Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Order of Products of Elements in Finite Groups

Antonio Beltrán, Richard Lyons, Alexander Moretó, Gabriel Navarro, Azahara Sáez and Pham Huu Tiep

Abstract

If G is a finite group, p is a prime and $x \in G$, it is an interesting problem to place x in a convenient small (normal) subgroup of G, assuming some knowledge of the order of the products xy, for certain p-elements y of G.

1. *Introduction*

It is currently a feature of finite group theory that many theorems on finite groups can only be proved by reducing them to a check that some property holds for all finite *simple* groups – the groups having no non-trivial normal subgroups. Then the classification of finite simple groups (see eg. [**9**]) comes into play and one has to be able to handle the three different families of simple groups with appropriate techniques. Often the groups of Lie type are the most difficult to deal with; at other times, it is the Monster or some other large sporadic group. Less often, the alternating groups are the ones causing the most trouble.

Our theorems in this paper, despite having quite elementary statements, are of this nature. We ask questions relating orders of products of elements in the group to the normal structure of the group. These questions have a rich story and lead to some cornerstone results in group theory such as Thompson's characterization of solvable finite groups as finite groups with no two nontrivial elements x, y satisfying $\gcd(o(xy), o(x)o(y)) = \gcd(o(x), o(y)) = 1$ in his famous N-groups paper series, cf. [**22**]. A further extension of Thompson's characterization and a p-solvable version of it were obtained much later in [**14**], using the full force of the classification of finite simple groups.

In this paper, we study these questions in the following direction. Let G be a finite group and N a normal subgroup of G, and let $x \in G$. Can we decide whether $x \in N$ if we know how the orders of y and xy are related, as y varies over G? (If indeed $x \in N$, then y and xy, which become equal modulo N, have related orders.) The answer naturally depends on our choice of the normal subgroup N. For certain N, there is an affirmative answer, but there are many open questions. In fact, our problem is related to several well-known and notoriously difficult conjectures on finite simple groups. We hope that some of the new techniques that we are providing can be used in these related problems.

Let G be a finite group, let p be a prime, and let $x \in G$. We wish to place x in a convenient small subgroup of G provided that we have information on the order of the products xy, where

---

2000 *Mathematics Subject Classification* 20C20, 20C15.

The third, fourth and fifth authors are partially supported by the Spanish Ministerio de Educación y Ciencia Proyecto MTM2016-76196-P, and Feder funds. The first, third and fourth authors are partially supported by Prometeo II/Generalitat Valenciana. The fifth author is also supported by BES-2014-068325. The sixth author gratefully acknowledges the support of the NSF (grant DMS-1665014).

Part of this work was done while the fifth author visited the Institut Universitari de Matemàtiques i Aplicacions de Castelló (IMAC). She thanks Antonio Beltrán and the Institute for their warm hospitality.

The authors are grateful to the referee for careful reading and helpful comments on the paper.

$y \in G$ is a p-element. Here is an example of the type of result that we are aiming at. Recall that $\mathbf{O}_p(G)$ is the largest normal subgroup of G with p-power order.

THEOREM A. *Let G be a finite group, let p be a prime, and let $x \in G$ be a p-element of G. Then xy is a p-element for every p-element $y \in G$ if and only if $x \in \mathbf{O}_p(G)$.*

As we will show below, Theorem A is an easy consequence of a well-known theorem of R. M. Guralnick and G. R. Robinson on extensions of the Baer–Suzuki theorem [**13**]. (Some modifications of this result are also obtained by Guralnick and G. Malle in [**11**].) We mention now that certain generalizations of Theorem A are not possible. For instance, Theorem A is not true if we only assume that xx^g is a p-element for every $g \in G$, and this is related to some results of Guralnick and the fourth author on the orders of the elements in a coset of a normal subgroup [**12**]. Also, it is asked in [**6**]: Let x be a p-element, if $P \in \mathrm{Syl}_p(G)$ and xy is a p-element for all $y \in P$, is it true then that $x \in P$? It turned out that this was a question by G. Zappa, to which M. Conder gave some counterexamples in [**3**].

In this paper we are concerned with products of elements of coprime orders. We propose a wealth of new results and we prove that they are true for any finite group G provided that Conjecture B below holds for any almost simple group whose socle is a composition factor of G.

CONJECTURE B. *Let G be an almost simple finite group with socle S, and let p be a prime divisor of $|S|$. If $x \in G$ is a nontrivial p'-element, then there exists a nontrivial p-element $y \in G$ such that p does not divide $o(xy)$.*

Conjecture B is related to a recent conjecture of Guralnick and the sixth author [**14**] (which is now a theorem thanks to [**17**]), and it constitutes yet another example of the difficulty of problems on products of conjugacy classes in simple groups. However, we will provide substantial evidence in support of Conjecture B, in what constitutes one of the main results of this paper.

THEOREM C. *Let G be an almost simple finite group with socle S, and let p be a prime divisor of $|S|$. Suppose that S is an alternating group, a sporadic group, or a simple group of Lie type in characteristic p. If $x \in G$ is a nontrivial p'-element, then there exists a nontrivial p-element $y \in G$ such that p does not divide $o(xy)$.*

As the reader will see, the proof of Theorem C for almost simple groups with socle a Lie-type group in defining characteristic is already highly nontrivial, relying on deep results on the structure of simple groups of Lie type [**9**] and the Deligne-Lusztig theory [**2**], [**4**]. It is our hope that results and techniques involved in the proof will be useful in other questions as well. At present, the remaining case of (large rank) Lie type groups in cross characteristic appears to be beyond reach.

Now, we can offer some applications.

THEOREM D. *Let G be a finite group, let p be a prime, and let $x \in G$ be a p'-element. Assume that Conjecture B holds for any almost simple group whose socle is a composition factor of G. Then $x \in \mathbf{O}_{p'}(G)$ if and only if p divides $o(xy)$ for every nontrivial p-element $y \in G$.*

It is convenient to remind the reader now of the following two examples. If $G = \mathsf{A}_8$, $p = 3$, $x = (1,2)(3,4)(5,6)(7,8)$ and $y = (1,2,3)$, then the order of xy^g is divisible by 6 for every

$g \in G$. (Of course, G has, exactly, one more class of nontrivial p-elements, so A_8 is not a counterexample to Conjecture B.) Also, if $p = 3$, $G = \mathrm{SL}_2(16)$ and $P \in \mathrm{Syl}_p(G)$, then there is $x \in G$ of order 17 such that p divides $o(xy)$ for all $1 \neq y \in P$, and $\langle x, P\rangle = G$. Hence, Theorem D is not true if we replace "for every nontrivial p-element of G" by "for every nontrivial p-element of only one Sylow p-subgroup of G".

Next, somewhat remarkably, we can characterize when a p-element x lies in $\mathbf{O}_p(G)$ by considering, unlike Theorem A, the order of xy for q-elements $y \in G$, for primes q different to p (assuming Conjecture B).

THEOREM E. *Let p be a prime, and let G be a finite group. Assume that Conjecture B holds for any almost simple group whose socle is a composition factor of G. Let $x \in G$ be a p-element. Then $x \in \mathbf{O}_p(G)$ if and only if q divides $o(xy)$ for all nontrivial q-element $y \in G$, for all $p \neq q$ prime dividing $|G|$.*

In fact, there is no need to restrict ourselves to p-elements or p'-elements, and Conjecture B is enough to guarantee several π-versions of the previous results.

THEOREM F. *Let G be a finite group, and let π be a non-empty set of primes. Assume that Conjecture B is true for any almost simple group whose socle is a composition factor of G. Let $x \in G$ be a π-element. Then $x \in \mathbf{O}_\pi(G)$ if and only if for every $p \in \pi'$ and every nontrivial p-element $y \in G$, p divides $o(xy)$.*

Applying Theorem F to every π-element of prime power order, we get the following characterization of groups with a normal Hall π-subgroup in terms of orders of products.

Recall that $\pi(n)$ is the set of primes dividing the integer n and we use $\pi(G)$ to denote $\pi(|G|)$.

COROLLARY G. *Let G be a finite group, and let π be a non-empty set of primes. Assume that Conjecture B is true for any almost simple group whose socle is a composition factor of G. Then G has a normal Hall π-subgroup if and only if for every π-element x of prime power order and every nontrivial π'-element y of prime power order, $\pi(o(y)) \subseteq \pi(o(xy))$.*

The particular case of Corollary G where $\pi = \{p\}$ is Theorem C of [**19**].

We wonder whether the following statement, which would unify both the case of Conjecture B where x has prime power order and G is simple and the aforementioned Guralnick–Tiep conjecture proved in [**17**], could possibly be true.

CONJECTURE H. *Let G be a finite simple group. Let $p \neq q$ be two prime divisors of $|G|$. Let $x \in G$ be a nontrivial p-element. Then there exists a nontrivial q-element $y \in G$ such that $o(xy)$ is coprime to pq.*

2. *Proof of Theorem F*

We start by proving Theorem A, which we restate.

THEOREM 2.1. *Let G be a finite group, let p be a prime, and let $x \in G$ be a p-element of G. Then xy is a p-element for every p-element $y \in G$ if and only if $x \in \mathbf{O}_p(G)$.*

Proof. Suppose first that $x \in \mathbf{O}_p(G)$. Since x lies in every Sylow p-subgroup of G, it is trivial that xy is a p-element for every p-element y of G. Conversely, assume that xy is a p-element for every p-element y of G. Since the set S of all p-elements of G is closed under left multiplication by x, and G is finite, S is closed under left multiplication by x^{-1}. Therefore, $x^{-i}(x^i)^g = [x^i, g]$ is a p-element for every $x^i \in \langle x \rangle$ and $g \in G$, and by applying Corollary B of [**13**], we get $x \in \mathbf{O}_p(G)$. □

Let us start with an easy lemma.

LEMMA 2.2. *Let L be a normal subgroup of a finite group G. Let π be a set of primes and let $x \in G$ be a π-element. If $[x, L] \neq 1$, then there exists a π-element in $xL - \{x\}$.*

Proof. By hypothesis, there is some $y \in L$ such that $[x, y] \neq 1$. Then $x^y = x[x, y] \in xL - \{x\}$ is a π-element. □

Now we specifically state what we need about almost simple groups in order to prove our results.

CONJECTURE 2.3. *Let G be an almost simple group with non-abelian simple socle S, and let p be a prime divisor of $|G|$. Assume that $G = \langle x \rangle S$, where x is a nontrivial p'-element. Then there exists a nontrivial p-element $y \in G$ such that p does not divide $o(xy)$. In particular, if π is a non-empty proper subset of $\pi(G)$ and $G = \langle x \rangle S$, where x is a nontrivial π-element, then there exists a nontrivial q-element $y \in G$ for some $q \in \pi'$ such that q does not divide $o(xy)$.*

As shown in Theorem C, Conjecture 2.3 holds whenever S is an alternating group, a sporadic group, or a simple group of Lie type in the same characteristic p.

Next, we prove Theorem F.

THEOREM 2.4. *Let G be a finite group. Assume that π is a set of primes. Assume that Conjecture 2.3 holds for all the almost simple groups whose socle is a composition factor of G. Let $x \in G$ be a π-element. Then $x \in \mathbf{O}_\pi(G)$ if and only if for every $q \in \pi'$ and every nontrivial $y \in G$ that is a q-element, q divides $o(xy)$.*

Proof. If $x \in \mathbf{O}_\pi(G)$, then for every $q \in \pi'$ and every nontrivial $y \in G$ that is a q-element, $xy \in \mathbf{O}_\pi(G)\langle y \rangle$. This subgroup contains a normal Hall π-subgroup. Then, if q does not divide $o(xy)$, xy is a π-element which lies in $\mathbf{O}_\pi(G)$, so $y \in \mathbf{O}_\pi(G)$ and this contradicts the fact that y is a nontrivial q-element.

Conversely, assume now that for every $q \in \pi'$ and every nontrivial $y \in G$ that is a q-element, q divides $o(xy)$. We want to prove that $x \in \mathbf{O}_\pi(G)$. Let G be a minimal counterexample. We may assume that π is a non-empty proper subset of $\pi(G)$.

Step 1: Let $L = \mathbf{O}_\pi(G)$. We claim that $L = 1$.

Suppose that $L > 1$. Assume that there exists $q \in \pi'$ and $yL \in G/L$ that is a nontrivial q-element, but that q does not divide $o(xyL)$. Since $yL = y_qL$, where y_q is the q-part of y, we may assume that $y \in G$ is a q-element. Then $L\langle xy \rangle$ is a q'-group, q does not divide $o(xy)$ and this contradicts our hypothesis. Therefore, the hypothesis holds for G/L and we deduce that $xL \in \mathbf{O}_\pi(G/L) = L/L$. It follows that $x \in L$. This is a contradiction.

Step 2: Let $r \in \pi'$. Put $R = \mathbf{O}_r(G)$. We claim that $R = 1$.

Assume that $R > 1$. We want to see that the hypothesis holds for $\overline{G} = G/R$. Take $q \in \pi'$ and $\overline{y} \in \overline{G}$, where $\overline{y}$ is a nontrivial q-element. We may assume that $y \in G$ is a nontrivial q-element. First, assume that $q = r$. Assume that q does not divide $o(\overline{xy})$. Therefore, $\overline{xy}$ is a q'-element and we deduce that there exists $z \in R$ such that $xyz = t$ for some q'-element $t \in G$. Notice that yz is a q-element. By hypothesis, $yz = 1$ and we deduce that $y \in R$, that is, $\overline{y} = \overline{1}$, which cannot happen. Now, suppose that $q \neq r$. Assume that q does not divide $o(\overline{xy})$. Since R is an r-group, observe that q does not divide $o(xy)$ either. This is a contradiction too. We deduce that the hypothesis holds for $\overline{G}$, as wanted.

Let $\overline{N} = \mathbf{O}_\pi(\overline{G})$. Since G is a minimal counterexample, by the above paragraph, we have $\overline{x} \in \overline{N}$. Since $\mathbf{O}_\pi(G) = 1$, we have that $\mathbf{O}_\pi(N) = 1$. Now, using the Schur-Zassenhaus theorem, we have that N is the semidirect product of the normal π'-group R and a π-group T that acts on R. We claim that T acts faithfully on R. Observe that we can write $C_N(R) = Z(R) \times X$, for some normal Hall π-subgroup X of N. Since $\mathbf{O}_\pi(N) = 1$, we deduce that $X = 1$ and the action of T on R is faithful. Put $H = \langle x \rangle R$. Since $[x, R] \neq 1$, we deduce from Lemma 2.2 that there exists a π-element in $xR - \{x\}$. Hence, there exists a nontrivial $y \in R$ such that r does not divide $o(xy)$. This contradicts our hypothesis. Then $R = 1$.

Step 3: We claim that $G = \langle x \rangle F$, where F is the generalized Fitting subgroup $\mathbf{F}^*(G)$.

By Steps 1 and 2, we know that $\mathbf{F}(G) = 1$. Therefore, $F = K_1 \times \cdots \times K_t$, where $\{K_1, \ldots, K_t\}$ are the minimal normal subgroups of G and K_i is a direct product of copies of some non-abelian simple group for every i. Furthermore, $\mathbf{C}_G(F) \subseteq F$ and all the simple groups that are direct factors of F are not π-groups (by Step 1).

Assume that $S = \langle x \rangle F < G$. Notice that the non-abelian composition factors of S are composition factors of G. The hypothesis holds for S, so we deduce that $x \in \mathbf{O}_\pi(S)$. Since $\mathbf{O}_\pi(S) \cap F \subseteq \mathbf{O}_\pi(F) = 1$, we have that $S = \langle x \rangle \times F$ and x acts trivially on F. In this case, $x \in \mathbf{C}_G(F) \subseteq F$, then $S = F$ and $x \in \mathbf{O}_\pi(S) = \mathbf{O}_\pi(F) = 1$. This is a contradiction with the fact that G is a counterexample. Therefore, $S = G$ and the step is proved.

Step 4: We claim that F is a minimal normal subgroup of G.

Assume as in Step 3 that $F = K_1 \times \cdots \times K_t$ with $t > 1$. Since x acts faithfully on F, then there is some $i \in \{1, \ldots, t\}$ such that x does not centralize K_i. The hypothesis holds for $\langle x \rangle K_i$ and we get a contradiction as in Step 3.

At this point, we have that $G = \langle x \rangle K$, where K is the unique minimal normal subgroup of G and K is the direct product of n copies of a non-abelian simple group S, for some integer n.

Step 5: We claim that $n = 1$.

Assume that $K = S_1 \times \cdots \times S_n$ for some integer $n > 1$, where $S_i \cong S$ for every i. We know that $\langle x \rangle$ acts transitively on $\{S_1, \ldots, S_n\}$. Since G is not a π-group, let $q \in \pi'$ be a prime divisor of $|S|$ and let $y \in S_1$ be a nontrivial q-element. We have that $y^x \in S_j$ for some $j \neq 1$ is a q-element. Hence $[y, x] = y^{-1}y^x$ is a q-element too and so is $[y, x]^{-1} = [x, y]$. Now, since $x^y = x[x, y]$ is a π-element, we deduce from our hypothesis that $[x, y] = 1$. Therefore, x centralizes all the q-elements of S_1. Similarly, x centralizes all the q-elements of S_j for every j. Since S_j is simple, S_j is generated by its q-elements, so x centralizes S_j for every j and we deduce that $G = \langle x \rangle \times K$. This contradicts Step 1.

Hence, we have that $G = \langle x \rangle S$ for some non-abelian simple group $S = \mathbf{F}^*(G)$, and recall that π is a non-empty proper subset of $\pi(G)$. Since we are assuming that Conjecture 2.3 holds for S, we have that $x = 1$ and this contradicts again the fact that G is a counterexample, completing the proof. □

Now, Theorem D is obtained from Theorem F by setting $\pi = p'$. (We notice that in this case, Conjecture B is only used for the prime p.) Theorem E is obtained from Theorem F by setting $\pi = \{p\}$.

3. *Almost simple groups. I*

First of all, we notice that Conjecture B can be checked character-theoretically (if the character table of G is known). In particular, it can be checked for all the character libraries stored in [**5**], and in particular for the almost simple groups with socle being a sporadic simple group or A_n with $5 \leq n \leq 8$. Of course, this follows from the following well-known lemma.

LEMMA 3.1. *Let G be a finite group, and let $x, y, z \in G$. Then there exist $g, h \in G$ such that $xy^g = z^h$ if and only if*

$$\Sigma(x,y,z) := \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\chi(z^{-1})}{\chi(1)} \neq 0\,.$$

Proof. This follows from Problem 3.9 of [**16**] or Corollary 4.13 of [**20**]. □

THEOREM 3.2. *Conjecture 2.3 holds if $S = \mathsf{A}_n$ for any $n \geq 5$.*

Proof. We proceed by induction on $n \geq 5$, with the induction base $5 \leq n \leq 9$ checked using [**5**]. For the induction step, assume $n \geq 10$, $\mathsf{A}_n \leq G \leq \mathsf{S}_n$, $p \leq n$, and let $1 \neq \sigma \in G$ be a p'-element. We will find a nontrivial p-element $y \in \mathsf{A}_n \leq G$ such that σy is a p'-element.

For any $\pi \in \mathsf{S}_n$, let $m_\pi := |\{1 \leq i \leq n \mid \pi(i) \neq i\}|$ be the number of points that are moved by π, and let n_π be the number of nontrivial cycles in the decomposition of π into a product of disjoint cycles. Clearly, $m_\pi \geq 2n_\pi$. It is easy to check, see eg. [**15**, Lemma 2], that $\pi \in \mathsf{A}_n$ if and only if $2|(m_\pi - n_\pi)$. Furthermore, given any two integers $l_1, l_2 \geq 2$, by [**15**, Theorem 7], π can be written as a product uv of an l_1-cycle $u \in \mathsf{S}_n$ and an l_2-cycle $v \in \mathsf{S}_n$ if and only if at least one of the following statements holds:

(a) $n_\pi = 2$ and π is a disjoint product of an l_1-cycle and an l_2-cycle;
(b) $l_1 + l_2 = m_\pi + n_\pi + 2s$ for some $s \in \mathbb{Z}_{\geq 0}$ and $|l_1 - l_2| \leq m_\pi - n_\pi$.

(i) First we consider the case $p = n$. If σ is an odd permutation, then by [**1**, Corollary 3.1], $\sigma = zy^{-1}$, where z is an $(n-1)$-cycle and $y \in \mathsf{A}_n$ is an n-cycle, yielding $\sigma y = z$ is a p'-element. Suppose $\sigma \in \mathsf{A}_n$. As $2|(m_\sigma - n_\sigma)$ and $m_\sigma \geq 2n_\sigma$, we have that $2 \leq m_\sigma - n_\sigma$. Hence by (b), $\sigma = zy^{-1}$, where z is an $(n-2)$-cycle and $y \in \mathsf{A}_n$ is an n-cycle, yielding $\sigma y = z$ is a p'-element.

(ii) From now on, we may assume that $p \leq n-1$. Applying the induction hypothesis to $n-1$, we are done if σ has a fixed point. Thus we may assume that $m_\sigma = n$.

Consider the case $n_\sigma = 1$, so that σ is an n-cycle. As mentioned in [**1**, p. 369], every element in A_n is a product of two n-cycles. For $p > 2$, we can therefore find a p-cycle $y \in \mathsf{A}_n$ such that $y = \sigma^{-1}z$ for some n-cycle z, yielding $\sigma y = z$ is a p'-element. For $p = 2$, we can apply the same argument, taking $1 \neq y \in \mathsf{A}_n$ to be a conjugate of $(12)(34)$.

Next we consider the case $n_\sigma \geq 2$ and $p \leq n/2$. As $m_\sigma = n$, we can write the p'-element $\sigma = \alpha\beta$ as a disjoint product of (necessarily) p'-elements $1 \neq \alpha \in \mathsf{S}_k$ and $1 \neq \beta \in \mathsf{S}_{n-k}$, and note that $n > k \geq n/2 \geq \max\{p, 5\}$. If $p > 2$, then by the induction hypothesis applied to $\alpha \in \mathsf{S}_k$, there is a p-element $1 \neq y \in \mathsf{A}_k$ such that αy is a p'-element, whence $\sigma y = (\alpha y)\beta$ is a p'-element in G. If $p = 2$, then the $2'$-element α is contained in A_k. By the induction hypothesis

applied to $\alpha \in \mathsf{A}_k$, we can now find a 2-element $y \in \mathsf{A}_k$ such that αy is a $2'$-element, whence $\sigma y = (\alpha y)\beta$ is a $2'$-element in G.

(iii) Now we may assume that $p < n = m_\sigma < 2p$; in particular, $p \geq 7$ as $n \geq 10$. In this case, $n_\sigma \leq m_\sigma/2 < p$ and $p < m_\sigma + n_\sigma \leq 3m_\sigma/2 < 3p$. Suppose first that $m_\sigma + n_\sigma \neq 2p$. Then by (b), we can find a p-cycle $y \in \mathsf{A}_n$ and a $(m_\sigma + n_\sigma - p)$-cycle z such that $\sigma = zy^{-1}$, yielding $\sigma y = z$ is a p'-element. Finally, assume that $m_\sigma + n_\sigma = 2p$. In this case, again by (b), we can find a p-cycle $y \in \mathsf{A}_n$ and a $(p+2)$-cycle z such that $\sigma = zy^{-1}$, completing the proof. □

4. *Almost simple groups. II*

In this section our main result will be

THEOREM 4.1. *Conjecture 2.3 holds whenever S is a simple group of Lie type in characteristic p.*

Our analysis will focus on a minimal counterexample (G, S, x), which has the following properties:

(M1) $S = \mathrm{soc}(G)$ is a finite simple group of Lie type in characteristic p;
(M2) $G = S\langle x \rangle$;
(M3) x is a p'-element;
(M4) For every nontrivial p-element y of G, xy is not a p'-element; and
(M5) $|S|$ is minimal subject to the foregoing conditions.

We fix these assumptions and notation for this section, except where explicitly noted otherwise.

We use [**5**] to check that certain exceptional groups S do not give counterexamples. Specifically, in our minimal counterexample (G, S, x),

$$S \ncong \mathsf{A}_6,\ {}^2F_4(2)',\ G_2(2)' \cong \mathrm{SU}_3(3),\ \text{or}\ {}^2G_2(3)' \cong \mathrm{SL}_2(8), \tag{4.1}$$

in characteristic $p = 2$, 2, 2, or 3, respectively.

Therefore, there is a simple algebraic group $\mathcal{G}$ of adjoint type over a field of characteristic p and a Steinberg endomorphism $F : \mathcal{G} \to \mathcal{G}$ such that $S = \mathbf{O}^{p'}(\mathcal{G}^F)$.

We also identify $J := \mathrm{Inndiag}(S) \lhd \mathrm{Aut}(S)$ with $\mathcal{G}^F$, see Definition 2.5.10 and Theorem 2.5.12 of [**9**].

$$\text{We let } j \text{ be the order of the element } Sx \text{ in } \mathrm{Aut}(S)/J \text{ and let } d = |J/S|. \tag{4.2}$$

We will assume that J is defined over $\mathbb{F}_q$ with $q = p^f$, in the sense that q is the common absolute value of the eigenvalues of F acting on the character group of an F-stable maximal torus of $\mathcal{G}$ (and so q is an integer unless J is a Suzuki-Ree group). Also let $\mathcal{G}^*$ denote the algebraic group dual to $\mathcal{G}$ (so $\mathcal{G}^*$ is simply connected). Sometimes we also view S as $L/\mathbf{Z}(L)$, where $L := \mathcal{G}_{\mathrm{sc}}^F$ and $\mathcal{G}_{\mathrm{sc}}$ is the simply connected algebraic group isogenous to $\mathcal{G}$ with a suitable Steinberg endomorphism $\mathcal{G}_{\mathrm{sc}} \to \mathcal{G}_{\mathrm{sc}}$ that we also denote by F. We refer to [**2**] and [**4**] for basic facts on finite groups of Lie type.

We fix all this notation, as well, throughout this section.

We begin with an elementary extension of the Borel-Tits theorem [**9**, 3.1.3(a)] to almost simple groups.

LEMMA 4.2. *If $1 \neq R \leq S$ is a p-subgroup, then there is a parabolic subgroup $P < S$ such that $R \leq U := \mathbf{O}_p(P)$, $P = \mathbf{N}_S(U)$, and $\mathbf{N}_G(R) \leq \mathbf{N}_G(U)$.*

Proof. Define $R_1 := R$, and $R_{n+1} := \mathbf{O}_p(\mathbf{N}_S(R_n))$ for any integer $n \geq 1$. By construction, we have that

$$R_{n+1} \geq R_n \geq R, \quad \mathbf{N}_G(R_{n+1}) \geq \mathbf{N}_G(R_n) \geq \mathbf{N}_G(R).$$

Since $\mathbf{N}_S(R_{n+1}) \geq \mathbf{N}_S(R_n)$, there must be some $n \geq 2$ such that $\mathbf{N}_S(R_n) = \mathbf{N}_S(R_{n-1})$, which implies that $R_{n+1} = R_n \geq R$. Applying the Borel-Tits theorem [**9**, (3.1.3)(a)] to R_n, we can find a parabolic subgroup $P < S$ such that

$$R_n \leq U := \mathbf{O}_p(P), \quad \mathbf{N}_S(R_n) \leq P = \mathbf{N}_S(U).$$

Now, $\mathbf{N}_S(R_n)$ normalizes $W := \mathbf{N}_U(R_n)$, and so $W \leq \mathbf{O}_p(\mathbf{N}_S(R_n)) = R_{n+1} = R_n$. It follows that $\mathbf{N}_U(R_n) = R_n$, $R_n = U$, and we are done. □

COROLLARY 4.3. *Neither of the following two conditions can hold for x.*
(i) *x normalizes a nontrivial p-subgroup R of G.*
(ii) *p divides $|\mathbf{C}_G(x)|$.*
In particular, if $j = 1$ then $x \in J$ is regular semisimple.

Proof. Clearly (ii) implies (i). Assume now that (i) holds, so that $x \in \mathbf{N}_G(R)$. Since S has p'-index in $G = S\langle x\rangle$, by Lemma 4.2 there is a parabolic subgroup $P < S$ such that $R \leq U := \mathbf{O}_p(P)$, $P = \mathbf{N}_S(U)$, and $\mathbf{N}_G(R) \leq H := \mathbf{N}_G(U)$. Note that all non-abelian composition factors of H are simple groups of Lie type in characteristic p of order smaller than $|S|$, but not ${}^2F_4(2)'$ or $G_2(2)'$ in characteristic 2, or ${}^2G_2(3)'$ in characteristic 3, by (4.1). As Theorem 3.2 handles the A_6 case, the minimality of G implies by Theorem 2.4 that $x \in \mathbf{O}_{p'}(H)$. Note that $U \leq \mathbf{O}_p(H)$, hence $[x, U] = 1$ and so $x \in \mathbf{C}_G(U)$. Recall (4.1) that $S \ncong \mathrm{Sp}_4(2)' \cong \mathsf{A}_6$ and $G \leq \mathrm{Aut}(S)$. Hence $\mathbf{C}_G(U) \leq U$ by [**8**, (13-2)], whence the p'-element x must be 1. □

Recall (4.2) that j is the least positive integer such that $x^j \in J = \mathrm{Inndiag}(S)$.

THEOREM 4.4. $x^j \neq 1$.

Proof. Assume the contrary: $x^j = 1$. By [**9**, Theorem 2.5.12(a)], $\mathrm{Aut}(S) = J \rtimes \Phi_S\Gamma_S$ for a certain subgroup Φ_S of field automorphisms, and a certain set Γ_S of graph automorphisms or graph-field automorphisms such that $\Phi_S\Gamma_S$ is a group. Hence we can find $x_1 \in \Phi_S\Gamma_S$ of order j such that $x \in Jx_1$.

(i) First we consider the case where x_1 is a field or a graph-field automorphism of S, in the sense of [**9**, Definition 2.5.13]. We will show that p divides $|\mathbf{C}_J(x)|$ in this case. For this purpose, we may replace x by any generator of $\langle x\rangle$. As shown in the proof of [**9**, Proposition 4.9.1(d)], $x = hx_1h^{-1}$ for some $h \in J$, and the action of x_1 on $J = \mathcal{G}^F$ is induced by some Steinberg endomorphism τ of $\mathcal{G}$ satisfying $F \in \langle\tau\rangle$ (possibly after replacing x by a suitable generator of $\langle x\rangle$). In this case,

$$|\mathbf{C}_J(x)| = |\mathbf{C}_J(x_1)| = |\mathbf{C}_{\mathcal{G}}(F) \cap \mathbf{C}_{\mathcal{G}}(\tau)| = |\mathbf{C}_{\mathcal{G}}(\tau)| = |\mathcal{G}^\tau|,$$

and so p divides $|\mathbf{C}_J(x)|$.

As $p \nmid |J/S|$, p also divides $|\mathbf{C}_S(x)|$, contradicting Corollary 4.3.

(ii) We have shown that x is a graph automorphism of S; in particular, J is not a Suzuki-Ree group. Assume in addition that j is a prime. In the untwisted case, we have that either $j = 2$ (so $p \neq 2$ as x is a p'-element), or $(J, j) = (D_4(q), 3)$ (and $p \neq 3$). In the twisted case $J = {}^d\Sigma(q)$ we have $d|j$, and so either $j = 2$ (and $p \neq 2$), or $(J, j, p) = ({}^3D_4(q), 3, \neq 3)$. Checking [**9**, Table 4.5.1]

for $j = 2$ and [**9**, Table 4.7.3A] for $j = 3$, we see that p divides $|\mathbf{C}_S(x)|$, again contradicting Corollary 4.3.

Thus j cannot be a prime. This implies that $J = {}^d\Sigma(q)$ with $d > 1$ and $d|j$. In this case, $x^{j/d}$ has order d modulo J, so $x^{j/d}$ is still a graph automorphism of S. We can also assume that $S \ncong \mathrm{PSU}_n(q)$ with $(n, q) = (3, 2)$, $(3, 3)$, $(4, 2)$, $(4, 3)$, and $S \ncong {}^3D_4(2)$, since Conjecture 2.3 can be checked by [**5**] to hold for all these small groups. Now we can use Tables 4.5.1 and 4.7.3A of [**9**] to check that $L := E(\mathbf{O}^{p'}(\mathbf{C}_J(x^{j/d}))) < S$ is a central product $L = L_1 * L_2 * \ldots * L_s$ of quasisimple groups in characteristic p; in particular, $[L, L] = L$ and $\mathbf{O}_{p'}(L) = \mathbf{Z}(L)$.

By the minimality of (G, S, x), Conjecture 2.3 holds for all composition factors of $L\langle x\rangle$. Hence by Theorem 2.4 we have that $x \in \mathbf{O}_{p'}(L\langle x\rangle)$. Now $[x, L] \subseteq \mathbf{O}_{p'}(L) = \mathbf{Z}(L)$. As $L = [L, L]$, we then get that $[x, L] = [x, [L, L]]$ is contained in $[[x, L], L] \subseteq [\mathbf{Z}(L), L] = \{1\}$. Thus $\mathbf{C}_S(x)$ contains L and so has order divisible by p, again a contradiction. □

Recall that $J = \mathcal{G}^F$ is defined over the field $\mathbb{F}_q$.

Proposition 4.5. *The following statements hold.*
(a) *If $q \geq 4$, then every nontrivial element in $\langle x^j\rangle$ is regular semisimple in J.*
(b) *If $q = 2$ or 3, then x^j is regular semisimple in J.*

Proof. (i) By Theorem 4.4, $x^j \neq 1$. Assume now that $1 \neq x^{jm}$ is not a regular semisimple element of J for some $m \geq 1$. Then $\mathbf{C}_S(x^{jm})$ contains a nontrivial unipotent element $u \in S$, which then centralizes any power of x^{jm}. Replacing x^{jm} by a suitable power of it, we may assume that $z := x^{jm}$ has prime order. By [**9**, Theorem 4.2.2], $L := \mathbf{O}^{p'}(\mathbf{C}_S(z)) < S$ is a central product $L = L_1 * L_2 * \ldots * L_s$, where each $L_i = {}^{d_i}\Sigma_i(q^{m_i})$ is a finite group of Lie type defined over $\mathbb{F}_{q^{m_i}}$ for some $m_i \geq 1$ (arising from a simple algebraic group with Dynkin diagram Σ_i, in the sense of [**9**, Definition 2.2.1]). Moreover, no L_i is isomorphic to $G_2(2)$ or ${}^2F_4(2)$ if $p = 2$, or ${}^2G_2(3)$ if $p = 3$. In particular, all non-abelian composition factors of $L\langle x\rangle$ are groups of Lie type in characteristic p, or A_6, and so they satisfy Conjecture 2.3 by the minimality of (G, S, x) and Theorem 3.2. Hence $x \in \mathbf{O}_{p'}(L\langle x\rangle)$ by Theorem 2.4.

Recall that $L_i = {}^{d_i}\Sigma_i(q^{m_i})$ is defined over $\mathbb{F}_{q^{m_i}}$ for any i. Under the extra assumption that $q \geq 4$, each L_i is a quasisimple group of Lie type in characteristic p, see [**9**, Theorem 2.2.7(b)]; in particular, $[L_i, L_i] = L_i$ and $\mathbf{O}_{p'}(L_i) = \mathbf{Z}(L_i)$. It follows that $[L, L] = L$ and $\mathbf{O}_{p'}(L) = \mathbf{Z}(L)$. As in the proof of Theorem 4.4, we now see that $[x, L] = 1$, whence p divides $|\mathbf{C}_G(x)|$, contradicting Corollary 4.3.

We are also done by Corollary 4.3 if $j = 1$ and $q \leq 3$. Suppose now that $q = 2$. Since the case $\mathrm{soc}(G) = D_4(2)$, ${}^3D_4(2)$ is checked using [**5**], we may assume that $S \ncong D_4(2)$, ${}^3D_4(2)$. It follows that $|\mathrm{Out}(S)| \leq 2$. On the other hand, $p = 2 \nmid |x|$, so $j = 1$ and we are done.

(ii) Now we consider the case where $q = 3$ and $j \geq 2$ but j is coprime to $p = 3$. In this case, we must have that $j = 2$, $|x| = 2m$ for some $m > 1$, and $z := x^m$ is either an inner-diagonal or a graph automorphism of order 2. We will also assume that

$$S \ncong A_2^{\pm}(3),\ A_3^{\pm}(3),\ B_2(3),\ B_3(3),\ C_2(3),\ D_4(3),\ G_2(3)$$

in which cases Conjecture 2.3 is checked using [**5**]. Now, using [**9**, Table 4.5.1], we can verify that $L := E(\mathbf{O}^{p'}(\mathbf{C}_J(z))) < S$ is a central product $L = L_1 * L_2 * \ldots * L_s$ of quasisimple groups over $\mathbb{F}_q$; in particular, $[L, L] = L$ and $\mathbf{O}_{p'}(L) = \mathbf{Z}(L)$. Again the minimality of (G, S, x) implies by Theorem 2.4 that $x \in \mathbf{O}_{p'}(L\langle x\rangle)$. Arguing as above, we deduce that $[x, L] = 1$ and so p divides $|\mathbf{C}_G(x)|$, contradicting Corollary 4.3. □

The next lemma obviously applies to an arbitrary finite group G.

LEMMA 4.6. *Let $N \lhd G$ and let $X \subseteq N$ be a normal subset of G. For any $\chi \in \mathrm{Irr}(G)$ and any $\alpha \in \mathrm{Irr}(N)$ lying under χ,*

$$\frac{\sum_{x\in X}\chi(x)}{|X|} = \frac{\chi(1)}{\alpha(1)}\cdot\frac{\sum_{x\in X}\alpha(x)}{|X|}.$$

Proof. Write $\chi|_N = \sum_{i=1}^t \alpha_i$, where $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_t \in \mathrm{Irr}(N)$ are G-conjugate. Since X is G-invariant, $\sum_{x\in X}\alpha_i(x) = \sum_{x\in X}\alpha(x)$ for all i. Hence the statement follows, as $t = \chi(1)/\alpha(1)$. □

Let $\mathcal{U}$ denote the set of regular unipotent elements in J. Note that $\mathcal{U} \subset S$ and $\mathcal{U}$ is a normal subset of G.

We return to the notation and conditions set up at the beginning of this section.

LEMMA 4.7. *Let*

$$Y := \big\{\chi \in \mathrm{Irr}(G) \,\big|\, \chi|_S \in \mathrm{Irr}(S)\big\}, \quad Y_0 := \big\{\chi \in Y \,\big|\, \chi(1) > 1\big\}.$$

Then there is no p'-element $z \in Sx$ and subset $Y' \subseteq Y_0$ such that the following two conditions hold:

(a) $\Sigma(x,z) := \sum_{\chi\in Y_0\smallsetminus Y'} \dfrac{|\chi(x)\chi(z^{-1})|}{\chi(1)} < |G/S|$, *and*

(b) $\sum_{u\in\mathcal{U}}\chi(x)\chi(u)\chi(z^{-1}) \in \mathbb{R}_{\geq 0}$ *for all* $\chi \in Y'$.

Proof. Let $z \in G$ be a p'-element fulfilling the two conditions (a) and (b). Consider any $\chi \in \mathrm{Irr}(G)$ and let $\alpha \in \mathrm{Irr}(S)$ be lying under χ. If α is x-invariant, then, since $G = \langle S, x\rangle$, α extends to G and furthermore $\chi|_S \in \mathrm{Irr}(S)$, that is, $\chi \in Y$. Suppose on the other hand that α is not x-invariant. Then $I := I_G(\alpha) < G$, $\chi|_S = e\sum_{i=1}^t \alpha_i$ with $\alpha_1, \ldots, \alpha_t$ being the set of all distinct G-conjugates of α and $t = |G : I|$. Furthermore, x acts on any G-module affording χ, permuting the t isotypic S-components (affording S-characters $e\alpha_1, \ldots, e\alpha_t$) transitively and fixed-point-freely. It follows that $\chi(x) = 0$ whenever $\chi \notin Y$. Thus, in the notation of Lemma 3.1,

$$\Sigma(x,y,z) = \sum_{\chi\in Y}\frac{\chi(x)\chi(y)\chi(z^{-1})}{\chi(1)}$$

for any $y \in G$.

Now if $\chi \in \mathrm{Irr}(G/S)$ and $u \in \mathcal{U}$, then $\chi(1) = 1$, $\chi(x)\chi(z^{-1}) = 1 = \chi(u)$. Since G/S is abelian, it follows by condition (b) that

$$\frac{1}{|\mathcal{U}|}\sum_{\chi\in\mathrm{Irr}(G/S)\cup Y',\ u\in\mathcal{U}}\frac{\chi(x)\chi(u)\chi(z^{-1})}{\chi(1)} \geq |G/S|. \tag{4.3}$$

Next, consider any $\chi \in Y_0$, so that $\alpha := \chi|_S \in \mathrm{Irr}(S)$, and let $\beta \in \mathrm{Irr}(J)$ lying above α. By [**2**, Proposition 8.3.3(i)] we have

$$\frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}}\beta(u) = 0, \ \pm 1.$$

Applying Lemma 4.6 to $S \lhd G$ and to $S \lhd J$ we then obtain

$$\left|\frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}}\chi(u)\right| = \left|\frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}}\alpha(u)\right| = \left|\frac{\alpha(1)}{\beta(1)}\cdot\frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}}\beta(u)\right| \leq 1.$$

Together with (4.3), this implies that

$$\frac{1}{|\mathcal{U}|}\left|\sum_{u\in\mathcal{U}}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(x)\chi(u)\chi(z^{-1})}{\chi(1)}\right|$$

$$\geq \left|\frac{1}{|\mathcal{U}|}\sum_{\chi\in\mathrm{Irr}(G/S)\cup Y',\ u\in\mathcal{U}}\frac{\chi(x)\chi(u)\chi(z^{-1})}{\chi(1)}\right| - \left|\frac{1}{|\mathcal{U}|}\sum_{\chi\in Y_0\smallsetminus Y',\ u\in\mathcal{U}}\frac{\chi(x)\chi(u)\chi(z^{-1})}{\chi(1)}\right|$$

$$\geq |G/S| - \left|\sum_{\chi\in Y_0\smallsetminus Y'}\frac{\chi(x)\chi(z^{-1})}{\chi(1)}\cdot\frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}}\chi(u)\right|$$

$$\geq |G/S| - \sum_{\chi\in Y_0\smallsetminus Y'}\frac{|\chi(x)\chi(z^{-1})|}{\chi(1)}\cdot\left|\frac{1}{|\mathcal{U}|}\sum_{u\in\mathcal{U}}\chi(u)\right|$$

$$\geq |G/S| - \sum_{\chi\in Y_0\smallsetminus Y'}\frac{|\chi(x)\chi(z^{-1})|}{\chi(1)} > 0.$$

Hence, there must be some $u\in\mathcal{U}$ such that

$$\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(x)\chi(u)\chi(z^{-1})}{\chi(1)}\neq 0,$$

and Lemma 3.1 contradicts our assumption that (G,S,p) is a counterexample to Conjecture 2.3. □

LEMMA 4.8. *We have that*

$$|\mathbf{C}_G(x)|\leq j|\mathbf{C}_J(x)|\leq j|\mathbf{C}_J(x^j)|.$$

If in addition x^j is regular semisimple and J is defined over $\mathbb{F}_q$, then the following upper bounds hold.

(i) $|\mathbf{C}_J(x^j)|\leq d|\mathbf{C}_S(x^j)|\leq d|\mathcal{T}^F|\leq d(q+1)^r$, *for some F-stable maximal torus $\mathcal{T}$ of $\mathcal{G}_{\mathrm{sc}}$ and* $r=\mathrm{rank}(\mathcal{G})$.

(ii) *Suppose some generator of $\langle x\rangle$ lies in $J\tau$, where $\tau\in\Phi_S$ is induced by a field automorphism of $\mathcal{G}$ which has q_0 as the common absolute value of its eigenvalues while acting on the character group of a τ-stable maximal torus of $\mathcal{G}$. Then there exist a τ-stable maximal torus of $\mathcal{G}$ and $e\leq|\mathbf{Z}(\mathcal{G}^*)|$ such that*

$$|\mathbf{C}_J(x)|\leq e|\mathcal{T}^\tau|\leq e(q_0+1)^r.$$

In fact, one can take $e=1$ if $d=1$.

Proof. The first claim and the inequality $|\mathbf{C}_J(x^j)|\leq d|\mathbf{C}_S(x^j)|$ are obvious. Next, to prove (i) we view S as $L/\mathbf{Z}(L)$, where $L:=\mathcal{G}_{\mathrm{sc}}^F$. Let z be an inverse image of x^j in $\mathcal{G}_{\mathrm{sc}}$ and let D be the full inverse image of $\mathbf{C}_S(x^j)$ in L. Then $\mathbf{C}_{\mathcal{G}_{\mathrm{sc}}}(z)=\mathcal{T}$ is a maximal torus of $\mathcal{G}_{\mathrm{sc}}$, and so $|\mathbf{C}_L(z)|=|\mathcal{T}^F|\leq(q+1)^r$. Next, there is a group homomorphism $f:D\to\mathbf{Z}(L)$ such that $vzv^{-1}=f(v)z$, and $D\geq\mathbf{Z}(L)$. Since $\mathrm{Ker}(f)=\mathbf{C}_L(z)$, it follows that

$$|\mathbf{C}_S(x^j)|=|D|/|\mathbf{Z}(L)|\leq|\mathbf{C}_L(z)|=|\mathcal{T}^F|\leq(q+1)^r,$$

completing the proof.

To prove (ii), first we note that we can replace $(J, \mathcal{G})$ by $(L = \mathcal{G}_{\rm sc}^F, \mathcal{G}_{\rm sc})$ if $d = 1$. Replacing x by a suitable generator of $\langle x\rangle$, we may assume that x acts on J as $g\tau$ with $g \in J$. Since $x^j \in J$ is regular semisimple, $\mathbf{C}_{\mathcal{G}}(x^j)^\circ = \mathcal{T}_1$, a maximal torus. By [**4**, Lemma 13.14(iii)], $|\mathbf{C}_{\mathcal{G}}(x^j)/\mathcal{T}_1| \le |\mathbf{Z}(\mathcal{G}^*)|$, and moreover $\mathbf{C}_{\mathcal{G}}(x^j) = \mathcal{T}_1$ in the case $d = 1$ after we make the noted replacement. As $\mathbf{C}_J(x) \le \mathbf{C}_J(x^j)$, we then have

$$|\mathbf{C}_J(x)| \le e|\mathbf{C}_{\mathcal{T}_1}(x)|.$$

Consider any $v \in \mathbf{C}_{\mathcal{T}_1}(x)$. By the Lang-Steinberg theorem, $g = h^{-1}\tau(h)$ for some $h \in \mathcal{G}$. Now

$$v = v^x = h^{-1}\tau(h)\tau(v)\tau(h^{-1})h,$$

yielding $hvh^{-1} \in \mathcal{G}^\tau$. We have shown that $\mathbf{C}_{\mathcal{T}_1}(x) \le \mathcal{T}^\tau$ for the maximal torus $\mathcal{T} = h\mathcal{T}_1h^{-1}$ of $\mathcal{G}$. Next, $x^j \in \mathbf{C}_{\mathcal{T}_1}(x)$ by [**2**, Proposition 3.5.1], so we also have that $hx^jh^{-1} \in \mathcal{T}^\tau$. Thus the regular semisimple element hx^jh^{-1} is τ-stable, and it is contained in the maximal torus $\mathcal{T}$. Since any regular semisimple element is contained in a unique maximal torus by [**4**, Proposition 14.6(ii)], it follows that $\mathcal{T}$ is τ-stable. Hence

$$|\mathbf{C}_{\mathcal{T}_1}(x)| \le |\mathcal{T}^\tau| \le (q_0 + 1)^r,$$

as desired. □

Recall (see for example [**26**]) that for any integers $n \ge 3$, $a \ge 2$, and $(a, n) \ne (6, 2)$, $a^n - 1$ has a *primitive prime divisor*, that is, a prime divisor that does not divide $\prod_{i=1}^{n-1}(a^i - 1)$; any such divisor will be denoted by $\mathrm{ppd}(a, n)$.

In the even-dimensional unitary case, that is when $S = \mathrm{PSU}_{2m}(q)$ with $m \ge 2$, we will need some extra information. Fix $\theta \in \mathbb{F}_{q^2}^\times$ with $\theta^q = -\theta$, and a basis $(e_1, \dots, e_m, f_1, \dots, f_m)$ of the natural module $W := \mathbb{F}_{q^2}^{2m}$, in which the Hermitian form has Gram matrix

$$\theta\Gamma = \begin{pmatrix} 0 & \theta I_m \\ -\theta I_m & 0 \end{pmatrix}.$$

Note that in this basis, $X \in \mathrm{GU}(W) = \mathrm{GU}_{2m}(q)$ if and only if ${}^tX^{(q)}\Gamma X = \Gamma$, and so we can consider the field automorphism σ that raises any entry of $X \in \mathrm{GU}(W)$ to its $p^{\rm th}$ power. We will also denote by σ its action on S. Then $\mathrm{Aut}(S) = J \rtimes \Phi_S$ with $\Phi_S = \langle\sigma\rangle$. In particular, $j|2f = |\sigma|$.

Proposition 4.9. *Suppose that $S = \mathrm{PSU}_{2m}(q)$ for some $m \ge 2$.*

(i) *Then*

$$|\mathbf{C}_J(x)| \le |\mathbf{Z}(\mathcal{G}^*)| \cdot |\mathcal{T}^{\sigma^{2f/j}}| \le |\mathbf{Z}(\mathcal{G}^*)| \cdot (q^{2/j} + 1)^{2m-1}$$

for a $\sigma^{2f/j}$-stable maximal torus $\mathcal{T}$ of $\mathcal{G}$.

(ii) *Suppose that $(m, q) \ne (3, 2)$ and $j \le 2$, so that $x \in \langle J, \sigma^f\rangle$. Choose $\ell = \mathrm{ppd}(p, 2mf)$ if $2|m$ and $\ell = \mathrm{ppd}(p, mf)$ if $2 \nmid m$. Then there is a p'-element $z \in Sx$ of order divisible by ℓ such that $|\mathbf{C}_J(z)| \le (q^{2m} - 1)/(q + 1)$.*

Proof. (i) By Proposition 4.5, x^j is regular semisimple. Replacing x by a suitable generator of $\langle x\rangle$, we may assume that x acts on J as $g\sigma^{2f/j}$ and $g \in J$. Now the statement follows from Lemma 4.8(ii).

(ii) First we note that $X \in H := \mathrm{GU}(W)$ is fixed by σ^f if and only $X = X^{(q)}$ and ${}^tX\Gamma X = \Gamma$, equivalently, $X \in \mathrm{Sp}_{2m}(q)$. Hence $\mathbf{C}_H(\sigma^f) = \mathrm{Sp}_{2m}(q)$. Furthermore, the choice of ℓ ensures that if $t_1 \in \mathrm{Sp}_{2m}(q)$ has order ℓ, then t_1 has simple spectrum on $W \otimes_{\mathbb{F}_{q^2}} \overline{\mathbb{F}}_{q^2}$, and so t_1 is

regular semisimple in $\mathrm{GU}(W)$. Furthermore, a Sylow ℓ-subgroup of $\mathrm{Sp}_{2m}(q)$, of order the ℓ-part $(q^{2m}-1)_\ell$ of $q^{2m}-1$, is also a Sylow ℓ-subgroup of H. Thus we have shown that some $Q_1 \in \mathrm{Syl}_\ell(H)$ is centralized by σ^f.

On the other hand, using the embedding

$$\mathrm{GL}_1(q^{2m}) \hookrightarrow \mathrm{Stab}_H(\langle e_1,\dots,e_m\rangle_{\mathbb{F}_{q^2}}) \cap \mathrm{Stab}_H(\langle f_1,\dots,f_m\rangle_{\mathbb{F}_{q^2}}) \cong \mathrm{GL}_m(q^2),$$

we can choose $Q \in \mathrm{Syl}_\ell(H)$ inside $\mathrm{GL}_1(q^{2m})$ and check that $\mathbf{C}_H(Q)L = H$ for $L := \mathrm{SU}(W)$. Now an H-conjugate t of t_1 in Q is regular semisimple in H, and $\mathbf{C}_H(t) \geq \mathrm{GL}_1(q^{2m})$. It follows that

$$\mathbf{C}_H(t) = \mathbf{C}_H(Q) = \mathrm{GL}_1(q^{2m}). \tag{4.4}$$

As shown above, Q is centralized by an H-conjugate of σ^f. Hence,

$$H \rtimes \langle\sigma^f\rangle = \mathbf{C}_{H\rtimes\langle\sigma^f\rangle}(Q)L = \mathbf{C}_{H\rtimes\langle\sigma^f\rangle}(t)L.$$

Taking quotient by $\mathbf{Z}(H)$ (and denoting the image of t in S also by t), we see that

$$\mathbf{C}_{J\rtimes\langle\sigma^f\rangle}(t)S = J \rtimes \langle\sigma^f\rangle. \tag{4.5}$$

Now we return to $G = \langle S, x\rangle \leq J \rtimes \langle\sigma^f\rangle$. Using (4.4) we can write $\mathbf{C}_G(t) = \bar{Q} \rtimes D$, where D is an ℓ'-group of order dividing $2(q^{2m}-1)/|\bar{Q}|$ and $\bar{Q} \in \mathrm{Syl}_\ell(S)$ is the image of $Q < L$ in S. Next, (4.5) implies that $G = \mathbf{C}_G(t)S$. As $\bar{Q} < S$, we can find $v \in D$ such that $z := tv \in Sx$. Now $|v|$ is coprime to $p\ell$, so $|z|$ is divisible by ℓ but not by p. Furthermore, the ℓ-part of z is t and $\ell \nmid (q+1) = |\mathbf{Z}(H)|$. It follows that

$$|\mathbf{C}_J(z)| \leq |\mathbf{C}_J(t)| = |\mathbf{C}_H(t)|/|\mathbf{Z}(H)|,$$

and we are done by (4.4). □

We now complete the proof of Theorem 4.1, in steps (a)–(g). Recall that x^j is regular semisimple. Our arguments will rely on Lemma 4.7. In the generic case, we choose $z = x$ and work with a suitable Y_0. In some non-generic cases, such as when $S = \mathrm{PSU}_{2m}(q)$, we will need to make a more refined choice of $z \in Sx$ to ensure the condition 4.7(b). We will denote by σ the field automorphism of S induced by the map $t \mapsto t^p$ of $\overline{\mathbb{F}}_p$. All the small cases excluded in the subsequent proof are handled using [**5**].

(a) We begin with the case $S = \mathrm{PSL}_2(q)$ and $q \geq 11$, whence $d = \gcd(2, q-1) = |\mathbf{Z}(\mathcal{G}^*)|$. First assume that $j = 1$, i.e. $G \leq J = \mathrm{PGL}_2(q)$. As x is regular semisimple, there is a unique $\epsilon = \pm 1$ such that $x \in G \cap T_1$, where $T_1 \cong C_{q-\epsilon}$ is a maximal torus of J. Then we can choose $z \in Sx$ a regular semisimple element in another maximal torus $T_2 \cong C_{q+\epsilon}$ of J. This ensures that $\chi(x)\chi(z) = 0$ for $\chi \in Y_0$ unless

$$\chi \in Y' := \{\chi \in Y_0 \mid \chi(1) = q\}.$$

Since $\chi(u) = 0$ for $\chi \in Y'$ and $u \in S$ any regular unipotent element, we are done.

Assume now that $j \geq 2$. We may assume that some generator of $\langle x\rangle$ lies in $J\tau$, where τ is induced by $\sigma^{f/j}$. Then by Lemma 4.8 we have $|\mathbf{C}_G(x)| \leq jd(q^{1/j}+1)$. Choosing $z = x$, $Y' = \emptyset$, and noting that $\chi(1) \geq (q-1)/d$ for all $\chi \in Y_0$, we see that

$$\Sigma(x,x) = \sum_{\chi(1)\geq(q-1)/d} \frac{|\chi(x)|^2}{\chi(1)} \leq \frac{d|\mathbf{C}_G(x)|}{q-1} \leq \frac{jd^2(q^{1/j}+1)}{q-1} < j \leq |G/S|,$$

if $2 \nmid q \geq 27$ or $2|q \geq 8$. The remaining cases of small q are handled using [**5**].

(b) Next we consider the case $S = \mathrm{PSL}_n(q)$ with $n \geq 3$ and

$$(n,q) \notin \{(3,2),(3,3),(3,4),(3,5),(3,7),(4,2),(4,3),(6,2)\}$$

By Lemma 4.8(i) we have $|\mathbf{C}_G(x)| \le jd(q^n-1)/(q-1)$ with $d = \gcd(n, q-1)$. Define

$$D := \begin{cases} (q^2-1)(q-1)/\gcd(3,q-1), & n=3,\\ (q^3-1)(q-1)/\gcd(2,q-1), & n=4,\\ (q^n-1)(q^{n-1}-q^2)/(q-1)(q^2-1), & n\ge 5,\ (n,q)\ne(6,3),\\ (q^5-1)(q^3-1), & (n,q)=(6,3), \end{cases}$$

and $Y' := \{\chi \in Y_0 \mid \chi(1) < D\}$. Then, according to [**24**, Theorem 3.1], $\chi|_S$ is a Weil character, of degree $(q^n-q)/(q-1)$ or $(q^n-1)/(q-1)$, for any $\chi \in Y_0$. The explicit formulae for Weil characters show that $\chi(u) = 0$ or 1 for any $u \in \mathcal{U}$. Choosing $z = x$ we now see that condition 4.7(b) holds. The assumption on (n, q) shows that

$$\Sigma(x,x) = \sum_{\chi(1)\ge D} \frac{|\chi(x)|^2}{\chi(1)} \le \frac{|\mathbf{C}_G(x)|}{D} < j \le |G/S|, \tag{4.6}$$

and so we are done.

(c) Next we consider the case $S = \mathrm{PSU}_n(q)$ with $n \ge 3$ and

$$(n,q) \notin \{(3,2),(3,3),(3,4),(3,5),(3,7),(3,8),(3,9),(3,11),(4,2),(4,3),(4,5),(5,2),(6,2)\}.$$

By Lemma 4.8(i) we have $|\mathbf{C}_G(x)| \le jd(q+1)^{n-1}$ with $d = \gcd(n, q+1)$. Define

$$D := \begin{cases} (q^2-q+1)(q-1)/\gcd(3,q+1), & n=3,\\ (q^n+1)(q^{n-1}-q^2)/(q+1)(q^2-1), & 2\nmid n\ge 5,\ (n,q)\ne(9,2),\\ 29240, & (n,q)=(9,2),\\ (q^2+1)(q^2-q+1)/\gcd(2,q-1), & n=4,\ j\le 2\\ (q^n-1)(q^{n-1}-q)/(q+1)(q^2-1), & 2|n\ge 6,\ j\le 2\\ (q^n-1)/(q+1), & 2|n\ge 4,\ j\ge 3, \end{cases}$$

and $Y' := \{\chi \in Y_0 \mid \chi(1) < D\}$.

Assume in addition that $2 \nmid q$ and $(n,q) \ne (9,2)$. Then, according to [**24**, Theorem 4.1], $\chi|_S$ is a Weil character, of degree $(q^n-q)/(q+1)$ or $(q^n+1)/(q+1)$, for any $\chi \in Y'$. The explicit formulae for Weil characters [**25**, Lemma 4.1] show that $\chi(u) = 0$ or 1 for any $u \in \mathcal{U}$. Choosing $z = x$ we now see that condition 4.7(b) holds. The assumption on (n, q) shows that (4.6) holds, since $(n,q) \ne (9,2)$. In the exceptional case of $(9,2)$, since $|\Phi_S\Gamma_S| = 2$ and $p \nmid |x|$, we must have that $j = 1$ and $G \le J = \mathrm{PSU}_9(2)\cdot 3$. It is straightforward to show that we can find $z \in Sx$ of order divisible by 19 and $|\mathbf{C}_J(z)| = 171$. Using [**18**], one can check for any $\chi \in Y'$ that either $\chi|_S$ is a Weil character of degree 170 and so again $\chi(u) = 0$ for $u \in \mathcal{U}$, or χ has 19-defect zero, whence $\chi(z) = 0$. Thus condition 4.7(b) holds. Furthermore, by Schwarz' inequality,

$$\Sigma(x,z) = \sum_{\chi(1)\ge D} \frac{|\chi(x)\chi(z^{-1})|}{\chi(1)} \le \frac{\sqrt{|\mathbf{C}_G(x)|\cdot|\mathbf{C}_G(z)|}}{D} \le \frac{\sqrt{3^9\cdot 171}}{29240} < 1,$$

and we are again done.

Now we will assume that $n = 2m \ge 4$. Suppose in addition that $j \le 2$. Then, according to [**24**, Theorem 4.1], $\chi|_S$ is again a Weil character, of degree $(q^n+q)/(q+1)$ or $(q^n-1)/(q+1)$, for any $\chi \in Y'$. We will choose $z \in Sx$ as specified in Proposition 4.9(ii). If $\chi \in Y'$ has degree $(q^n-q)/(q+1)$, then $\chi(u) = 0$ for $u \in \mathcal{U}$ by [**25**, Lemma 4.1]. On the other hand, if $\chi \in Y'$ has degree $(q^n-1)/(q+1)$, then it has ℓ-defect 0 (since $\ell \ge 2f+1$) and so $\chi(z) = 0$. Thus condition 4.7(b) holds. Furthermore,

$$\Sigma(x,z) \le \frac{\sqrt{|\mathbf{C}_G(x)|\cdot|\mathbf{C}_G(z)|}}{D} \le \frac{\sqrt{jd(q+1)^{n-1}\cdot j(q^n-1)/(q+1)}}{D} < j,$$

and so we are done.

Finally, we consider the case $n = 2m \ge 4$ but $j \ge 3$. This implies that $q \ge 8$ (since $f \ge 2$ and moreover $j \ne 2$ if $2|q$). We now choose $z = x$. By [**24**, Theorem 4.1], $\chi|_S$ is a Weil character

of degree $(q^n+q)/(q+1)$ for $\chi \in Y'$, whence $\chi(u)=0$ for $u \in \mathcal{U}$ by [**25**, Lemma 4.1], and condition 4.7(b) holds. Now by Proposition 4.9(i) we have $|\mathbf{C}_G(x)| \le j \cdot |\mathbf{Z}(\mathcal{G}^*)| \cdot (q^{2/3}+1)^{n-1}$ and so

$$\Sigma(x,x) \le \frac{|\mathbf{C}_G(x)|}{D} \le \frac{j \cdot |\mathbf{Z}(\mathcal{G}^*)| \cdot (q^{2/3}+1)^{n-1}}{(q^n-1)/(q+1)} < j,$$

completing the treatment of type A.

(d) Here we consider the case $S = \mathrm{PSp}_{2n}(q)$ with $n \ge 2$ and

$$(n,q) \notin \{(2,2),(2,3),(2,4),(2,5),(2,7),(3,2),(3,3),(4,2),(5,2),(6,2)\}.$$

By Lemma 4.8(i) we have $|\mathbf{C}_G(x)| \le jd(q+1)^n$ with $d = \gcd(2,q-1) = |\mathbf{Z}(\mathcal{G}^*)|$. Define

$$D := \begin{cases} (q^n-1)/2, & 2 \nmid q \\ (q^n-1)(q^n-q)/2(q+1), & 2|q. \end{cases}$$

By [**24**, Theorems 5.2, 5.5], $Y' := \{\chi \in Y_0 \mid \chi(1) < D\}$ is empty.

First we consider the case $j \ge 2$. Then $q \ge p^2$, and we may assume that a generator of $\langle x \rangle$ lies in $J\sigma^{f/j}$. Hence $|\mathbf{C}_G(x)| \le jd(q^{1/j}+1)^n$ by Lemma 4.8(ii). Choosing $z = x$, we then see that

$$\Sigma(x,x) \le \frac{|\mathbf{C}_G(x)|}{D} \le \frac{jd(q^{1/2}+1)^n}{D} < j,$$

and we are done.

Assume now that $j = 1$, and so $G \le J$. Define

$$Y_1 := \{\chi \in Y_0 \mid \chi(1) < D_1 := (q^n-1)(q^n-q)/2(q+1)\}.$$

By [**24**, Theorem 5.2, 5.5], Y_1 can be non-empty only when $2 \nmid q$, in which case $\chi|_S$ is one of the two Weil characters, of odd degree $(q^n-\epsilon)/2$ for (exactly one) $\epsilon = \pm 1$ for any $\chi \in Y_1$. These two Weil characters are fused by any element in $J \smallsetminus S$. It follows that $Y_1 = \emptyset$ if $G > S$. Now we choose z to be an element in $\mathrm{PSL}_2(q^n) < S$ of order $(q^n-\epsilon)/2$ in the case $G = S$ and $2 \nmid q$, and $z = x$ otherwise. In the former case, $\chi(z) = 0$ for any $\chi \in Y_1$ and $|\mathbf{C}_G(z)| = (q^n-\epsilon)/2$. Hence

$$\Sigma(x,z) = \sum_{\chi(1) \ge D_1} \frac{|\chi(x)\chi(z^{-1})|}{\chi(1)} \le \frac{\sqrt{|\mathbf{C}_G(x)| \cdot |\mathbf{C}_G(z)|}}{D_1} \le \frac{d(q+1)^n}{(q^n-1)(q^n-q)/2(q+1)} < 1,$$

and we are done.

(e) Next, let $S = \Omega_{2n+1}(q)$ with $n \ge 3$, $p \ge 3$, and $(n,q) \ne (3,3)$. By Lemma 4.8(i) we have $|\mathbf{C}_G(x)| \le 2j(q+1)^n$. Next, by [**24**, Theorems 6.1], $\chi(1) \ge D := (q^n-1)(q^n-q)/(q^2-1)$ for all $\chi \in Y_0$. Choosing $z = x$ and $Y' := \emptyset$, we have

$$\Sigma(x,x) \le \frac{|\mathbf{C}_G(x)|}{D} \le \frac{2j(q+1)^n}{(q^n-1)(q^n-q)/(q^2-1)} < j,$$

and we are done.

(f) Here we consider the case $S = P\Omega^{\epsilon}_{2n}(q)$ with $n \ge 4$, $\epsilon = \pm$, and

$$(n,q) \ne (4,2),(4,3),(5,2).$$

By Lemma 4.8(i) we have $|\mathbf{C}_G(x)| \le jd(q+1)^n$ with $d = \gcd(4, q^n-\epsilon)$. Define

$$D := \begin{cases} (q^3-1)(q^2+1)(q-1)/2, & n=4, \\ (q^n+1)(q^{n-1}-q)/(q^2-1), & n \ge 5,\ (n,q,\epsilon) \ne (6,2,\pm),(5,3,-), \\ 5002, & (n,q,\epsilon) = (5,3,-),\ \mathbf{C}_G(x^j)S \ge J, \\ 2551, & (n,q,\epsilon) = (5,3,-),\ \mathbf{C}_G(x^j)S \not\ge J, \\ q^{14}, & (n,q) = (6,2), \end{cases}$$

and $Y' := \{\chi \in Y_0 \mid \chi(1) < D\}$. Accordingly, we choose $z = x$ if $n = 4$ or $n \geq 6$ but $(n,q) \neq (6,2)$, $z \in S = Sx = G$ of order $\ell = 31$ if $(n,q,\epsilon) = (6,2,+)$ and $\ell = 13$ if $(n,q,\epsilon) = (6,2,-)$. In all cases we have $|\mathbf{C}_G(z)| \leq dj(q+1)^n$. The assumption on (n,q) now implies that

$$\Sigma(x,z) = \sum_{\chi(1)\geq D} \frac{|\chi(x)\chi(z^{-1})|}{\chi(1)} \leq \frac{\sqrt{|\mathbf{C}_G(x)| \cdot |\mathbf{C}_G(z)|}}{D} \leq \frac{jd(q+1)^n}{D} < j$$

in all but possibly the case where $(n,q,\epsilon) = (5,3,-)$ and $\mathbf{C}_G(x^j)S \not\geq J$. Assume we are in this exceptional case. Then $\mathbf{C}_{G\cap J}(x)S < J$ and $|J/S| = d = 4$, so we have, as in the proof of Lemma 4.8,

$$|\mathbf{C}_{G\cap J}(x^j)| \leq 2|\mathbf{C}_S(x^j)| \leq 2(q+1)^5.$$

Since $|G/(G\cap J)| = j$, we get

$$|\mathbf{C}_G(x)| \leq |\mathbf{C}_G(x^j)| \leq j|\mathbf{C}_{G\cap J}(x^j)| \leq 2j(q+1)^5$$

(instead of the weaker bound $|\mathbf{C}_G(x)| \leq dj(q+1)^5$), and so (4.6) holds in this case as well.

It remains to verify condition 4.7(b). This condition obviously holds in the case where $n \geq 5$ but $(n,q,\epsilon) \neq (6,2,\pm)$, $(5,3,-)$, since in this case $Y' = \emptyset$ by [**24**, Theorem 7.6].

If $n = 4$, then [**18**] implies that $q|\chi(1)$ for all $\chi \in Y'$ (in fact $\chi|_S$ is the nontrivial unipotent character of smallest degree). Now if $\gamma \in \mathrm{Irr}(J)$ lies above $\chi|_S$, then $q|\gamma(1)$ implies by [**2**, Theorem 8.4.8] that γ is not a semisimple character of J, whence $\sum_{u\in\mathcal{U}} \gamma(u) = 0$ by [**2**, p. 280]. It follows from Lemma 4.6 that $\sum_{u\in\mathcal{U}} \chi(u) = 0$ as well.

Suppose $(n,q) = (6,2)$. By [**21**], for any $\chi \in Y'$ either $q|\chi(1)$, or χ has ℓ-defect 0. In the former case, arguing as in the preceding paragraph we see that $\sum_{u\in\mathcal{U}} \chi(u) = 0$. In the latter case, $\chi(z) = 0$ by the choice of z.

Finally, assume that $(n,q,\epsilon) = (5,3,-)$. Consider any $\chi \in Y'$. According to [**5**], $\chi|_S$ is either a unique character α of degree 2379, or one of the two characters $\beta_{1,2}$ of degree 2501. In the former case, $q|\chi(1)$ and so $\sum_{u\in\mathcal{U}} \chi(u) = 0$ as shown above. In particular, condition 4.7(b) holds in the case $\mathbf{C}_G(x^j)S \not\geq J$. Next, using [**18**] one can check that β_1 and β_2 are fused in J. Hence in the remaining case $\mathbf{C}_G(x^j)S \geq J$ we have that $\chi|_S = \alpha$ and again condition 4.7(b) holds.

(g) Now we consider exceptional groups of Lie type, and we assume that

$$S \ncong {}^2B_2(8),\ {}^2G_2(27),\ G_2(3),\ G_2(4),\ {}^3D_4(2),\ {}^2F_4(2)',\ F_4(2),\ {}^2E_6(2).$$

We will choose $z = x$, $Y' = \emptyset$, and let D denote the smallest degree of nontrivial complex irreducible characters of S, as listed in [**23**, Table 1]. Again by Lemma 4.8(i) we have $|\mathbf{C}_G(x)| \leq jd(q+1)^r$ if $S \ncong {}^3D_4(q)$, and $|\mathbf{C}_G(x)| \leq j(q^2+q+1)^2$ if $S \cong {}^3D_4(q)$. Now we can check that

$$\Sigma(x,x) = \sum_{\chi(1)\geq D} \frac{|\chi(x)|^2}{\chi(1)} \leq \frac{|\mathbf{C}_G(x)|}{D} < j.$$

This completes the proof of Theorem 4.1.

We now drop the assumptions and notation from the beginning of this section.

Proof of Theorem C. It suffices to prove the statement in the case $G = \langle S, x\rangle$. In this case, as mentioned in the first paragraph of Section 3, if S is a sporadic simple group, then the statement was checked using [**5**]. The cases where S is an alternating group, respectively a simple group of Lie type in characteristic p, follow from Theorem 3.2 and Theorem 4.1, respectively.

We conclude by giving some evidence in support of Conjecture B in the case $p = 2$ and $G = S$ is an odd-characteristic group of Lie type.

REMARK 4.10. Suppose that S is either a simple classical group in odd characteristic, or $S \in \{{}^2G_2(q), G_2(q), {}^3D_4(q), E_8(q)\}$ with $2 \nmid q$, or $S \cong E_6(q)$ with $4|(q-1)$, or $S \cong {}^2E_6(q)$ with $4|(q+1)$. Then, as shown in §§7.2, 7.4 of [**10**], S contains a regular 2-element u. Certainly, we can also find a regular semisimple element $y \in S$ of odd order. Now by [**7**], $y^S \cdot (u^{-1})^S$ contains any nontrivial semisimple element of S. In particular, if $1 \neq x \in S$ is semisimple of odd order, then we may assume $x = yu^{-1}$, i.e. $xu = y$ has odd order for a nontrivial 2-element u.

References

1. E. BERTRAM, 'Even permutations as a product of two conjugate cycles', *J. Comb. Theory Ser. A* 12 (1972) 368–380.

2. R. CARTER, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters* (Wiley, Chichester, 1985).

3. M. CONDER, 'Answer to a 1962 question by Zappa on cosets of Sylow subgroups', *Adv. Math.* 313 (2017) 167–195.

4. F. DIGNE and J. MICHEL, *Representations of Finite Groups of Lie Type* (London Mathematical Society Student Texts, Cambridge University Press, 1991).

5. The GAP Group, 'GAP–groups, algorithms, and programming, version 4.8.6', 2016, `http://www.gap-system.org.`

6. D. GOLDSTEIN and R. M. GURALNICK, 'Cosets of Sylow p-subgroups and a question of Richard Taylor,' *J. Algebra* 398 (2014) 569–573.

7. R. GOW, 'Commutators in finite simple groups of Lie type', *Bull. London Math. Soc.* 32 (2000) 311–315.

8. D. GORENSTEIN and R. LYONS, 'The local structure of finite groups of characteristic 2 type', *Mem. Amer. Math. Soc.* 276 (1983).

9. D. GORENSTEIN, R. LYONS and R. SOLOMON, *The Classification of the Finite Simple Groups*, Number 3, Mathematical Surveys and Monographs Volume 40 (Amer. Math. Soc., 1998).

10. R. M. GURALNICK, M. W. LIEBECK, E. A. O'BRIEN, A. SHALEV and P. H. TIEP, 'Surjective word maps and Burnside's p^aq^b theorem', *Invent. Math.*, to appear.

11. R. M. GURALNICK and G. MALLE, 'Variations on the Baer–Suzuki theorem', *Math. Z.* 279 (3–4) (2015) 981–1006.

12. R. M. GURALNICK and G. NAVARRO, 'Squaring a conjugacy class and cosets of normal subgroups', *Proc. Amer. Math. Soc.* 144 (5) (2016) 1939–1945.

13. R. M. GURALNICK and G. R. ROBINSON, 'On extensions of the Baer-Suzuki theorem', *Israel J. Math.* 82 (1–3) (1993) 281–297.

14. R. M. GURALNICK and P. H. TIEP, 'Lifting in Frattini covers and a characterization of finite solvable groups', *J. Reine Angew. Math.* 708 (2015) 49–72.

15. M. HERZOG, G. KAPLAN and A. LEV, 'Representation of permutations as products of two cycles', *Discrete Math.* 285 (2004) 323–327.

16. I. M. ISAACS, *Character Theory of Finite Groups* (AMS Chelsea Publishing, Providence, RI, 2006).

17. H. LEE, 'Triples in Finite Groups and a Conjecture of Guralnick and Tiep', PhD Thesis, University of Arizona, 2017.

18. F. LÜBECK, *Character degrees and their multiplicities for some groups of Lie type of rank* < 9, `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/DegMult/index.html`

19. A. MORETÓ and A. SÁEZ, 'Prime divisors of orders of products', *Proc. Edim. Math. Soc.*, to appear.

20. G. NAVARRO, *Character Theory and the McKay Conjecture* (Cambridge Studies in Advanced Mathematics, Cambridge, 2018).

21. H. N. NGUYEN, 'Low-dimensional complex characters of the symplectic and orthogonal groups', *Comm. Algebra* 38 (2010) 1157–1197.

22. J. G. THOMPSON, 'Nonsolvable finite groups all of whose local subgroups are solvable', *Bull. Amer. Math. Soc.* 74 (1968), 383–437.

23. P. H. TIEP, 'Low dimensional representations of finite quasisimple groups', Proceedings of the London Math. Soc. Symposium "Groups, Geometries, and Combinatorics", Durham, 2001 (A. A. Ivanov et al eds., World Scientific, 2003, N. J. et al) 277–294.

24. P. H. TIEP and A. E. ZALESSKII, 'Minimal characters of the finite classical groups', *Comm. Algebra* 24 (1996) 2093–2167.

25. P. H. TIEP and A. E. ZALESSKII, 'Some characterizations of the Weil representations of the symplectic and unitary groups', *J. Algebra* 192 (1997) 130–165.

26. K. ZSIGMONDY, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* 3 (1892) 265–284.

A. Beltrán
Departamento de Matemáticas, Universidad Jaume I, 12071 Castellón, Spain

abeltran@mat.uji.es

R. Lyons and P. H. Tiep
Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA

lyons@math.rutgers.edu
tiep@math.rutgers.edu

A. Moretó, G. Navarro and A. Sáez
Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain

alexander.moreto@uv.es
gabriel@uv.es
azahara.saez@uv.es