G(s) \cong H := \mathrm{Spin}_{2n-2}^-(q)(q + 1)$ or $C_G(s) \leq \mathrm{GU}_n(q)$ if $n \geq 6$ is even, or $C_G(s) \leq \mathrm{GU}_{n-1}(q)(q + 1)$ if $n = 4$ or n is odd. Moreover, the number of elements with centralizer H is given in Table 8.*

TABLE 8. Centralizer $\mathrm{Spin}_{2n-2}^-(q)(q + 1)$ in $\mathrm{Spin}_{2n}^+(q)$

| | q even | $q^n \equiv 1 \pmod{4}$ | $q^n \equiv 3 \pmod{4}$ |
|---------|----------|-------------------------|-------------------------|
| $n = 4$ | $3q/2$ | $3(q - 1)$ | — |
| $n > 4$ | $q/2$ | $q - 1$ | q |

Proof. Assume that q is odd. We first work inside the group $\mathrm{SO}_{2n}^+(q)$. Under the action of T , the natural module decomposes into an orthogonal sum $V_1 \perp V_2$, with $\dim V_1 = 2n - 2$, $\dim V_2 = 2$. The elements $x \in T$ for which $x|_{V_1}$ and $x|_{V_2}$ do not have the same eigenvalues have centralizer contained in $\mathrm{SO}_{2n-2}^-(q) \times \mathrm{SO}_2^-(q)$. Moreover, if $x|_{V_1} \neq \pm \mathrm{Id}$, then the centralizer is contained in $\mathrm{GU}_{n-1}(q) \times (q + 1)$. Thus, elements with centralizer $\mathrm{SO}_{2n-2}^-(q) \times \mathrm{SO}_2^-(q)$ are those acting as $\pm \mathrm{Id}$ on V_1 (and of order dividing $q + 1$ on V_2); hence they are the elements in a subgroup $H \cong C_2 \times C_{q+1}$ of T , and they are all real. Apart from the two central elements, we have $2q$ such elements and q classes. Now let's study the elements which lie inside $H' := H \cap \Omega_{2n}^+(q)$. If $q \equiv 1 \pmod{4}$, then H' is cyclic

of order $q + 1$ with $q - 1$ noncentral elements in $(q - 1)/2$ classes. Lifting to $\text{Spin}_{2n}^+(q)$, each element has two preimages, so we get $q - 1$ classes.

If $q \equiv 3 \pmod{4}$ and n is even, $H' \cong C_2 \times C_{(q+1)/2}$, which contains 3 involutions (1 central), so there are $q - 1$ noncentral elements including two involutions, lying in $(q - 3)/2 + 2$ classes. The involutions lift to one class each and all other classes have two preimage classes, so there are again $(q - 3) + 2 = q - 1$ classes.

If $q \equiv 3 \pmod{4}$ and n is odd, then the central involution has spinor norm -1 and H' has only one involution, so it is cyclic of order $q + 1$ with no nontrivial central elements. Thus we find q elements with this centralizer and so $(q - 1)/2 + 1 = (q + 1)/2$ classes in $\Omega_{2n}^+(q)$. Again, the only element with only one preimage class is the involution, so we find q classes in G .

The elements $x \in T$ for which $x|_{V_1}$ and $x|_{V_2}$ have the same eigenvalues (which can only happen if n is even), have centralizer $\text{GU}_n(q)$. For $n = 4$, their lifts to $\text{Spin}_8^+(q)$ are interchanged with those of centralizer $\text{Spin}_{2n-2}^-(q)(q + 1)$ by triality, so we get $3(q - 1)$ classes with this centralizer in total.

The case where q is even is much easier since there $\text{Spin}_{2n}^+(q) = \text{SO}_{2n}^+(q)$. \square

Proposition 3.10. *Theorem 1.1 holds for the groups $\text{O}_{2n}^+(q)$, $n \geq 4$, with C containing elements which act as an element of order $\Phi_{2n-2}^*(q)$ on a $(2n - 2)$ -dimensional subspace and as an element of order > 2 dividing $q + 1$ on its orthogonal complement.*

Proof. Let C be the conjugacy class of an element $x \in \text{O}_{2n}^+(q)$ as in the statement. Then x is regular semisimple in a maximal torus T of order $(q^{n-1} + 1)(q + 1)$ in the group $G := \text{PCO}_{2n}^+(q)$ of adjoint type. Such an element exists unless $(n, q) = (4, 2)$. For the group $\text{O}_8^+(2)$ it can be checked using GAP that there exist triples as required with elements of order 9, so now assume that $(n, q) \neq (4, 2)$. We estimate the structure constant $n_a(C)$ in G . The characters of G not vanishing on x lie in Lusztig series parametrized by semisimple elements in the dual torus $T^* \leq G^* = \text{Spin}_{2n}^+(q)$. We distinguish three types of such elements: the central elements, the elements with centralizer $\text{Spin}_{2n-2}^-(q) \times \text{Spin}_2^-(q)$, and the remaining elements, having centralizer $\text{GU}_n(q)$ (for n even) or smaller; see Lemma 3.9.

The Lusztig series for central elements $s \in T^*$ contain the extensions to G of unipotent characters of G' . Those which do not vanish on x take the values ± 1 on x . Furthermore, $|N_G(T) : T| = 2n - 2$, so there are exactly $d(2n - 3)$ nonlinear such characters. The minimal degree of a nonlinear unipotent character of G equals $b_1 := (q^n - 1)(q^{n-1} + q)/(q^2 - 1)$ by [49, Prop. 7.2], so the contribution of characters from $\mathcal{E}(G, s)$ with $s \in Z(G^*)$ to $|\epsilon_a(C)|$ is at most

$$(2n - 3) \frac{1}{b_1} = \frac{(2n - 3)(q^2 - 1)}{(q^n - 1)(q^{n-1} + q)}.$$

Next, let $s \in T^*$ with centralizer $\text{Spin}_{2n-2}^-(q)\text{Spin}_2^-(q)$; the corresponding semisimple character χ_s has degree $b_2 := (q^n - 1)(q^{n-1} - 1)/(q + 1)$. By Proposition 3.3, $\chi_s(x^a)$ has absolute value at most 2, and thus the same holds for all the $n - 1$ characters in $\mathcal{E}(G, s)$. By Lemma 3.9 there are at most q such semisimple elements up to conjugation, so these characters contribute at most

$$q(n - 1)2^3 \frac{1}{b_2} = \frac{8(n - 1)q(q + 1)}{(q^n - 1)(q^{n-1} - 1)}$$

to $\epsilon_a(G)$. If n is even, there are at most $(q+1)^2 - 2(q+1) = q^2 - 1$ further elements s_0 with centralizer $Z_0 := \mathrm{GU}_n(q)$, each conjugate to its inverse. The remaining elements in T^* have centralizer $Z_r := \mathrm{GU}_{(n-1)/r}(q^r)(q+1)$, with $r|(n-1)$ such that $(n-1)/r$ is odd, and for each r there are at most $(q^r+1)(q+1) - (q+1)^2 = (q^r - q)(q+1) < q^r(q+1)$ such elements s_r , falling into at most $q^r(q+1)/r$ classes. By Proposition 3.3 we have $|\chi_{s_0}(x)| \leq 2$, respectively $|\chi_{s_r}(x)| \leq 2r$. Thus, the remaining characters contribute at most

$$\frac{8(n-1)(q^2-1)}{|G : Z_0|_{q'}} + \sum_{r|n-1} \frac{(n-1)q^r(q+1)(2r)^3}{r^2|G : Z_r|_{q'}}$$

to $|\epsilon_a(C)|$. This shows that $n_a(C) \geq \frac{1}{2}|C|^2/|G|$ for $(n, q) \neq (4, 2)$.

The maximal subgroups of G containing elements of order divisible by $\Phi_{2n-2}^*(q)$ are given in Lemma 2.9 and Table 4. By our choice of x it stabilizes a unique decomposition of the underlying space, into a 2-dimensional subspace and its orthogonal complement. The stabilizer $H_1 := \mathrm{GO}_{2n-2}^-(q) \times \mathrm{GO}_2^-(q) \cap G$ of this decomposition has index $q^{2(n-1)}(q^n - 1)(q^{n-1} - 1)/(q+1)$. The index of $H_2 := N_G(\mathrm{SU}_n(q))$, for n even, is at least $q^{n(n-1)/2}(q^{n-1} - 1)$, the index of $H_3 := N_G(\Omega_n(q^2))$, for n odd, is at least $q^{(n^2-1)/2}(q^n - 1)$.

For $n = 4$, there is one more subgroup $\mathrm{Spin}_7(q)$, again with too few triples by Proposition 3.7, and a subgroup $N_G(\mathrm{U}_3(q))$, of index at least $q^9(q^4 - 1)(q^3 - 1)$. Thus, not all triples can lie inside these proper subgroups. By explicit computation in **GAP**, the groups $\mathrm{O}_8^+(3)$ and $\mathrm{O}_8^+(5)$ possess generating triples of elements of order 7, resp. 21. The only other group in Table 4 containing elements of order $o(x)$ is \mathfrak{A}_{16} in $\Omega_{14}^+(2)$, but there the number of triples is too small. \square

Proposition 3.11. *Theorem 1.1 holds for the groups $\mathrm{U}_n(q)$, $n \geq 3$ odd, $(n, q) \neq (3, 2)$, with C containing elements of order $\Phi_{2n}^*(q)$.*

Proof. Let $x \in C$, with centralizer a cyclic torus T of order $(q^n + 1)/(q + 1)$ in $G := \mathrm{PGU}_n(q)$. The minimal degree of a nonprincipal unipotent character of G is at least $(q^n - q)/(q + 1)$ by [49, Thm. 4.1], so the nonlinear unipotent characters of G' contribute at most

$$\frac{(n-1)(q+1)}{(q^n - q)}$$

to $|\epsilon_a(C)|$ in G . The nontrivial elements in the dual torus T^* in $G^* = \mathrm{SU}_n(q)$ of order $(q^n + 1)/(q + 1)$ have centralizers of types $Z_r := G^* \cap \mathrm{GU}_{n/r}(q^r)$ for $r|n$, $r > 1$. Let s_r denote an element with centralizer Z_r . Then $C_W(v) \cong W(T) \cong C_n$, $W(s) = \mathfrak{S}_{n/r}$, and $C_{W(s)}(v) \cong N_{Z_r}(T)/T \cong C_{n/r}$, so by Proposition 3.3 we have $|\chi_{s_r}(x)| \leq r$. By [14, Thm. 7A] the n/r characters in $\mathcal{E}(G, s_r)$ not vanishing on x lie in the same p -block as χ_{s_r} , for all Zsigmondy prime divisors p of $\Phi_{2n}(q)$, so their value on x has the same absolute value as $\chi_{s_r}(x)$. Up to conjugation there are at most q^{r-1}/r elements with centralizer $\mathrm{SU}_{n/r}(q^r)$, so the characters in Lusztig series for noncentral elements of G^* contribute at most

$$\sum_{r|n} \frac{nq^{r-1}r^3}{r^2|G : Z_r|_{q'}} = \sum_{r|n} \frac{nrq^{r-1}}{|G : Z_r|_{q'}}$$

to $|\epsilon_a(C)|$. Using these estimates an easy calculation now shows that $|\epsilon_a(C)| < 0.5$ for all $n \geq 5$, $(n, q) \neq (5, 2)$, so that $n_a(C) \geq |C|^2/(2|G|)$. For $n = 3$, the structure constant can be computed explicitly as $|T|(q^2 + 3q + 1)$ for $q \neq 3, 5$.

For the groups $U_3(3)$, $U_3(5)$ and $U_5(2)$ it can be checked by direct calculation that there exist generating triples. For the remaining cases, by Lemma 2.5 the only maximal subgroups to consider are the images in $\text{PGU}_n(q)$ of normalizers of $\text{GU}_{n/r}(q^r)$ in $\text{GU}_n(q)$, for $r|n$, of index at least $q^{n^2/4}(q^{n-1} - 1)/r$, resp. $q^3(q^2 - 1)/3$ if $n = 3$. Again, not all triples can lie in these subgroups. \square

The excluded group $U_3(2)$ is solvable.

Proposition 3.12. *Theorem 1.1 holds for the groups $U_n(q)$, $n \geq 4$ even, $(n, q) \neq (4, 2)$, with C containing elements of order $\Phi_{2n-2}^*(q)$.*

Proof. Let $x \in C$, with centralizer a cyclic torus T of order $q^{n-1} + 1$ in $G := \text{PGU}_n(q)$. The minimal degree of a nonprincipal unipotent character of G' is at least $(q^n + q)/(q + 1)$ by [49, Thm. 4.1], so the $n - 2$ nonlinear unipotent characters of G' not vanishing on regular elements of T contribute at most

$$\frac{(n-2)(q+1)}{(q^n+q)}$$

to $|\epsilon_a(C)|$ in G . The nontrivial elements in the dual torus T^* in $G^* = \text{SU}_n(q)$ of the same order have centralizers of types $Z_r := \text{GU}_{(n-1)/r}(q^r)$ for $r|(n-1)$. Let s_r denote an element with centralizer $\text{GU}_{(n-1)/r}(q^r)$. Then $C_W(v) \cong W(T) \cong C_{n-1}$, $W(s) = \mathfrak{S}_{(n-1)/r}$, and $C_{W(s)}(v) \cong N_{Z_r}(T)/T \cong C_{(n-1)/r}$, so by Proposition 3.3 we have $|\chi_{s_r}(x)| \leq r$. By [14, Thm. 7A] the $(n-1)/r$ characters in $\mathcal{E}(G, s_r)$ not vanishing on x lie in the same p -block as χ_{s_r} , for all Zsigmondy prime divisors p of $\Phi_{2n-2}(q)$, so their value on x has the same absolute value as $\chi_{s_r}(x)$. Up to conjugation there are at most q^{r-1}/r elements with centralizer $\text{GU}_{(n-1)/r}(q^r)$, so the characters in Lusztig series for noncentral elements of G^* contribute at most

$$\sum_{r|n} \frac{(n-1)q^{r-1}r^3}{r^2|G : Z_r|_{q^r}} = \sum_{r|n} \frac{(n-1)r q^{r-1}}{|G : Z_r|_{q^r}}$$

to $|\epsilon_a(C)|$. It follows that $|\epsilon_a(C)| < 0.5$ and thus $n_a(C) \geq |C|^2/(2|G|)$ for all even $n \geq 4$, $(n, q) \neq (4, 2), (4, 3), (6, 2)$.

For $U_6(2)$, $U_4(3)$ and $U_4(5)$, a direct calculation shows that there exist generating triples. By Lemma 2.6 the only maximal subgroup to consider in the remaining cases is $\text{GU}_{n-1}(q)$, of index $q^{n-1}(q^n - 1)/(q + 1)$; thus not all triples can lie in proper subgroups. \square

The excluded group $U_4(2)$ is isomorphic to $S_4(3)$, treated in Proposition 3.8.

Proposition 3.13. *Theorem 1.1 holds for the groups $L_n(q)$, $n \geq 3$, $(n, q) \neq (3, 2), (4, 2)$, with*

- (a) C containing elements of order $\Phi_n^*(q)$ if n is odd, and
- (b) C containing elements of order $\Phi_{n-1}^*(q)$, if n is even.

Proof. First assume that n is odd. Let $x \in C$, with centralizer a cyclic torus T of order $(q^n - 1)/(q - 1)$ in $G := \text{PGL}_n(q)$. The minimal degree of a nonprincipal unipotent

character of G is at least $(q^n - q)/(q - 1)$ by [49, Thm. 3.1], so the nonlinear unipotent characters of G' contribute at most

$$\frac{(n-1)(q-1)}{(q^n - q)}$$

to $|\epsilon_a(C)|$ in G . The noncentral elements in the dual torus T^* in $G^* = \mathrm{SL}_n(q)$ of the same order have centralizers of types $Z_r := G^* \cap \mathrm{GL}_{n/r}(q^r)$ for $r|n$, $r > 1$. Let s_r denote an element with centralizer Z_r . Then $C_W(v) \cong W(T) \cong C_n$, $W(s) = \mathfrak{S}_{n/r}$, and $C_{W(s)}(v) \cong N_{Z_r}(T)/T \cong C_{n/r}$, so by Proposition 3.3 we have $|\chi_{s_r}(x)| \leq r$. Again by [14, Thm. 7A] the values of the n/r characters in $\mathcal{E}(G, s_r)$ not vanishing on x have the same absolute value as $\chi_{s_r}(x)$. Up to conjugation there are at most q^{r-1}/r elements with centralizer Z_r , so the characters in Lusztig series for noncentral elements of G^* contribute at most

$$\sum_{r|n} \frac{nq^{r-1}r^3}{r^2|G : Z_r|_{q'}} = \sum_{r|n} \frac{nrq^{r-1}}{|G : Z_r|_{q'}}$$

to $|\epsilon_a(C)|$. It follows that $|\epsilon_a(C)| < 0.5$ for all $n \geq 5$, $(n, q) \neq (5, 2)$, so that $n_a(C) \geq \frac{1}{2}|C|^2/|G|$. For $n = 3$, the structure constant can be computed explicitly from the known character table as $|T|(q^2 - 3q + 1)$ for $q \neq 2, 4$.

By direct computation, the groups $L_3(4)$ and $L_5(2)$ contain generating triples. By Lemma 2.3, the only maximal subgroups to consider in the remaining cases are the image in G of $\mathrm{GU}_n(q^{1/2})$ if q is a square, of index at least $q^{n(n-1)/4}(q^{n-1} - 1)$ and with $q^{n/2} - 1$ conjugates containing x , and of the normalizers of $\mathrm{GL}_{n/r}(q^r)$ in $\mathrm{GL}_n(q)$, for $r|n$, $r > 1$, of index at least $q^{n^2/4}(q^{n-1} - 1)/r$, resp. $q^3(q^2 - 1)/3$ if $n = 3$.

If now $n \geq 4$ is even, the same arguments apply to show that $|\epsilon_a(C)| < 0.5$ unless $(n, q) = (4, 2)$, so that $n_a(C) \geq \frac{1}{2}|C|^2/|G|$.

By direct computation, the group $L_4(4)$ contains generating triples. The only maximal subgroups to consider in the remaining cases are, by Lemma 2.3, the image in G of $\mathrm{GU}_n(q^{1/2})$, with q a square, of large index and less than $q^{n/2}$ conjugates containing x , and the end node parabolic subgroups P_1, P_{n-1} , of index $(q^n - 1)/(q - 1)$. Since both P_i contain the full normalizer of the maximal torus T of order $q^{n-1} - 1$, there are at most $|P_i|/|T|$ elements from C in P_i , so each contains at most $(q - 1)|G|/((q^n - 1)(q^{n-1} - 1))$ triples, which is sufficiently small for our estimate. \square

The excluded group $L_4(2) \cong \mathfrak{A}_8$ will be treated in Lemma 4.4. The groups $L_2(q)$ are the subject of the next section.

3.4. The groups $L_2(q)$. We now consider $\mathrm{SL}_2(q)$ and $L_2(q)$, where the results are somewhat different especially for q even.

From the subgroup structure of $\mathrm{SL}_2(q)$, it is quite easy to see that if $q > 11$, then the only maximal subgroups containing the split torus are the normalizer of the torus and the two Borel subgroups. Similarly, the normalizer of the nonsplit torus is the unique maximal subgroup containing the nonsplit torus.

We first deal with q odd.

Lemma 3.14. *Let $S = L_2(q)$ with $q \geq 11$ and odd. Let C be a conjugacy class of elements of order $(q - 1)/2$. Then Theorem 1.1 holds for C . Also, Theorem 1.1 holds for $L_2(9)$ with C a class of elements of order 5.*

Proof. We work in $G = \mathrm{SL}_2(q)$. First assume that $q > 11$. Let C be a conjugacy class of elements of order $q - 1$ in G . It is a trivial matrix computation to show that $\mathrm{tr}(xy)$ with $x, y \in C$ can be any element of \mathbb{F}_q . Thus, there exist $x, y \in C$ and $z \in C$ or $z \in -C^{-2}$ so that $xyz = 1$. We claim that $G = \langle x, y \rangle$ in either case. If not, then x, y are contained in a Borel subgroup B . However, if $x, y \in C \cap B$, we see that xy is either unipotent or conjugate to x^2 . Thus, $G = \langle x, y \rangle$. Passing to the quotient $\mathrm{L}_2(q)$ gives the result. For $q = 9, 11$ the claim follows by direct computation. \square

We note that if $q = 5$ or $q = 7$ and C is a conjugacy class of elements of order q in $G = \mathrm{L}_2(q)$, then there exists a generating triple from C with product 1. It is also straightforward to check that if V is a nontrivial absolutely irreducible kG -module, then an element of order q has no eigenspace of dimension greater than $(1/3) \dim V$.

We next consider $G = \mathrm{L}_2(q)$ with q even. If $q = 4$, then $G = \mathfrak{A}_5 \cong \mathrm{L}_2(5)$, a case already dealt with.

Lemma 3.15. *Let $G = \mathrm{L}_2(q)$ with $q > 7$ and even. Let C be a conjugacy class of elements of order $q - 1$. Let k be an algebraically closed field of characteristic p .*

- (a) *There exist $x, y, z \in C$ with product 1 and $G = \langle x, y \rangle$.*
- (b) *If $p > 2$ and V is any nontrivial irreducible kG -module, then every eigenspace of x has dimension at most $(1/3) \dim V$.*
- (c) *If $p = 2$ and V is any nontrivial irreducible kG -module of dimension greater than 2, then every eigenspace of x has dimension at most $(1/3) \dim V$.*

Proof. (a) follows just as for q odd. Now first suppose that $p > 2$. Thus, $\dim V = q - 1 + e$ where $e = 0, 1, 2$ by the well-known representation theory of $\mathrm{L}_2(q) = \mathrm{PGL}_2(q)$. Let B be a Borel subgroup containing $x \in C$. Let U be the unipotent radical of B . Then U has $q - 1$ nontrivial eigenspaces on V permuted transitively by x . Thus V is a direct sum of a rank 1 free x -module and an x -submodule of dimension e . Thus, any eigenspace of x has dimension at most $1 + e$, whence (b) holds.

Now assume that $p = 2$. Then every nontrivial irreducible module is a tensor product of Frobenius twists of the natural module. It is trivial to check that either every eigenspace for elements of C has dimension at most 1 or V is the Steinberg module of dimension q and the largest eigenspace is the trivial eigenspace of dimension $2 < q/3$. \square

We close this section with a result for the nonsplit tori in $\mathrm{SL}_2(q)$ with q even.

Lemma 3.16. *Let $G = \mathrm{SL}_2(q)$ with $q > 3$ even. Let $x \in G$ have order $q + 1$. If k is an algebraically closed field of characteristic 2 and V is an irreducible nontrivial kG -module, then x has distinct eigenvalues on V and $C_V(x) = 0$.*

Proof. V is a tensor product of distinct Frobenius twists of the natural 2-dimensional module. If $q = 2^f$, there are exactly f distinct twists. It is straightforward to see that possible eigenvalues are distinct on V and $C_V(x) = 0$. \square

4. ALTERNATING AND SPORADIC GROUPS

In this section we prove Theorem 1.1 for alternating and sporadic groups. We first recall a translation result for generation. See [27, Lemma 4.6] for example.

Lemma 4.1. *Let G be a finite group generated by x, y, z with product 1. Then for any $d \geq 1$ there is a normal subgroup N generated by x^d, y^d and d conjugates of z with product 1 generating N . Moreover G/N is cyclic of order dividing d .*

Lemma 4.2. *Let $n \geq 11$ be odd and set $G = \mathfrak{A}_n$. Then there exist three $n - 2$ cycles with product 1 that generate G .*

Proof. Set $x = (2\ 4\ 5\ 6\ \dots\ n)$ and $u = (1\ 2)(3\ 4)$. Then $w := ux = (1\ 2\ \dots\ n)$. Set $s = w^4$. Then $v := u^s = (5\ 6)(7\ 8)$. Set $y = x^s$. So $w = vy$. Thus, $y^{-1}(vu)x = 1$ with vu an involution moving 8 points. Let $H := \langle x, y \rangle$. Since y does not fix 1 or 3 or $\{1, 3\}$, H is transitive. Since x is an $n - 2$ cycle and n is odd, H is primitive and then applying [51, Thm. 13.8], H is triply transitive. It follows by [51, Thm. 15.1] that either $H = G$ or $n \leq 21$. By inspection of the triply transitive degree n groups with $11 \leq n \leq 21$ generated by $n - 2$ cycles, no possibility remains for H since $n \geq 11$.

So $G = \langle x, y \rangle$, where x and y are $n - 2$ cycles and their product is an involution. By the translation principle, a subgroup of index at most 2 in G is generated by x^2 and two conjugates of y with product 1. \square

Lemma 4.3. *Let $n \geq 12$ be even and set $G = \mathfrak{A}_n$. Then there exist three $n - 3$ cycles with product 1 that generate G .*

Proof. Set $u = (1\ 2)(3\ 4)(5\ 6)$ and $x = (1\ 3\ 5\ 7\ 8\ \dots\ n)$. Then $w = xu$ is the standard n -cycle. Set $s = w^6$. So $w = yv$, where $y = x^s$ and $v = u^s$. Note that vu is an involution moving exactly 12 points and $y^{-1}(vu)x = 1$. Set $H = \langle x, y \rangle$. By construction H is transitive. It is obviously primitive unless $3|n$ and then the fixed points F of x would have to be a block (i.e. $\{2, 4, 6\}$ as well as $vu(F) = \{1, 3, 5\}$). Since $x(1) = 3$ and $x(5) = 7$, this is a contradiction. So H is primitive.

By [51, Thm. 13.8], H is 4-transitive. By [51, Thm. 15.1], $n \leq 25$. The only possibilities for H other than G would be for H to be a Mathieu group with $n = 12, 22$ or 24 . In all three cases, we see that the Mathieu group M_n does not contain both an involution moving exactly 12 points and an $n - 3$ cycle. \square

A computer check shows the following:

Lemma 4.4. *Let $5 \leq n \leq 10$. Then Theorem 1.1 holds for \mathfrak{A}_n with C the class of a k -cycle, where $k = 5$ for $n = 5, 6$ and $k = 7$ otherwise.*

The result is pretty close for \mathfrak{A}_{10} : for a fixed element x of order 7, only 42 out of the 7446 pairs (y, z) with y, z conjugate to x and $xyz = 1$ do generate G (this is roughly one in 177), all others generate intransitive subgroups: for example, 2856 pairs generate an \mathfrak{A}_9 , 3717 generate an \mathfrak{A}_8 . The generating triple for \mathfrak{A}_{10} can be obtained by translation from the rigid genus 0 triple of \mathfrak{S}_{10} consisting of elements of cycle shapes $(2^5, 7, 7.2)$.

Proposition 4.5. *Theorem 1.1 holds for sporadic groups and for the Tits group, with C as indicated in Table 9.*

Proof. In Table 9 we give, for each sporadic simple group G , a conjugacy class C (in Atlas notation), the index $A_G(C) := |N_G(\langle g \rangle) : C_G(g)|$ for $g \in C$, the structure constant $n_1(C)$ (and, if that is different, $n_{-2}(C)$) in G , and the list of conjugacy classes of maximal

TABLE 9. Structure constants for sporadic groups

| G | C | $A_G(C)$ | $n_a(C)$ | max. overgroups of $g \in C$ |
|---------------|-----|----------|-----------------|--|
| M_{11} | 11a | 5 | 35 80 | $L_2(11) : 2 14$ |
| M_{12} | 11a | 5 | 640 1180 | $M_{11} : 35 80 (2\times), L_2(11) : 2 14$ |
| J_1 | 19a | 6 | 496 419 | $19.6 : 3 3$ |
| M_{22} | 11a | 5 | 3632 3776 | $L_2(11) : 2 14$ |
| J_2 | 7a | 6 | 12528 | $U_3(3) : 397, L_3(2).2 : 12$ |
| M_{23} | 23a | 11 | 17646 18222 | $23.11 : 11$ |
| ${}^2F_4(2)'$ | 13a | 6 | 114870 114195 | $L_3(3).2 : 106 133(2\times), L_2(25) : 1650$ |
| HS | 11a | 5 | 363464 367964 | $M_{22} : 3632 3776, M_{11} : 35 80 (2\times)$ |
| J_3 | 19a | 9 | 131161 | $L_2(19) : 4 (2\times)$ |
| M_{24} | 23a | 11 | 441904 455728 | $M_{23} : 17646 18222, L_2(23) : 5 29$ |
| McL | 11a | 5 | 7372675 7463800 | $M_{22} : 3632 3776 (2\times), M_{11} : 35 80$ |
| He | 17a | 8 | 14113998 | $S_4(4).2 : 13892$ |
| Ru | 29a | 14 | 174426828 | $L_2(29) : 35$ |
| Suz | 13a | 6 | * | $G_2(4), L_3(3).2 (2\times), L_2(25)$ |
| ON | 31a | 15 | 479254117 | $L_2(31) : 7 (2\times)$ |
| Co_3 | 23a | 11 | * | M_{23} |
| Co_2 | 23a | 11 | * | M_{23} |
| Fi_{22} | 13a | 6 | * | $O_7(3) (2\times), {}^2F_4(2)'$ |
| HN | 19a | 9 | 756228015580 | $U_3(8).3 : 134923$ |
| Ly | 67a | 22 | * | 67.22 |
| Th | 19a | 18 | 252411100157582 | $U_3(8).6 : 539180, L_2(19).2 : 36$ |
| Fi_{23} | 17a | 16 | * | $S_8(2), S_4(4).4$ |
| Co_1 | 13a | 12 | * | $3.Suz.2, (\mathfrak{A}_4 \times G_2(4)).2$ |
| J_4 | 43a | 14 | * | 43.14 |
| Fi'_{24} | 29a | 14 | * | 29.14 |
| B | 47a | 23 | * | 47 : 23 |
| M | 71a | 35 | * | $L_2(71)$ |

*: the values are too large to be printed

subgroups containing an element from C . Here, the structure constant in G as well as in any maximal subgroup H nontrivially intersecting C is easily computed from the character tables, using GAP for example, since we chose C such that only almost quasi-simple or metabelian maximal subgroups H occur. It remains to check that these contributions are less than $n_a(C)$.

The lists of maximal subgroups are taken from the Atlas [8] or from the Atlas home page [53]. \square

5. AN APPLICATION TO REPRESENTATION THEORY

Here, we prove our main results, Corollary 1.2 and Theorem 1.3, from the introduction. We first recall Scott's Lemma [47]. Let k be a field of characteristic $p \geq 0$.

Lemma 5.1. *Suppose that $G = \langle g_1, \dots, g_r \rangle$ with $g_1 \cdots g_r = 1$. Then for any finite-dimensional kG -module V we have*

$$\sum_{i=1}^r \dim[g_i, V] \geq \dim V - \dim V^G + \dim[G, V].$$

We shall apply this when $r = 3$ and G has no fixed points on V or V^* . Noting that $\dim C_V(g_i) = \dim V - \dim[g_i, V]$, this gives

$$\sum_{i=1}^3 \dim C_V(g_i) \leq \dim V.$$

Recall our notation $C^a := \{x^a \mid x \in C\}$ for C a conjugacy class of G . The connection between our previous results on generation and the size of eigenspaces is made by:

Lemma 5.2. *Let k be algebraically closed. Let $x, y \in \mathrm{GL}_n(k) = \mathrm{GL}(V)$ be conjugate with product xy conjugate to x^2 , where $n \geq 2$. Set $G = \langle x, y \rangle$. If V contains no 1-dimensional kG -submodules and has no 1-dimensional kG -quotient module, then every eigenspace of x has dimension at most $n/3$.*

Proof. Let θ be an eigenvalue of x with the θ -eigenspace of maximal dimension among all eigenspaces. Set $z = (xy)^{-1}$,

$$x' = \theta^{-1}x, \quad y' = \theta^{-1}y, \quad z' = \theta^2z.$$

Then $x'y'z' = 1$. By hypothesis, V and V^* have no fixed points for $H = \langle x', y' \rangle$. Note that the fixed space of each of these elements has dimension at least that of the θ -eigenspace of x , so an application of Scott's Lemma to this triple shows that this dimension is at most $n/3$. \square

Let's say that a finite group G has property (E) if there exists $g \in G$ such that for any algebraically closed field k and any kG -module V for which G has no fixed points on V or V^* , every eigenspace of g on V has dimension at most $(1/3) \dim V$. Note that nontrivial irreducible representations of a group G with property (E) are necessarily of dimension at least 3; in particular, G is perfect. We will say that G has property (E) in characteristic p if the result holds for modules over fields of characteristic p .

Corollary 5.3. *Let G be a finite nonabelian simple group other than $L_2(q)$ with q even. Then G has property (E). All finite nonabelian simple groups have property (E) in characteristic not 2.*

Proof. Let $x, y \in G$ as in Theorem 1.1(b). Then G has property (E) with respect to $g := x$. The result follows by the previous lemma unless $G = L_2(q)$ with q even or $q = 7$. If $q = 7$ or we are considering modules in any characteristic other than 2 and q is even, the result follows for irreducible modules by Lemma 3.15 (and the remarks above it). For any eigenvalue other than 1, property (E) can be checked on irreducible modules. The condition for the eigenvalue 1 follows by Scott's Lemma from Theorem 1.1. \square

The same proof in the remaining cases yields:

Corollary 5.4. *Let G be a finite nonabelian simple group and k an algebraically closed field of characteristic p . There exists $x \in G$ such that if V contains no composition factors of dimension at most 2, then every eigenspace of x has dimension at most $(1/3) \dim V$.*

We now move towards composite groups:

Lemma 5.5. *Let $G = G_1 \times G_2$ be a direct product of finite groups. Assume that G_1 and G_2 both have property (E). Then so does G .*

Proof. We may assume that k is algebraically closed. Let $g_i \in G_i$ as in property (E). We claim that $g := (g_1, g_2) \in G$ satisfies (E) for G . As in the previous proof we may assume that V is irreducible. Thus, $V = V_1 \otimes V_2$, with V_i irreducible for G_i and at least one of them not the trivial module, say V_1 .

By assumption every eigenspace of g_1 on V_1 has dimension at most $(1/3) \dim V_1$. Choose a g_2 -invariant filtration $0 < W_1 < \dots < W_r = V_2$ of V_2 with 1-dimensional quotients, so $r = \dim V_2$. It is clear that on $V_1 \otimes (W_{j+1}/W_j)$ each eigenspace of g has the same dimension as an eigenspace of g_1 and so of dimension at most $(1/3) \dim V_1$. The result follows. \square

The previous result implies that direct products of finite nonabelian simple groups have property (E) in any characteristic not 2, and also in characteristic 2 as long as we avoid $L_2(q)$ with q even.

In this last case, we will need a different result. If S is a finite subset of $GL(V)$, let $\text{avg}(S, V) := |S|^{-1} \sum_{s \in S} \dim C_V(s)$.

Corollary 5.6. *Let $G = L_1 \times \dots \times L_t$ where $L_i \cong L_2(q)$ with $q \geq 4$ even. Let k be an algebraically closed field of characteristic 2. Let V be a kG -module with no trivial composition factors. Let $X = X_1 \times \dots \times X_t$ where $X_i \leq L_i$ is cyclic of order $q + 1$.*

- (a) $\text{avg}(X, V) \leq (1/3) \dim V$.
- (b) *There exists $x \in X$ with $\dim C_V(x) < (1/3) \dim V$.*

Proof. Clearly the second statement follows from the first. To prove the first statement, it suffices to assume that V is irreducible. So $V = V_1 \otimes \dots \otimes V_t$ with each V_i an irreducible kL_i -module (and at least one nontrivial). By Lemma 3.16 we have that $C_V(X) = 0$. Since $|X|$ is odd, the result follows by [26, Thm. 1.1]. \square

Combining the previous results yields:

Corollary 5.7. *Let G be a direct product of a finite number of isomorphic nonabelian simple groups. Let k be an algebraically closed field and V be a kG -module with no trivial composition factors. Then there exists $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

We can now solve a conjecture stated in the 1966 thesis of Peter Neumann [45]. There are two new ingredients in our proof. The first is the previous result. However, we also improve his result even for solvable groups. The idea is to consider the average dimension over some coset of a normal subgroup. This result does require the irreducibility assumption (consider the augmentation ideal for an elementary abelian 2-group in any odd characteristic).

Theorem 5.8. *Let G be a finite group acting irreducibly and nontrivially on the kG -module V . There exists an element $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

Proof. Let $R := \text{End}_{kG}(V)$. This is a division ring. We may replace k by the center of R , and so R is a central simple algebra over k . Now extend k to a Galois splitting field L of R . Then $V \otimes_k L$ is a direct sum of Galois conjugates of V . Any element has the same size fixed space on each of these conjugates. We can then extend scalars and assume that k is algebraically closed, so there is no harm in assuming that V is absolutely irreducible.

Let N be a minimal normal subgroup of G . If N is an elementary abelian p -group for $p > 2$, the result follows by [32] (see also [26, Thm. 1.1]).

Suppose that $F(G) = 1$. Then $N = L_1 \times \cdots \times L_t$ is a direct product of isomorphic nonabelian simple groups and V is a completely reducible kN -module with no fixed points. The result follows by Corollary 5.7.

The remaining case is when N is an elementary abelian 2-group. If N acts homogeneously on V , then N is central and there is a fixed point free element in N . Let $\Omega = \{V_1, \dots, V_m\}$ denote the homogeneous components of N with $m > 1$. Then G acts transitively on Ω . Thus, there exists $g \in G$ with no fixed points on Ω .

We will prove that $\text{avg}(gN, V) \leq (1/3) \dim V$. This completes the proof for then certainly some element in the coset gN has fixed point space of dimension at most $(1/3) \dim V$. Let $\Delta \subseteq \Omega$ be an orbit for g with $\delta = |\Delta|$. Let $W = \bigoplus_{i \in \Delta} V_i$. We will in fact prove that $\text{avg}(gN, W) \leq (1/3) \dim W$ and clearly this suffices. Obviously, $\dim C_W(gy) \leq (1/\delta) \dim W$ for every $y \in N$. Thus, if $\delta > 2$, our assertion has been proved. It remains to consider the case that $\delta = 2$. By reordering, we may assume that $W = V_1 \oplus V_2$. Consider the image of N in $\text{GL}(W)$. Since the V_i are distinct nontrivial weight spaces for N , the image of N in $\text{GL}(W)$ is M , an elementary abelian group of order 4. In computing this average on W , we may mod out by the kernel of the action of N on W and so we are averaging over the coset gM of size 4. Let $M = \{1, z_1, z_2, z\}$, where z_i is trivial on V_i (and so acts as -1 on the other factor).

Write $g = (s, t)\tau$ in $\text{GL}(W)$, where τ is an involution interchanging coordinates (identify V_1 with V_2). Then $g^2 = (st, ts)$ and so we see that $c := \dim C_W(g) = \dim C_{V_1}(st)$. Note that $(gz)^2 = g^2$ and $(gz_i)^2 = g^2 z$. Thus, $\dim C_W(gz) = \dim C_W(g) = c$ and $\dim C_W(gz_i) \leq \dim V_1 - c$ (since $g^2 z$ and g^2 have no common fixed points). Thus,

$$\begin{aligned} \text{avg}(gN, W) &= \frac{1}{4}(2 \dim C_W(g) + 2 \dim C_W(gz_i)) \\ &\leq \frac{1}{4} 2 \dim V_1 = \frac{1}{4} \dim W < \frac{1}{3} \dim W. \end{aligned}$$

This completes the proof. □

Remark 5.9.

- (1) Neumann [45] proved that for solvable G there exists an element $g \in G$ with $\dim C_V(g) \leq (7/18) \dim V$. Segal and Shalev [48], using the classification of finite simple groups, showed that for all groups one could obtain $(1/2) \dim V$ as a bound. Isaacs et al. [32] improved this to $(1/p) \dim V$ as long as V is a completely reducible G -module (where p is the smallest prime dividing the order of G ; for $p = 2$, they used the classification of finite simple groups via a result of [23]). Maróti and the first author [26] improve this by showing that one can take V to be any module with no trivial composition factors and improve the bound to strictly less than $(1/p) \dim V$, where p is the smallest prime divisor of $|G|$.

- (2) As we have already noted, one cannot improve the $1/3$. See the next section for examples, showing that even for arbitrarily large dimension, one cannot do better than $1/9$.

We close this section by extending our result to infinite linear groups as announced in Theorem 1.3 of the introduction:

Theorem 5.10. *Let G be a nontrivial irreducible subgroup of $\mathrm{GL}(V)$ with V a finite-dimensional vector space over a field k . There exists $g \in G$ with $\dim C_V(g) \leq (1/3) \dim V$.*

Proof. As in the proof of Theorem 5.8 there is no harm in assuming that V is absolutely irreducible. Let $n := \dim(V)$. By passing to a subgroup we may assume that G is finitely generated. By passing to the subfield of k generated by the matrix entries of the finitely many generators and their inverses we may assume that k is finitely generated as a field over the prime field. Indeed, we may assume that $G \leq \mathrm{GL}_n(R)$, where R is a finitely generated subring of k (whose quotient field is k). Let M be a maximal ideal of R such that the image \bar{G} of G in $\mathrm{GL}_n(R/M)$ is still absolutely irreducible. (This can be easily done. Choose n^2 elements of G that form a basis for $M_n(k)$. This is an open condition on the spectrum of R and so holds for a dense subset of maximal ideals of R .)

By the Nullstellensatz, R/M is finite, so by the result for finite groups in Theorem 5.8, we may choose an element $\bar{g} \in \bar{G}$ whose fixed space has dimension at most $n/3$. This is equivalent to the rank of $I - \bar{g}$ being at least $(2/3)n$, whence the same is obviously true for any lift $g \in G$ of \bar{g} . \square

6. SOME CHARACTERISTIC 0 RESULTS

Under suitable circumstances, one can improve Theorem 1.3. If G is a compact Lie group (or complex algebraic group), then as the dimension increases, the dimension of any weight space of a maximal torus divided by the dimension tends to 0 [24, Thm. 6].

Here, we specialize to irreducible complex representations of nonabelian simple groups where we prove much better upper bounds for the maximal size of eigenspaces of suitable elements.

Theorem 6.1. *For any $\epsilon > 0$ there exists $N > 0$ with the following property: for all finite quasi-simple groups G there exists $g \in G$ so that for all irreducible $\mathbb{C}G$ -modules V of dimension $\dim V > N$ every eigenspace of g is of dimension at most $\epsilon \dim V$.*

Proof. We first consider the case that G is quasi-simple of Lie type. Furthermore, we may assume that G is not one of the finitely many exceptional covering groups. Now for $G = \mathrm{SL}_2(q)$, $q \geq 5$, let g be a regular semisimple element of odd order $(q-1)/2$ or $(q+1)/2$, and otherwise let g be (a lift to the central extension G of) a regular semisimple element of order $\Phi_e^*(q)$ in the maximal torus T of $G/Z(G)$ as given in Table 7 for classical groups, respectively as in Table 6 for exceptional groups. Note that such regular semisimple elements exist whenever there is a suitable Zsigmondy prime, that is, in all but finitely many cases. Then $|C_G(g)| = |T|$. Let V be an irreducible $\mathbb{C}G$ -module, with character χ , and set $d := \dim V = \chi(1)$. Then, the multiplicity of any linear character λ of $H := \langle g \rangle$ in $\chi|_H$ is

$$\langle \chi, \lambda \rangle_H = \frac{1}{|H|} \sum_{t \in H} \chi(t) \bar{\lambda}(t) \leq \frac{1}{|H|} \left(d + |H| |T|^{1/2} \right).$$

Thus, any eigenspace of g on V has at most dimension $(\frac{1}{|H|} + \frac{|T|^{1/2}}{d}) \dim V$. Since $|H| = \Phi_e^*(q)$ goes to infinity as q^e does and since $|T|^{1/2}/d \rightarrow 0$ (by [49, Table 1]), the claim follows.

Next consider $G = \mathfrak{A}_n$. Let x be a cycle of odd length $n - e$ with $e = 2$ or 3 . For sufficiently large n , it follows by [35, Thm. 1.2] that $|\chi(x^j)| < \chi(1)^{1/2}$ for all $x^j \neq 1$. Now let H be the subgroup generated by such an x . Arguing as we did for the case of Lie type groups, we see that this implies that the multiplicity of any irreducible character of H in the restriction of a nontrivial character χ of \mathfrak{A}_n is less than $\chi(1)/(n - e) + \chi(1)^{1/2}$. The result follows.

Suppose that G is the double cover of \mathfrak{A}_n . Let π be the projection from G onto \mathfrak{A}_n . Let $x \in G$ with $\pi(x)$ a product of a 2-cycle and 2^f -cycle where $n/2 \leq 2^f \leq n - 4$. It follows by [31, Thm. 3.9] that every noncentral element y of $H = \langle x \rangle$ is conjugate to yz , where z is the central involution in G . Thus $\chi(y) = 0$ for every such y if χ is a faithful character of G . This implies that every eigenspace of x is either 0-dimensional or has dimension $\chi(1)/2^f$.

Since the result is asymptotic, we need not consider sporadic groups or the covers of \mathfrak{A}_6 and \mathfrak{A}_7 . □

We give two sample results showing how the bound obtained in the proof of the previous theorem can be strengthened with a bit more work for the groups of Lie type.

Proposition 6.2. *Let $G = E_8(q)$. Then there exists $g \in G$ such that for every irreducible $\mathbb{C}G$ -module V the dimension of every eigenspace of g on V is at most $(1/q^8) \dim V$.*

Proof. Let $g \in G$ of order $\Phi_{30}(q) = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$. Then g generates a TI-torus T of G , with $|N_G(T)/T| = 30$ (see Table 6). Let $\chi \in \text{Irr}(G)$ be a nontrivial character. By Proposition 3.3 we have $|\chi(s)| \leq 30$ for all powers $s = g^b \neq 1$ of g . Thus, the multiplicity of any linear character of T in $\chi|_T$ is at most

$$\frac{\chi(1) + 30|T|}{|T|} = \frac{\chi(1)}{|T|} + 30 \leq \frac{\chi(1)}{q^8}$$

as claimed, since $\chi(1) > q^{28}$ by [39]. □

Proposition 6.3. *Let $G = O_{2n}^-(q)$. Then there exists $g \in G$ such that for every irreducible $\mathbb{C}G$ -module V the dimension of every eigenspace of g on V is at most $(1/\Phi_{2n}^*(q)) \dim V + n$.*

Proof. Consider G as the derived subgroup of $\text{PCO}_{2n}^{\circ -}(q)$ and let $g \in G$ of order $\Phi_{2n}^*(q)$. Then g is a regular element in a cyclic maximal torus of $\text{PCO}_{2n}^{\circ -}(q)$ of order $q^n + 1$, and any nontrivial power of g is conjugate to precisely n of its powers. Let $\chi \in \text{Irr}(G)$ be a nontrivial character. By Proposition 3.3 we have $|\chi(s)| \leq n$ for all powers $s = g^b \neq 1$ of g . Thus, the multiplicity of any linear character of $H := \langle g \rangle$ in $\chi|_H$ is at most

$$\frac{\chi(1) + n|H|}{|H|} = \frac{\chi(1)}{|H|} + n,$$

as claimed. □

The following examples show that (as opposed to the simple group case) even in characteristic 0, one cannot get arbitrarily small ratios for $\dim C_V(g)/\dim V$ as $\dim V$ increases (and V is irreducible).

Example 6.4. Let $L = \mathfrak{A}_5$ and let W be an irreducible 5-dimensional module in characteristic 0 (all we need assume is that the characteristic is not 2).

Set $G(m) = L \times \cdots \times L$ (m copies) acting on $V(m) = W \otimes \cdots \otimes W$ (m copies). Then $\dim C_{V(m)}(g) > (1/50) \dim V(m)$ for all $g \in G(m)$.

Proof. If g has order 5, then $\chi_{V(m)}(g) = 0$ and $\dim C_{V(m)}(g) = (1/5) \dim V(m)$ for all m .

If g has order 2, we claim that $\dim C_{V(m)}(g) > (1/2) \dim V(m)$. By induction on m , it suffices to assume that $g = (h, \dots, h)$ with $h \in L$ of order 2. Then $\chi_{V(m)}(h) = 1$, whence the trivial eigenspace of g has dimension $(1/2)(\dim V(m) + 1) > (1/2) \dim V(m)$ (but as m increases, the ratio gets arbitrarily close to $1/2$).

If g has order 3, then $\chi_{V(m)}(h) = \pm 1$, whence the trivial eigenspace of g has dimension at least $(1/3)(\dim V(m) - 2) \geq (1/5) \dim V(m)$ (and $1/5$ is achieved for $m = 1$).

Now take g arbitrary. We may write (up to reordering) $g = g_1 \otimes g_2 \otimes g_3 \otimes g_5$ acting on $V(a_1) \otimes V(a_2) \otimes V(a_3) \otimes V(a_5)$ with $m = \sum a_i$ and g_i has each component of order i . Thus, g_1 is trivial on $V(a_1)$ and by the previous results, $\dim C_{V(a_i)}(g_i) \geq (1/5) \dim V(a_i)$ for $i = 3, 5$ and $\dim C_{V(a_2)}(g_2) > (1/2) \dim V(a_2)$. Thus, the result follows. \square

We get a similar result for \mathfrak{A}_4 . The proof is essentially the same as in the previous example:

Example 6.5. Let $L = \mathfrak{A}_4$ and let W be the irreducible 3-dimensional module in characteristic not 2. Set $G(m) = L \times \cdots \times L$ (m copies) acting on $V(m) = W \otimes \cdots \otimes W$ (m copies). Then $\dim C_{V(m)}(g) \geq (1/9) \dim V(m)$ for all $g \in G(m)$.

We next show that for direct products of simple groups and for sufficiently large dimension, Example 6.4 is the worst case.

Lemma 6.6. *Let L be a finite nonabelian simple group and V an irreducible nontrivial $\mathbb{C}L$ -module. Let $G = G(m)$ be the direct product of m copies of L and $V(m)$ be the tensor product of m copies of V . Let $\epsilon > 0$. If m is sufficiently large, then there exists an element $g \in G$ such that $\dim C_{V(m)}(g) < (1/50 + \epsilon) \dim V(m)$.*

Proof. Let χ be the character of V . Let e be the exponent of L (i.e. the smallest positive integer e such that $x^e = 1$ for all $x \in L$). Choose $g_1, \dots, g_s \in L$ such that the least common multiple of the orders of the g_i is e . Set $y = (g_1, \dots, g_s)$ in $G(s)$. Consider $(y, \dots, y) \in G(st)$ acting on $V(st)$. We see that for any $0 < j < e$ we have $|\chi(y^j)|/\chi(1)^{st} \rightarrow 0$ as t increases. It follows that $V(st)$ is very close to a free module for $\langle y \rangle$ and in particular

$$\lim_{t \rightarrow \infty} \frac{\dim C_{V(st)}(y)}{\dim V(st)} = \frac{1}{e}.$$

Thus, if m is sufficiently large, we can find $g \in G$ satisfying the conclusion unless $e \leq 50$. An easy inspection shows that $e > 50$ is true for every L aside from $L = \mathfrak{A}_5$.

So now suppose that $L = \mathfrak{A}_5$ (note that $e = 30$). So $\dim V = 3, 4$ or 5 . If $\dim V = 4$, an element of order 3 has no fixed points and so the same is true for an element of order 3 of the form $(x, 1, \dots, 1) \in L(m)$ for any m . If $\dim V = 5$, then V is a free module for an element of order 5. An element of order 3 has a 1-dimensional fixed space. If m is large enough, we can choose an involution whose fixed space has dimension very close to $(1/2) \dim V$. Arguing as above, we can choose an element $g \in L(m)$ whose fixed point

space has dimension as close as we want to $(1/50) \dim V(m)$, whence the result holds in this case.

Finally suppose that $\dim V = 3$. Every element of order 3 in $L(t)$ has a fixed space of dimension 3^{t-1} . Consider $g = (h, h^2)$ with h of order 5 acting on $V(2)$. Then the fixed space of g is 1-dimensional and so $(1/9) \dim V(2)$. An involution has a fixed space of dimension 1 on V . Thus, we see that there is an element of order 30 acting on $V(m)$ for any $m \geq 4$ with $\dim C_V(g) = (1/81) \dim V(m)$. \square

We can extend the previous result to the case of primitive groups.

Theorem 6.7. *Let G be a finite group and W an irreducible primitive $\mathbb{C}G$ -module. Let s be any positive number greater than $1/50$. If $\dim W$ is sufficiently large, then there exists $g \in G$ such that $\dim C_W(g) < s \dim W$.*

Proof. We may assume that W is faithful. Any normal subgroup of G acts homogeneously on W , whence any abelian normal subgroup of G is central. If $Z(G) \neq 1$, the result is clear. So we may assume that $F(G) = 1$. So $F^*(G) = L_1 \times \cdots \times L_t$ with L_i simple, and every irreducible $F^*(G)$ -submodule of W is isomorphic to $V_1 \otimes \cdots \otimes V_t$, where V_i is a nontrivial irreducible L_i -module. If $\dim V_i$ is large enough, it follows by Theorem 6.1 that there exists $g_i \in L_i$ with fixed space of dimension less than $(1/50) \dim V_i$, a contradiction. Thus there are only finitely many possible isomorphism types for the L_i . We may assume that t is as large as we wish (otherwise $F^*(G)$ has bounded order, whence so does $|G|$ and so $\dim V$ is bounded). So we may assume that $L_i \cong L_1$ for $1 \leq i \leq m$ for m as large as we wish and that $V_i \cong V_1$ for those i (since there are only a bounded number of possible isomorphism types of irreducible modules). By the previous lemma, for m sufficiently large, there exists $(g_1, \dots, g_m) \in L_1(m)$ with $\dim C_{V(m)}(g) < s \dim V(m)$ with $V = V_1$. Setting $g = (g_1, \dots, g_m, 1, \dots, 1) \in F^*(G)$, we see that $\dim C_W(g) < s \dim W$, as required. \square

7. PRODUCTS OF CLASSES AND POWERS

A conjecture of Thompson asserts that for any finite nonabelian simple group there is a conjugacy class C such that $G = C \cdot C$, that is, any element of G is the product of two elements in C . A proof of this seems out of reach at present, although we expect that, in some sense, most classes will do. We propose the following partial results. First we consider rank 1 groups. Here, we set $G^\# := G \setminus \{1\}$.

Theorem 7.1. *Let G be a rank 1 finite simple group of Lie type. Let C be the G -conjugacy class of an element x of order $o(x) > 2$. Assume that one of the following holds:*

- (1) $G = L_2(q)$ with q odd and x is not unipotent;
- (2) $G = L_2(q)$ with q even and $o(x)$ does not divide $q + 1$;
- (3) $G = {}^2G_2(q^2)$, $q^2 \geq 27$, and $o(x)$ is not divisible by 3;
- (4) $G = {}^2B_2(q^2)$, $q^2 \geq 8$; or
- (5) $G = U_3(q)$ and x is regular of order $(q^2 - q + 1)/d$ or $(q^2 - 1)/d$, with $d = \gcd(3, q + 1)$.

Then $G^\# \subseteq CC$.

Proof. If $G = L_2(q)$, this is a straightforward matrix computation; see also Macbeath [41]. For the Suzuki groups ${}^2B_2(q^2)$ the generic character table is available in Chevie and

the claim can be checked by computer. (By [21, Thm. 2] we actually only need to worry about the classes of elements of order 4.) Similarly, for the Ree groups ${}^2G_2(q^2)$, $q^2 \geq 27$, by loc. cit. and our restriction on C we only have to check that the square of any class of semisimple elements of order greater than 2 meets all nonsemisimple classes, which is immediate using the table in Chevie.

Finally, the character table of $U_3(q)$ can also be found in Chevie, and we only need to verify that squares of regular semisimple classes of order $(q^2 - q + 1)/d$ or $(q + 1)/d$ contain all nonsemisimple classes. \square

This has the following immediate consequence:

Theorem 7.2. *Let w_1 and w_2 be nontrivial words in the free group on d generators.*

- (a) *If $G = {}^2B_2(q^2)$, $q^2 \geq 8$ and $w_i^2(G^d) \neq 1$ for $i = 1, 2$, then $G = w_1(G^d)w_2(G^d)$.*
- (b) *If $G = {}^2G_2(q^2)$, $q^2 \geq 27$, and $w_i^9(G^d) \neq 1 \neq w_i^6(G^d)$ for $i = 1, 2$, then $G = w_1(G^d)w_2(G^d)$.*

The main result of [36] is a version of this for any pair of words w_1 and w_2 and any sufficiently large nonabelian simple group (where sufficiently large depends on the choice of w_1 and w_2).

Next we consider some rank 2 groups.

Theorem 7.3. *Let G be a simple group $L_3(q)$ ($q > 2$), $S_4(q)$, $G_2(q)$, ${}^3D_4(q)$ or ${}^2F_4(q^2)'$. Then there exists a conjugacy class C of semisimple elements of G such that $G^\# \subseteq CC$.*

TABLE 10. Conjugacy classes in some rank 2 groups

| G | $o(x)$ |
|-----------------------|---|
| $L_3(q)$ | $(q^2 + q + 1)/(3, q - 1)$ or $(q^2 - 1)/(3, q - 1)$ |
| $S_4(q)$, q even | $q^2 - 1$ |
| $S_4(q)$, q odd | $(q^2 + 1)/2$ |
| $G_2(q)$, $q \geq 3$ | $(q^2 + q + 1)/(3, q - 1)$ |
| ${}^3D_4(q)$ | $q^4 - q^2 + 1$ |
| ${}^2F_4(q^2)$ | Φ'_{24} |

Proof. Let C be the conjugacy class of a regular semisimple element x of order as given in Table 10. We claim that the (C, C, C') structure constant is nonzero for any nontrivial conjugacy class C' of G . For the first four families of groups, the complete generic character table is available in the Chevie-system, and the claim can be checked by computer.

The group ${}^2F_4(2)'$ is covered by the square of class 13a, so it remains to consider ${}^2F_4(q^2)$ for $q^2 \geq 8$. Here, the complete character table is known in principle, but is only partly contained in Chevie. Now note that for any class C' of semisimple elements, our claim follows by the elementary observation [21, Thm. 2]. By Lemma 3.2 the irreducible characters not vanishing on C are the irreducible Deligne–Lusztig characters $R_{T,\theta}$, with $|T| = \Phi'_{24}$, and some of the unipotent characters.

Let y be a nonsemisimple element of G . By [6, Prop. 7.5.3] we have $R_{T,\theta}(y) = 0$ unless the semisimple part of y is conjugate to an element of T . Since all nonidentity elements of T are regular, this implies that $R_{T,\theta}(y) = 0$ unless y is unipotent. In the latter case, $R_{T,\theta}(y)$ does not depend on θ by [6, Cor. 7.2.9]. Let $I := \{\pm R_{T,\theta} \mid 1 \neq \theta \in \text{Irr}(T)\} \subset \text{Irr}(G)$ and $I' := \text{Irr}(G) \setminus I$. By the orthogonality relations we have $|\sum_{x \in I} \chi(x)^2| < |T|$. Writing $a := R_{T,\theta}(y)$, $d := R_{T,\theta}(1)$ we find

$$\begin{aligned} |n(C, C, C')| &= \frac{|C|^2}{|G|} \left| \sum_{x \in I} \frac{\chi(x)^2 \chi(y)}{\chi(1)} + \sum_{x \in I'} \frac{\chi(x)^2 \chi(y)}{\chi(1)} \right| \\ &\geq \frac{|C|^2}{|G|} \left(\left| \sum_{x \in I'} \frac{\chi(x)^2 \chi(y)}{\chi(1)} \right| - \frac{|a|}{d} |T| \right). \end{aligned}$$

Now $a = R_{T,\theta}(y)$ is the value of a Green function and these have been determined by the second author [42], from which we get $|a| \leq q^{16} + 2q^{15}$. Since $|T| \leq q^4 + 2q^3$ and $d = |G|_{2'}/|T| \geq q^{20}$ we have $|a| \cdot |T|/d < 1/2$. It can now be computed from the unipotent part of the character table in Chevie that $n(C, C, C') > 0$ for all unipotent classes C' . \square

Remark 7.4. It's easily seen that for all simple groups in Theorems 7.1 and 7.3 at least one of the classes is real, so Thompson's conjecture holds for all these groups.

For the other types of simple groups, we give an approximation by showing that $G^\#$ is covered by a product of two classes.

For most families of simple classical groups of Lie type this was already shown in [44, Thm. 2.1–2.6]:

Theorem 7.5 (Malle–Saxl–Weigel (1994)). *Let G be a simple classical group of Lie type not of type $O_{4n}^+(q)$ and different from $U_3(3)$ and $O_8^-(2)$. Then there are two conjugacy classes of G whose product covers $G^\#$.*

It is straightforward to check from their character tables that this continues to hold for $U_3(3)$ and $O_8^-(2)$.

We next handle the remaining family of classical groups, giving a small improvement of the argument in [36, §7] for $O_{4n}^+(q)$, $n > 2$.

Theorem 7.6. *Let G be a simple classical group of Lie type $O_{4n}^+(q)$ with $n \geq 2$. Then there exist two conjugacy classes of G whose product covers $G^\#$.*

Proof. If $n = 2$, we choose the two classes as in [44, Thm. 2.7], so that only three irreducible characters do not vanish on either class, which moreover are unipotent. The values of the unipotent characters of a group of type D_4 are contained in Chevie, and one computes that the result holds.

Now assume that $n \geq 3$. Let C_1 be the class of an element of order a Zsigmondy prime divisor of $q^{2n-1} - 1$ inside the subgroup $GL_{2n-1}(q)$ and C_2 the class of an element of order the product of a Zsigmondy prime divisor of $q^{2n-2} + 1$ with a Zsigmondy prime divisor of $q^2 + 1$, inside a subgroup $\Omega_{4n-4}^-(q) \times \Omega_4^-(q)$, as in [36, §7]. The claim is proved in the last section of that paper aside from a small number of cases. There are precisely 3 nontrivial characters that vanish on neither C_1 nor C_2 described there (the Steinberg character, γ and δ) which take on the value ± 1 on each C_i . We want to show that any

nontrivial class C_3 is contained in C_1C_2 . By a result of Gow [21], we may assume that C_3 consists of nonsemisimple elements and so the Steinberg character vanishes on C_3 . By a general bound of Gluck [20, Thm. 1.11 and 5.3], $|\gamma(C_3)| \leq (19/20)\gamma(1)$. We use the trivial estimate that $|\delta(C_3)| \leq |C_G(z)|^{1/2} < (1/20)\delta(1)$ for $z \in C_3$. \square

Next, we extend this result to the exceptional groups of Lie type. (For those of small rank, it has already been shown above.)

Theorem 7.7. *Let G be a simple group $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$. There exist two conjugacy classes of semisimple elements of G whose product covers $G^\#$.*

TABLE 11. Conjugacy classes in exceptional groups

| G | $o(x_1)$ | $o(x_2)$ | χ |
|--------------|-------------------------------|-------------|---------------------------------|
| $F_4(q)$ | Φ_{12} | Φ_8 | $1, F_4[i], F_4[-i], \text{St}$ |
| $E_6(q)$ | $\Phi_9/(3, q-1)$ | Φ_8 | $1, \text{St}$ |
| ${}^2E_6(q)$ | $\Phi_{18}/(3, q+1)$ | Φ_8 | $1, \text{St}$ |
| $E_7(q)$ | $(\Phi_2\Phi_{18})_{\{2,3\}}$ | Φ_7 | $1, \text{St}$ |
| $E_8(q)$ | Φ_{20} | Φ_{24} | $1, E_8[i], E_8[-i], \text{St}$ |

Proof. For each type, we choose C_i to contain semisimple elements x_i of order as indicated in Table 11. (Such elements exist since G contains maximal tori with cyclic subgroups of that order.)

We first determine the irreducible characters of G simultaneously not vanishing on both classes. It is easy to check that no nontrivial element of G_{ad} has centralizer order divisible by Zsigmondy primes p_1, p_2 for both element orders (for example, for $G = F_4(q)$ using that the only semisimple algebraic group of rank at most four whose order polynomial is divisible by both Φ_8 and Φ_{12} is F_4). Thus, by Lemma 3.2, only unipotent characters may possibly take nonzero values on both C_1, C_2 .

The list in [6, 13.9] shows that apart from the two, respectively four, characters χ listed in Table 11 (where $1_G, \text{St}$ denote the trivial and the Steinberg character, and otherwise the notation is as in loc. cit.) all other unipotent characters have degree divisible by at least one of the two Zsigmondy primes p_i , hence are of p_i -defect 0. Thus, only the listed characters may potentially not vanish on both C_1, C_2 .

Now let C be any nontrivial conjugacy class of G . We use the character formula ([43, Thm. I.5.8]) to estimate the structure constant $n(C_1, C_2, C)$. The value of the Steinberg character St on semisimple elements equals the p -part of their centralizer order, up to sign, and is zero on all other elements (see [6, Thm. 6.4.7]). The elements in both classes C_1, C_2 are regular, so $|\text{St}(x_i)| = 1$. Also, the values of the characters $F_4[\pm i]$ and $E_8[\pm i]$ on our regular semisimple elements have absolute value 1 (for example by block theory for the Zsigmondy primes p_i). Thus we are done if we can show that $|\chi(C)| < \chi(1)/3$ for the one or three nontrivial unipotent characters.

Now $\text{St}(1) = q^{24}, q^{36}, q^{36}, q^{63}, q^{120}$, respectively, and $F_4[\pm i](1) > q^{20}$, $E_8[\pm i](1) > q^{104}$. On the other hand, $|\chi(x)| \leq \sqrt{|C_G(x)|}$ for $x \in C$. The largest centralizers of nontrivial elements in G have order at most $q^{36}, q^{56}, q^{56}, q^{99}, q^{190}$, respectively, so we are done. \square

Finally, we note that:

Proposition 7.8. *Let G be a simple sporadic group or \mathfrak{A}_n , $n \geq 7$. Then there exist two conjugacy classes C of G whose elements have odd coprime order such that $G^\# \subseteq CC$.*

Proof. If G is sporadic, this is straightforward using the character tables. In fact, we can always choose both classes to contain elements of prime order $p > 2$ with this property.

Similarly, this is clear for \mathfrak{A}_n , $7 \leq n \leq 16$, with elements of orders

$$(5, 7), (3, 7), (3, 7), (5, 7), (5, 11), (5, 11), (11, 13), (11, 13), (11, 13), (7, 13),$$

respectively. If $n \geq 17$, we can take two classes of ℓ -cycles with $3n/4 \leq \ell \leq n - 2$ by Bertram [4, Thm. 1], and two such odd coprime ℓ exist unless $n = 18$. In the latter case we can also take C to contain elements of order 17. A random computer search shows that the square of one of these already covers $\mathfrak{A}_{18}^\#$. \square

Proof of Theorem 1.4. For all finite nonabelian simple groups G other than $L_2(q)$, $q = 7$ or 17, we produce two elements whose order is prime to 6 such that their classes C_1, C_2 satisfy $G^\# \subseteq C_1C_2$. If G is sporadic or an alternating group \mathfrak{A}_n with $n \geq 7$, the claim is an immediate consequence of Proposition 7.8. For $n = 5$ we use that the product of the classes 5a and 5b covers $\mathfrak{A}_5^\#$, and similarly for \mathfrak{A}_6 .

So assume that G is a simple group of Lie type. If G has rank 1, the result follows by Theorem 7.1. Indeed, for $L_2(q)$ with q odd, we take for x an element of order prime to 6 in one of the two maximal tori. Such elements will exist unless $q \in \{5, 7, 17\}$. The latter two cases have been excluded in the statement of (b), and the group $L_2(5) \cong \mathfrak{A}_5$ was already settled. For $L_2(q)$ with $q \geq 8$ even, take for x an element of order dividing $q - 1$ and prime to 3. For ${}^2G_2(q^2)$, take any elements of order prime to 6, for ${}^2B_2(q^2)$ take any elements of odd order; finally, for $U_3(q)$, $q > 2$, take elements of order $(q^2 - q + 1)/\gcd(3, q + 1)$ (which is prime to 6).

For the groups of rank 2 in Theorem 7.3, we may take for C the class occurring in Table 10, except for $S_4(2^f)$, which is covered by the product of any two distinct classes of elements of order $q^2 + 1$. The remaining exceptional groups are covered by the product of two classes as in Table 11, which consist of elements of order prime to 6.

For the groups occurring in Theorem 7.5 which have not yet been discussed, it is straightforward to check from [44] that the two conjugacy classes can be taken to have order a Zsigmondy prime greater than 3 except possibly for

$$L_6(2), L_7(2), U_4(2), U_6(2), U_7(2), S_6(2), S_{12}(2).$$

Now $L_6(2)^\#$ is covered by the square of class 31a, $L_7(2)^\#$ by the square of 127a, $U_4(2)$ by the square of 5a, $U_6(2)$ and $S_6(2)$ by the square of 7a, and $S_{12}(2)$ by the square of class 31a. For $G = U_7(2)$ the character table is not available in GAP. We claim that the product of classes of elements of orders 43 and 11 covers $G^\#$. First, by Lemma 3.2 it is easy to see that only (some) unipotent characters take nonzero values on both classes. These are contained in Chevie, and the claim can then be verified. The group $O_8^-(2)$ excluded in Theorem 7.5 is covered by the square of class 17a.

For the 8-dimensional orthogonal groups of plus type, the classes in [44, Thm. 2.7] can be chosen to contain elements of order prime to 6, except for $O_8^+(2)$. The latter group

is covered by the square of class 7a. For $n \geq 3$, the two classes for $O_{4n}^+(q)$ chosen in Theorem 7.6 consist of elements of order prime to 6.

Finally, it is straightforward to see that any element of $L_2(q)$ is a product of two unipotent elements. \square

In [36], a weaker version of Theorem 1.4 was proved.

We obtain the following consequence:

Theorem 7.9. *Let G be a finite nonabelian simple group. Let m be a prime power. Then every element of G is a product of two m th powers.*

Proof. By Theorem 1.4 we may assume that $\gcd(m, 6) = 1$. Now for G sporadic or $G = \mathfrak{A}_n$, $n \geq 7$, our claim follows from Proposition 7.8. The groups \mathfrak{A}_5 and \mathfrak{A}_6 are both covered by products of two 3-elements or two 5-cycles.

So assume that G is a group of Lie type. Let B denote a Borel subgroup of G and U^- the opposite of the unipotent radical of B . If $\gcd(m, |B|) = 1$, we use Chernousov–Ellers–Gordeev [7, Thm. 2.1], which asserts that every element of G is conjugate to an element of U^-B , and so a product of two m th powers.

So now assume that $\gcd(m, |B|) \neq 1$. For all groups G of rank 1 except possibly $L_2(2^f)$, by Theorem 7.1 there exists a conjugacy class of elements of order prime to $|B|$ whose square covers $G^\#$. For $L_2(2^f)$ it's easily seen that any element is a product of two elements of order dividing $q + 1$. Similarly, for the groups in Theorem 7.3 the claim is clear except for $G = S_4(2^f)$. Here, again $G^\#$ is also covered by products of two elements of order dividing $q^2 + 1$. For all other groups, we have already argued in the previous proof that they can be covered by products of two elements whose order is prime to $|B|$. \square

8. FURTHER GENERATION RESULTS

We use our results on overgroups of suitable cyclic subgroups in simple groups to derive the following:

Theorem 8.1. *Let S be a finite simple group different from $O_8^+(2)$. There exists a conjugacy class C of S consisting of elements of order prime to 6 such that if $1 \neq x \in S$, then $S = \langle x, y \rangle$ for some $y \in C$.*

In the one exception, we can instead take C to be a class of elements of order 15 (and so in all cases, there is a class C of elements of odd order satisfying the conclusion). Moreover, if $1 \neq x \in S$ has odd order, then we can choose the class to consist of elements of order 7.

Before we begin the proof, we point out some easy consequences including the affirmative answer to a question of Getz [19]. Recall that a quasi-simple group is a perfect central cover of a simple group.

Corollary 8.2. *Let S be a finite quasi-simple group. If T is a solvable subgroup of S , then there exists a solvable subgroup $T_1 \geq T$ and an element $s \in S$ of order prime to 6 such that $S = \langle T_1, s \rangle$.*

Proof. It is trivial to reduce to the case that S is simple (elements of order prime to 6 in the simple group can be lifted to elements of order prime to 6 in a covering group).

The result is now immediate unless $S = \text{O}_8^+(2)$. Consider that case. Let T_1 be a maximal solvable subgroup of S containing T . The result follows by the remarks above unless T_1 is a 2-group. However, it is clear that a Sylow 2-subgroup of S is not a maximal solvable subgroup of S (it is contained in a minimal parabolic subgroup which is still solvable). \square

Corollary 8.3. *Let S be a finite quasi-simple group. Then S can be generated by two conjugate elements of order prime to 6.*

In the proof of the theorem, we need the following observation (see Guralnick [22, 2.2] for a slightly different proof):

Lemma 8.4. *Let C be a nontrivial conjugacy class in a finite simple group G . Then C is not contained in the union of any two proper subgroups.*

Proof. Suppose that C is contained in $X \cup Y$, with X, Y proper subgroups. Replacing X and Y by maximal subgroups, we still have the hypothesis and C is not contained in either X or Y since clearly $G = \langle C \rangle$.

Choose $x \in C \cap (X \setminus Y)$. Note that if $y \in Y$, then $x^y \in X$ (for $x^y \in Y$ implies that $x \in Y$). Thus $\langle x^Y \rangle$ is contained in X and normalized by Y obviously and also by x . Since Y is maximal, $G = \langle Y, x \rangle$ normalizes the proper subgroup $\langle x^Y \rangle \leq X$, a contradiction. \square

Example 8.5. Note that one cannot replace 2 by 3 in the lemma: take $G = \text{SL}_n(2)$ or $\text{Sp}_{2n}(2)$ and let X, Y, Z be the stabilizers in G of three vectors in a 2-space. Then every transvection of G fixes a hyperplane and so fixes at least one of the vectors in this 2-space. Thus the class of transvections is contained in the union of three subgroups. A similar argument applies to the class of transpositions in the nonsimple group \mathfrak{S}_n .

Proof of Theorem 8.1. We use two types of standard arguments. In the first situation, let's call it (S1), we let y be an element as in Theorem 1.1(a), of order prime to 6. If there are no more than two maximal subgroups of S containing y , then by Lemma 8.4 any conjugacy class in $S \setminus \{1\}$ contains an element x outside of these maximal subgroups, whence $S = \langle x, y \rangle$. In some of the cases where there are more than 2 maximal subgroups, we compute (as in [5]) directly that no conjugacy class is contained in the union of the maximal subgroups containing y .

In the second situation (S2), we produce two conjugacy classes C_2, C_3 of S , at least one of them containing elements of order prime to 6, such that the (C, C_2, C_3) -structure constant is nonzero for any nontrivial conjugacy class C of S and such that no maximal subgroup of S can contain elements from both C_2 and C_3 , in which case we're done again.

Assume first that S is sporadic. Let y be an element of prime order as in Table 9. Then unless

$$S \in \{M_{12}, Ti, HS, McL, Suz, Fi_{22}\}$$

we are in situation (S1). It is easily checked from the character tables that in each of the six exceptions S listed above, for any prime p there are less elements of order p in the (disjoint) union of the relevant maximal subgroups than in any class of elements of order p in S , except for elements of order 5 in HS , elements of order 3 in Suz , and elements of order 2 or 3 in Fi_{22} . In HS , we reach situation (S2) with $C_2 = 11a$ and $C_3 = 20a$; and in both Suz and Fi_{22} with $C_2 = 11a$ and $C_3 = 13a$.

Now let S be of exceptional Lie type. Here, we take y to be an element generating a cyclic subgroup as in Table 6. Note that the order of y is coprime to 6 unless possibly when $S = E_7(q)$. Again, y is contained in at most two maximal subgroups, except for $S \in \{G_2(3), F_4(2)\}$, and we may conclude as before. For $G_2(3)$ and $F_4(2)$ we are in situation (S2) with the classes $9a, 13a$, respectively $13a, 17a$. For $S = E_7(q)$, let C denote a nontrivial conjugacy class. We have shown in Proposition 7.7 that the (C, C_2, C_3) -structure constant is nonzero, where C_2 contains elements of order Φ_7 and C_3 contains elements as in Table 6, whence there exist $(x, y, z) \in (C, C_2, C_3)$ with $xyz = 1$. Since the order of the maximal subgroup ${}^2E_6(q).D_{q+1}$ is not divisible by (a Zsigmondy prime divisor of) Φ_7 , we necessarily have $S = \langle y, z \rangle = \langle x, y \rangle$, so we are in situation (S2). Clearly, y has order prime to 6.

Now consider $S = \mathfrak{A}_n$, $n \geq 5$. When $\gcd(n, 6) = 1$, then by [5, Prop. 6.9] for any $1 \neq x \in \mathfrak{A}_n$ there exists an n -cycle y such that $\langle x, y \rangle = \mathfrak{A}_n$. Suppose that $n = 2m$ is even. Then choose e with $1 \leq e \leq 6$ such that $\gcd(m + e, m - e) = 1$ and $\gcd(m \pm e, 6) = 1$. Let $y \in \mathfrak{A}_n$ be the product of disjoint cycles of length $m + e$ and $m - e$. Clearly, y is not contained in any imprimitive subgroup. Thus, for $n \geq 16$, y is contained in a unique maximal subgroup by [52]. If $n = 6, 8, 10, 12$ or 14 , a computer check shows that one can take y of order $5, 7, 5, 35$ or 13 , respectively. Now suppose that n is odd and divisible by 3. Let $y \in \mathfrak{A}_{n-1}$ be chosen as above. If $n > 16$, it follows as above that y is not contained in any imprimitive subgroup. Clearly, given $1 \neq x \in S$, we can choose a conjugate y' of y such that $\langle x, y' \rangle$ is transitive and so primitive. It again follows by [52] that $S = \langle x, y' \rangle$. If $n < 16$, then we need only consider $n = 9$ and 15 . If $n = 15$, take y to be of order 13 and if $n = 9$, take y of order 7. It is straightforward to check that the result holds.

For S simple of classical Lie type, we typically take y to be the smallest power of an element as in Table 7 of order prime to 6. First let $S = L_n(q)$ with $n \geq 4$ even. The possible maximal subgroups containing such an element y are given in Lemma 2.4. Note that case (2) does not arise since n is even. If $q = r^2$ is a square, then $o(y)$, the prime to 6 part of $(q^{n-1} - 1)/\gcd(n, q - 1) = (r^{n-1} - 1)(r^{n-1} + 1)/(n, q - 1)$, is divisible by a Zsigmondy prime divisor of $(r^{n-1} - 1)$, so case (1) is out as well. Hence there are at most two maximal subgroups containing y , and the only cases for which the lemma does not apply are $L_4(2) \cong \mathfrak{A}_8$ and $L_4(4)$. For $S = L_4(4)$ the $(C, 63a, 85a)$ -structure constants are nonzero, and none of the subgroups in Lemma 2.3 contains elements of orders 63 and 85.

Now let $S = L_3(q)$. Then by Lemma 2.3 there are at most two maximal overgroups of y (viz. cases (1) and (4) for $f = 3$), so we are done unless $S \in \{L_3(2) \cong L_2(7), L_3(4)\}$. For the first group, see [5, Table 5]; for $L_3(4)$ the $(C, 5a, 7a)$ -structure constants are nonzero.

Next let $S = L_n(q)$ with $n \geq 5$ odd. Let C_2 denote the conjugacy class of an element of order $o_1 := (q^n - 1)/d(q - 1)$, and let C_3 be the class of an element of order $o_2 := ((q^{n-1} - 1)/d)'_{2,3}$, where $d = (n, q - 1)$. By the argument in the proof of [44, Thm. 2.1] only the trivial and the Steinberg character of S take nonzero values on both classes, and thus the (C, C_2, C_3) -structure constant does not vanish for any nontrivial class C of S . Now consider the subgroups in Lemma 2.3. Cases (2) and (3) are out since n is odd, and case (1) is excluded as before. The extension field subgroups $\mathrm{GL}_{n/f}(q^f)$ occur for prime divisors $f|n$. Now note that their order is not divisible by a Zsigmondy prime divisor of $q^{n-1} - 1$, which exists unless $(n, q) = (7, 2)$. But in the latter case, there is just one overgroup, so we are done again.

Next let $S = U_n(q)$ with $n \geq 4$ even, $(n, q) \neq (4, 2)$. If (n, q) is none of $(6, 2), (10, 2), (4, 3), (4, 5)$, then by Lemma 2.6 there is only one maximal subgroup containing y and we are done. For $(n, q) = (10, 2)$ the argument in [44, Thm. 2.2] shows that the (C, C_2, C_3) -structure constant does not vanish for any nontrivial class C of S , where C_2 contains elements of order 19 and C_3 elements of order $(q^n - 1)/(q - 1) = 1023$. None of the groups in Lemma 2.6 contains elements of order 13. The same may be applied to $U_4(5)$, with elements of order 7, respectively 13. For $U_6(2)$, the $(C, 11a, 12f)$ -structure constant is nonzero for any $C \neq \{1\}$, and the class $12f$ has trivial intersection with $U_5(2)$ as well as with M_{22} . For $U_4(3)$, the $(C, 7a, 9a)$ -structure constants are nonzero and none of the relevant maximal subgroups contains elements of order 9.

Now let $S = U_n(q)$ with $n \geq 3$ odd. Firstly, if n is prime and (n, q) is different from $(3, 3), (3, 5), (5, 2), (9, 2)$, then by Lemma 2.5 there is a unique maximal subgroup containing our element y , and we are done. The same holds in fact for $U_3(3)$ and $U_5(2)$. Else, we let C_2 denote a class of elements of order $(q^n + 1)/d(q + 1)$ and C_3 a class of elements of order $(q^{n-1} - 1)/d$, where $d = \gcd(n, q + 1)$. By [44, Thm. 2.2], the (C, C_2, C_3) -structure constants are nonzero in S . The extension field subgroups in Lemma 2.7(1) and (3) are ruled out by Zsigmondy. For $U_3(5)$ the $(C, 7a, 8a)$ -structure constants are nonzero, and no maximal subgroup contains elements of orders 7 and 8.

For $S = O_{2n+1}(q)$, we are done by Lemma 2.7 unless $n = p = 3$ or $(2n + 1, q) = (7, 5)$. Suppose that $n = p = 3$. In this case, we take y to be of order $(q + 1)'_{2,3}$. If $q > 3$, then Lemma 2.7 still implies that y is in a unique maximal subgroup. For $O_7(3)$ we may take y of order 13, for $O_7(5)$ of order 31.

Now let $S = S_{2n}(q)$. Let y be an element of the largest possible order prime to 6 dividing $q^n + 1$. Let \mathcal{M} denote the set of maximal subgroups of S containing y . First assume that q is even. If $n > 3$, it follows by Lemma 2.8 that all maximal subgroups containing y contain the centralizer of y . Let z be a generator for the centralizer of y . It was shown in [5, 5.8] that for any $g \in S$, we have that $S = \langle g, z' \rangle$ for some conjugate z' of z . Thus, the same is true for y . If $n = 2$, we may assume that $q \neq 2$. If q is a square, then $|\mathcal{M}| = 2$ and the result follows. If q is not a square, then $|\mathcal{M}| = 3$. If $q \geq 8$, it follows by [37] that $|s^S \cap M| \leq (4/3q)|s^S| \leq |s^S|/6$, whence the result. If $n = 3$, then the same argument applies for $q > 4$. See [5, Table 2] for the case $q = 4$. For $S_6(2)$ a computer check shows that we can take for y an element of order 7.

Now assume that q is odd. Let s be a nontrivial element of S . Suppose that s^S is contained in the union of the maximal subgroups containing y . Excluding the cases with $(n, q) = (4, 3), (6, 3), (6, 5)$, the only maximal subgroups containing y are one for each prime divisor of n and if n is odd, the normalizer of $SU_n(q)$. Suppose that s^S intersects $b \geq 3$ of the maximal subgroups containing y . It follows that s is contained in a conjugate of the normalizer $Sp_{2n/f}(q^f)$ for some prime $f > b$. By [5, 2.1 and 2.3], $|s^S \cap M| \leq (4/3q^{f-1})|s^S|$ for any proper subgroup M of S . Thus,

$$\left| \bigcup_{M \in \mathcal{M}} (s^S \cap M) \right| \leq (4(f - 1)/3q^{f-1})|s^S| < |s^S|,$$

a contradiction. For $S_4(3), S_6(3), S_6(5)$ a computer check shows that we may take y of order 5, 13, 31, respectively.

For $S = \mathrm{O}_{2n}^-(q)$, let C_2 denote a class of elements of order $o_1 := (q^n + 1)/(4, q^n + 1)$ and C_3 a class of semisimple elements of order $o_2 := (q^{n-1} + 1)_{2,3'}$. The arguments in the proof of [44, Thm. 2.5] show that only the trivial and the Steinberg character do not vanish on both C_2, C_3 . Thus, the structure constant $n(C, C_2, C_3)$ is nonzero for any nontrivial class C of S . None of the subgroups listed in Lemma 2.10 and Table 5 contains elements of orders o_1, o_2 , except possibly when no Zsigmondy prime for $q^{n-1} + 1$ exists, that is, when $(2n, q) = (8, 2)$. For the latter group, the $(C, 17a, 21a)$ -structure constants are nonzero, and no maximal subgroup contains elements of orders 17 and 21.

Next consider $S = \mathrm{O}_{2n}^+(q)$, $n \geq 4$. If $n = 4$ and $q > 4$, the result follows by [5, Lemma 5.15] (the element chosen there has order prime to 6). If $n = 4 = q$, the result follows by [5, Table 3]. Similarly, the result follows by [5, Lemmas 5.13, 5.14] if $n > 4$. For $S = \mathrm{O}_8^+(3)$ we may take y of order 13. The group $\mathrm{O}_8^+(2)$ is an exception.

For $S = \mathrm{L}_2(q)$, let C_2 be a class of elements of order p and C_3 a class of elements of order $(q + 1)/(2, q + 1)$. Then the (C, C_2, C_3) -structure constant is nonzero. For $q \geq 5$ prime to 6, no proper subgroup of G contains elements of orders p and $(q + 1)/(2, q + 1)$. For $q = p^f$ with $p = 2, 3$, let C_2 be a class of elements of order $(q - 1)/(2, q - 1)$ instead; again the structure constants do not vanish, one of C_2, C_3 contains elements of order prime to 6, and no proper maximal subgroup does contain elements from both classes unless $q = 9$, so $S = \mathfrak{A}_6$, which was already considered. \square

We end this section by demonstrating with the example of $E_8(q)$ how our methods can also be used to show that simple groups admit a so-called unmixed Beauville-structure (see for example [16]):

Theorem 8.6. *The simple groups $E_8(q)$, where q is any prime power, admit an unmixed Beauville structure.*

Proof. By [16, Def. 1.1] it suffices to show that $E_8(q)$ has two generating systems (x_1, y_1) , (x_2, y_2) such that the orders of x_1, y_1, x_1y_1 are pairwise prime to those of x_2, y_2, x_2y_2 .

By Proposition 3.5 we already know that there exists a conjugacy class C of G such that G is generated by $x_1, y_1 \in C$ with $(x_1y_1)^{-1} \in C$, containing elements of order $n := \Phi_{30}(q)$. Now let C_1 be a class of elements of order $\Phi_{24}(q)$, C_2 a class of elements of order $\Phi_{20}(q)$, and C_3 a class containing the product of a (long) root element x with a semisimple element of order Φ_{14} (from the subgroup $E_7(q)$ lying in $C_G(x)$). Note that all three classes contain elements of order prime to n . Using Lemma 3.2 it is immediate to see that at most unipotent characters might take nonzero values on the two semisimple classes simultaneously. Moreover, from the tables in [6, 13.9] one sees that in fact at most four unipotent characters have this property. Apart from the trivial character, this is the Steinberg character (which vanishes on the nonsemisimple class C_3) and two further characters of degree $> q^{100}$. Since the elements in all three classes have centralizer order less than q^{10} , we conclude that $n(C_1, C_2, C_3) \neq 0$.

The result of Cooperstein [10] shows that no proper subgroup of G containing long root elements has order divisible by $\Phi_{20}(q)$ and $\Phi_{24}(q)$. \square

Acknowledgements: The authors wish to thank Thomas Breuer for checking some of the maximal subgroups of classical groups, Frank Lübeck for help in dealing with $F_4(3)$,

Klaus Lux for determining the degrees of irreducible representations of $SU_3(8)$ over \mathbb{F}_2 and Pham Huu Tiep for pointing out two results on the alternating groups and their covers.

REFERENCES

- [1] J. BAMBERG, T. PENTTILA, Overgroups of cyclic Sylow subgroups of linear groups. *Comm. Algebra* **36** (2008), 2503–2543.
- [2] I. BAUER, F. CATANESE, F. GRUNEWALD, Beauville surfaces without real structures. Pp. 1–42 in: *Geometric methods in algebra and number theory*, Progr. Math., vol. 235, Birkhäuser Boston, 2005.
- [3] I. BAUER, F. CATANESE, F. GRUNEWALD, Chebycheff and Belyi polynomials, dessins d’enfants, Beauville surfaces and group theory. *Mediterr. J. Math.* **3** (2006), 121–146.
- [4] E. BERTRAM, Even permutations as a product of two conjugate cycles. *J. Combinatorial Theory Ser. A* **12** (1972), 368–380.
- [5] T. BREUER, R. GURALNICK, W. KANTOR, Probabilistic generation of finite simple groups. II. *J. Algebra* **320** (2008), 443–494.
- [6] R. W. CARTER, *Finite groups of Lie type. Conjugacy classes and complex characters*. Wiley Classics Library. John Wiley & Sons, Chichester, 1993.
- [7] V. CHERNOUSOV, E. ELLERS, N. GORDEEV, Gauss decomposition with prescribed semisimple part: short proof. *J. Algebra* **229** (2000), 314–332.
- [8] J.H. CONWAY, R.T. CURTIS, S.P. NORTON, R.A. PARKER, R.A. WILSON, *Atlas of Finite Groups*. Clarendon Press, Oxford, 1985.
- [9] B. N. COOPERSTEIN, Maximal subgroups of $G_2(2^n)$. *J. Algebra* **70** (1981), 23–36.
- [10] B. N. COOPERSTEIN, Subgroups of exceptional groups of Lie type generated by long root elements. I, II. *J. Algebra* **70** (1981), 270–282 and 283–298.
- [11] F. DIGNE, J. MICHEL, *Representations of finite groups of Lie type*. London Math. Soc. Student Texts, 21. Cambridge University Press, Cambridge, 1991.
- [12] E.W. ELLERS, N. GORDEEV, On conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.
- [13] W. FEIT, On large Zsigmondy primes. *Proc. Amer. Math. Soc.* **102** (1988), 29–36.
- [14] P. FONG, B. SRINIVASAN, The blocks of finite general linear and unitary groups. *Invent. Math.* **69** (1982), 109–153.
- [15] P. FONG, B. SRINIVASAN, Brauer trees in classical groups. *J. Algebra* **131** (1990), 179–225.
- [16] S. GARION, M. PENEGINI, New Beauville surfaces, moduli spaces and finite groups. *Monatsh. Math.*, to appear.
- [17] S. GARION, M. LARSEN, A. LUBOTZKY, Beauville surfaces and finite simple groups. Preprint 2010.
- [18] M. GECK, G. HISS, F. LÜBECK, G. MALLE, G. PFEIFFER, CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), 175–210.
- [19] J. GETZ, An approach to nonsolvable base change and descent for GL_2 over number fields. Preprint.
- [20] D. GLUCK, Sharper character value estimates for groups of Lie type. *J. Algebra* **174** (1995), 229–266.
- [21] R. GOW, Commutators in finite simple groups of Lie type. *Bull. London Math. Soc.* **32** (2000), 311–315.
- [22] R. GURALNICK, Some applications of subgroup structure to probabilistic generation and covers of curves. Pp. 301–320 in: *Algebraic groups and their representations* (Cambridge, 1997), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 517, Kluwer Acad. Publ., Dordrecht, 1998.
- [23] R. GURALNICK, W. KANTOR, Probabilistic generation of finite simple groups. *J. Algebra* **234** (2000), 743–792.
- [24] R. GURALNICK, M. LARSEN, C. MANACK, Low dimensional representations of simple Lie groups. Preprint.
- [25] R. GURALNICK, G. MALLE, Simple groups admit Beauville structures, Preprint.

- [26] R. GURALNICK, A. MARÓTI, Average dimension of fixed points with applications. *Adv. Math.* **226** (2011), 298–308.
- [27] R. GURALNICK, M. NEUBAUER, Monodromy groups of branched coverings: the generic case. Pp. 325–352 in: *Recent developments in the inverse Galois problem* (Seattle, WA, 1993), *Contemp. Math.*, 186, Amer. Math. Soc., Providence, RI, 1995.
- [28] R. GURALNICK, C. PRAEGER, T. PENTTILA, J. SAXL, Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc.* **78** (1999), 167–214.
- [29] C. HERING, Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geom. Dedicata* **2** (1974), 425–460.
- [30] G. HISS, G. MALLE, Low dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **4** (2001), 22–63; Corrigenda: *ibid.* **5** (2002), 95–126.
- [31] P. HOFFMAN, J. HUMPHREYS, *Projective representations of the symmetric groups. Q-functions and shifted tableaux*. The Clarendon Press, Oxford University Press, New York, 1992.
- [32] I. M. ISAACS, T. M. KELLER, U. MEIERFRANKENFELD, A. MORETÓ, Fixed point spaces, primitive character degrees and conjugacy class sizes. *Proc. Amer. Math. Soc.* **134** (2006), 3123–3130.
- [33] P. KLEIDMAN, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra* **110** (1987), 173–242.
- [34] P. KLEIDMAN, The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups. *J. Algebra* **117** (1988), 30–71.
- [35] M. LARSEN, A. SHALEV, Characters of symmetric groups: sharp bounds and applications. *Invent. Math.* **174** (2008), 645–687.
- [36] M. LARSEN, A. SHALEV, P. TIEP, Waring problem for finite simple groups. Preprint, 2010.
- [37] M. LIEBECK, J. SAXL, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc.* **63** (1991), 266–314.
- [38] M. LIEBECK, G. SEITZ, A survey of maximal subgroups of exceptional groups of Lie type. Pp. 139–146 in: *Groups, Combinatorics and Geometry* (Durham, 2001), World Scientific, 2003.
- [39] F. LÜBECK, Smallest degrees of representations of exceptional groups of Lie type. *Comm. Algebra* **29** (2001), 2147–2169.
- [40] F. LÜBECK, G. MALLE, (2, 3)-generation of exceptional groups. *J. London Math. Soc. (2)* **59** (1999), 109–122.
- [41] A. M. MACBEATH, Generators of the linear fractional groups. Pp. 14–32 in: *Proc. Sympos. Pure Math.*, Vol. XII, Houston, Tex., 1967, Amer. Math. Soc., Providence, R.I.
- [42] G. MALLE, Die unipotenten Charaktere von ${}^2F_4(q^2)$. *Comm. Algebra* **18** (1990), 2361–2381.
- [43] G. MALLE, B. H. MATZAT, *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.
- [44] G. MALLE, J. SAXL, TH. WEIGEL, Generation of classical groups. *Geom. Dedicata* **49** (1994), 85–116.
- [45] P. M. NEUMANN, *A study of some finite permutation groups*. Ph.D. thesis, Oxford, 1966.
- [46] A. RYBA, Short proofs of embeddings into exceptional groups of Lie type. *J. Algebra* **249** (2002), 402–418.
- [47] L. SCOTT, Matrices and cohomology. *Ann. of Math. (2)* **105** (1977), 473–492.
- [48] D. SEGAL, A. SHALEV, On groups with bounded conjugacy classes. *Quart. J. Math. Oxford* **50** (1999), 505–516.
- [49] P. H. TIEP, A. ZALESSKII, Minimal characters of the finite classical groups. *Comm. Algebra* **24** (1996), 2093–2167.
- [50] TH. WEIGEL, Generation of exceptional groups of Lie-type. *Geom. Dedicata* **41** (1992), 63–87.
- [51] H. WIELANDT, *Finite permutation groups*. Academic Press, New York-London, 1964.
- [52] A. WILLIAMSON, On primitive permutation groups containing a cycle. *Math. Z.* **130** (1973), 159–162.
- [53] R. WILSON, P. WALSH, J. TRIPP, I. SULEIMAN, R. PARKER, S. NORTON, S. NICKERSON, S. LINTON, J. BRAY, R. ABBOTT, *ATLAS of Finite Group Representations - Version 3*, <http://brauer.maths.qmul.ac.uk/Atlas/v3/>

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, 3620 S. VERMONT AVENUE, LOS ANGELES, CA 90089-2532, USA.

E-mail address: `guralnic@usc.edu`

FB MATHEMATIK, TU KAISERSLAUTERN, POSTFACH 3049, 67653 KAISERSLAUTERN, GERMANY.

E-mail address: `malle@mathematik.uni-kl.de`