Commutators in finite quasisimple groups

Martin W. Liebeck
Imperial College
London SW7 2BZ
UK

E.A. O'Brien
University of Auckland
Auckland
New Zealand

Aner Shalev
Hebrew University
Jerusalem 91904
Israel

Pham Huu Tiep
University of Arizona
Tucson, AZ 85721
USA

Abstract

The Ore Conjecture, now established, states that every element of every finite simple group is a commutator. We prove that the same result holds for all the finite quasisimple groups, with a short explicit list of exceptions. In particular, the only quasisimple groups with non-central elements which are not commutators are covers of A_6, A_7, $L_3(4)$ and $U_4(3)$.

1 Introduction

The Ore conjecture, that every element of every finite (non-abelian) simple group is a commutator, was proved in [17]. In other words, the *commutator width* of every finite simple group is 1. One might expect that the same is true for every finite quasisimple group (i.e., perfect group G such that $G/Z(G)$ is simple). But this is not the case, as was shown by Blau [2]; he lists all quasisimple groups having central elements which are not commutators. On the other hand, Gow [10] has shown that if G is a quasisimple group of Lie type in characteristic p with $Z(G)$ a p'-group, then every semisimple element of G is a commutator.

It is interesting to ask precisely which quasisimple groups possess non-commutators and what they are, and in this paper we answer this question

Liebeck acknowledges the support of a Maclaurin Fellowship from the New Zealand Institute of Mathematics and its Applications. O'Brien acknowledges the support of the Marsden Fund of New Zealand (grant UOA 0721). Shalev acknowledges the support of an ERC Advanced Grant 247034, an EPSRC Visiting Fellowship, an Israel Science Foundation Grant, and a Bi-National Science Foundation grant United States-Israel. Tiep acknowledges the support of the NSF (grant DMS-0901241).

completely. As a consequence, we show that the commutator width of every quasisimple group is at most 2.

Theorem 1 *Let G be a finite quasisimple group. Then every element of G is a commutator, with the exceptions listed in Table 1.*

In particular, the only quasisimple groups having non-central elements which are not commutators are $3.\mathsf{A}_6$, $6.\mathsf{A}_6$, $6.\mathsf{A}_7$, $Z.L_3(4)$ *with* $Z \geq Z_2 \times Z_4$, *and* $Z.U_4(3)$ *with* $Z \geq Z_3 \times Z_6$.

Table 1: Non-commutators x in quasisimple groups

$G/Z(G)$	$Z(G)$	$o(x)$, $x \in Z(G)$	$o(x)$, $x \notin Z(G)$
A_6	Z_3	$-$	12
A_6	Z_6	6	$15, 24$
A_7	Z_6	6	15
$L_3(4)$, $U_4(3)$, M_{22}, Fi_{22}	Z_6	6	$-$
$L_3(4)$, $U_4(3)$, M_{22}	Z_{12}	$6, 12$	$-$
$U_6(2)$, ${}^2E_6(2)$	$\geq Z_6$	6	$-$
$L_3(4)$	$Z_2 \times Z_4$	2	6
	$Z_4 \times Z_4$	4	12
	$Z_2 \times Z_{12}$	$2, 6, 12$	$6, 42$
	$Z_4 \times Z_{12}$	$4, 6, 12$	$12, 84$
$U_4(3)$	$Z_3 \times Z_6$	6	6
	$Z_3 \times Z_{12}$	$6, 12$	$6, 12$

Corollary 2 *Every element of every finite quasisimple group is a product of two commutators.*

We provide two ways to deduce this corollary from Theorem 1. The first is based on the proportion of commutators in quasisimple groups. Using Table 1, one can check that this proportion is at least $151/216$, with equality for $6.\mathsf{A}_6$. In particular, if C is the set of commutators in a finite quasisimple group G, then $|C| > |G|/2$, and this immediately implies $C^2 = G$. The second method is based on the claim that a finite group G satisfying the inequality $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-2} < 2$ has commutator width at most 2 (see Lemma 2.2), and this is verified in Lemma 2.3 for the groups in Table 1.

We note that the sum $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-2}$ has other applications. In [9, 1.6] it is shown that the commutator map $f : G \times G \to G$ is almost measure preserving on finite simple groups G – namely, for any $X \subseteq G$ we have $||f^{-1}(X)|/|G|^2 - |X|/|G|| = o(1)$ as $|G| \to \infty$. That proof works for every collection of finite groups in which $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-2} \to 1$ as $|G| \to \infty$. As shown in [16], this is true for finite quasisimple groups, so we obtain the following.

Proposition 3 *The commutator map on finite quasisimple groups is almost measure preserving.*

In [17] we proved that every element of each of the following quasisimple classical groups is a commutator: $SL_n(q)$, $SU_n(q)$, $Sp_n(q)$, $\Omega_n^{\pm}(q)$. The Schur multipliers of the finite simple groups can be found in [14, 5.1.4]. To prove Theorem 1 it therefore remains to consider the following cases:

(i) double covers of alternating groups;

(ii) spin groups;

(iii) simply connected groups of exceptional Lie type with nontrivial centres (these are types E_6^{ϵ} and E_7);

(iv) nontrivial covers of sporadic groups;

(v) covers of the simple groups with exceptional Schur multipliers: A_6, A_7 and the groups in Table 5.1.D of [14].

We consider cases (iv) and (v) in Section 2, and cases (i)–(iii) in Sections 3, 4, and 5 respectively.

2 Preliminaries

As in [17], we use the following well known character-theoretic criterion of Frobenius to prove that elements are commutators.

Lemma 2.1 *If G is a finite group and $g \in G$, then g is a commutator if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

Lemma 2.2 *Let G be a finite group G satisfying the inequality*

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-2} < 2.$$

Then G has commutator width at most 2.

Proof. It is well known (see for example [22, Section 9]) that the number $N(g)$ of ways to express $g \in G$ as a product of two commutators is $|G|^3 \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)/\chi(1)^3$. Using the fact that $|\chi(g)| \leq \chi(1)$ for the nontrivial characters, we obtain

$$| \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)/\chi(1)^3 - 1| \leq \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \chi(1)^{-2}.$$

Hence if the sum on the right hand side is less than 1, then $N(g) \neq 0$ for all $g \in G$, so G has commutator width at most 2. ■

Lemma 2.3 *Theorem* 1 *and Corollary* 2 *hold for the following quasisimple groups:*

(a) *nontrivial covers of sporadic groups,*

(b) *covers of* A_6 *and* A_7*,*

(c) *covers of the simple groups with exceptional Schur multipliers listed in Table* 5.1.*D of* [*14*].

Proof. The character tables of these groups are available in the Character Table Library of GAP [8] or from [20]. From these one checks using Lemma 2.1 that every element is a commutator, with the exceptions in Table 1, and that the exceptions satisfy the inequality of Lemma 2.2. ■

Our proof of Theorem 1 for cases (i)-(iii) listed at the end of Section 1 will be inductive, and the following lemma addresses the base cases needed for the induction.

Lemma 2.4 *Every element of each of the following groups is a commutator:*

(a) $2\mathsf{A}_n$, $5 \leq n \leq 13$,

(b) $Spin_{2n+1}(3)$ *with* $2 \leq n \leq 5$,

(c) $Spin_{2n+1}(5)$ *with* $1 \leq n \leq 3$,

(d) $Spin^+_{2n}(3)$ *with* $3 \leq n \leq 5$,

(e) $Spin^-_{2n}(3)$ *with* $2 \leq n \leq 5$, *and*

(f) $Spin^-_{2n}(5)$ *with* $2 \leq n \leq 4$.

Proof. Many of the character tables of these groups are available in the Character Table Library of GAP [8] or from [20]; the remainder were constructed directly using the MAGMA [3] implementation of the algorithm of Unger [24]. From the character tables one checks using Lemma 2.1 that every element is a commutator. ■

3 Double covers of alternating groups

Denote by $2\mathsf{A}_n$ ($n \geq 5$) the (quasisimple) double cover of the alternating group A_n. In this section we prove that every element of $2\mathsf{A}_n$ is a commutator.

Definition 3.1 *Let $G = 2\mathsf{A}_n$ with $n \geq 5$, acting naturally on $\{1, 2, \ldots, n\}$. An element x of G is breakable if it lies in a central product $2\mathsf{A}_r * 2\mathsf{A}_{n-r}$ of natural subgroups (which stabilize an r-subset of $\{1, 2, \ldots, n\}$), and one of the following holds:*

(1) $5 \leq r \leq n - 5$;

(2) $r \geq 5$, $g = xy$ *with* $x \in 2\mathsf{A}_r$ *and* $y \in 2\mathsf{A}_{n-r}$, *and* y *is a commutator in* $2\mathsf{A}_{n-r}$.

Otherwise, x is unbreakable.

By the argument of [17, 2.9], Theorem 1 for $G = 2\mathsf{A}_n$ will follow immediately if we prove that every unbreakable element in G with $n \geq 14$ and every element in G with $5 \leq n \leq 13$ is a commutator in G.

First we mention the following obvious observation.

Lemma 3.2 *Every 2-element g in $G = 2\mathsf{A}_4$ is a commutator in G.*

For $x \in 2\mathsf{S}_n$, denote its image in S_n by $\bar{x}$.

Lemma 3.3 *Assume $n \geq 13$ and $g \in 2\mathsf{A}_n$ is unbreakable. Then $\bar{g}$ is S_n-conjugate to one of the following permutations:*

(i) $(1, 2, \ldots, a)(a + 1, a + 2, \ldots, a + b)(n - 2, n - 1, n)$, *with* $a + b = n - 3$ *and* $a, b \geq 2$ *are even;*

(ii) $(1, 2, \ldots, a)(a + 1, a + 2, \ldots, a + b)$, *with* $a + b = n$ *and* $a, b \geq 2$ *are even;*

(iii) $(1, 2, \ldots, n - 3)(n - 2, n - 1, n)$ *and* n *is even;*

(iv) $(1, 2, \ldots, n)$ *and* n *is odd.*

In particular, $|C_{\mathsf{A}_n}(\bar{g})| \leq (3/4) \cdot (n - 3)^2$.

Proof. Decompose $\bar{g} = \bar{x}_1\bar{x}_2 \ldots \bar{x}_s\bar{y}_1\bar{y}_2 \ldots \bar{y}_t$ into a product of disjoint cycles, where the $\bar{x}_i$ have odd lengths $a_1 \leq \ldots \leq a_s$, and the $\bar{y}_j$ have even lengths $b_1 \leq \ldots \leq b_t$. Note that $a_1 \geq 3$ (if $s \geq 1$), otherwise $\bar{g} \in 2\mathsf{A}_{n-1}$ is breakable.

1) First we assume that $t \geq 2$. We choose

$$\bar{x} = \bar{x}_1\bar{x}_2 \dots \bar{x}_s\bar{y}_3 \dots \bar{y}_t, \quad \bar{y} = \bar{y}_1\bar{y}_2.$$

In this case, $\bar{x} \in \mathsf{A}_r$ with $r = \sum_{i=1}^{s} a_i + \sum_{j=3}^{t} b_j$ and $\bar{y} \in \mathsf{A}_{n-r}$ with $n - r = b_1 + b_2 \geq 4$. Next we choose $y \in 2\mathsf{A}_{n-r}$ which projects onto $\bar{y}$. Then gy^{-1} projects onto $\bar{x}$, so $g = xy$ for some $x \in 2\mathsf{A}_r$ which projects onto $\bar{x}$. If $n - r = 4$, then $b_1 = b_2 = 2$, whence y is a 2-element so it is a commutator in $2\mathsf{A}_{n-r}$ by Lemma 3.2. Hence, the unbreakability of g implies that $r \leq 4$. If $s = 1$, then $a_1 = 3$ and we arrive at (i). If $s = 0$, then we arrive at (ii).

2) Now we assume that $t \leq 1$, which implies $t = 0$ as $\bar{g} \in \mathsf{A}_n$. Assume $s \geq 3$. Choosing

$$\bar{x} = \bar{x}_1\bar{x}_2, \quad \bar{y} = \bar{x}_3 \dots \bar{x}_s,$$

we see that $g = xy$, where $x \in 2\mathsf{A}_r$ with $r = a_1 + a_2 \geq 6$ and $y \in 2\mathsf{A}_{n-r}$ with $n - r = \sum_{i=3}^{s} a_i \geq 3$. Since g is unbreakable, we must have $n - r \leq 4$, which implies that $s = 3$, $a_3 = 3$ so $n = 9$, contrary to our assumption. If $s = 2$ but $a_1 \geq 5$, then choosing $\bar{x} = \bar{x}_1$ and $\bar{y} = \bar{x}_2$ we see that $g = xy$ is breakable. Hence we arrive at (iii) or (iv).

The bound on centralizer order follows immediately. ■

We now embark on our proof that unbreakable elements of $2\mathsf{A}_n$ are commutators; it is based on Lemma 2.1. In what follows, let z denote the central involution of $2\mathsf{A}_n$. First we estimate the character ratios coming from the *spin* characters of $2\mathsf{A}_n$.

Lemma 3.4 *Let $n \geq 14$ and let $g \in G = 2\mathsf{A}_n$ be unbreakable. Then*

$$E_1(g) := \sum_{\chi \in \mathrm{Irr}(G),\ z \notin \mathrm{Ker}(\chi)} \left| \frac{\chi(g)}{\chi(1)} \right| < 0.484.$$

Proof. Consider one of the two double covers H of S_n and embed G in H. It is well known, see for instance [11], that the spin characters of H are labelled by the set $\mathcal{D}(n) = \mathcal{D}^+(n) \cup \mathcal{D}^-(n)$ of partitions of n into distinct parts. Here, each $\lambda \in \mathcal{D}^+(n)$ has an even number of even (positive) parts and gives rise to a unique spin character of H which splits into two irreducible constituents over G. On the other hand, each $\lambda \in \mathcal{D}^-(n)$ has an odd number of even (positive) parts and gives rise to two spin characters of H which restrict to the same irreducible character of G. It follows that the number N of spin characters of G is

$$2|\mathcal{D}^+(n)| + |\mathcal{D}^-(n)| \leq 2p_2(n) \leq 2p(n),$$

where $p(n)$ is the number of partitions of n and $p_2(n) = |\mathcal{D}(n)|$. It is also well known [1, Th. 14.5] that $p(n) < e^{\pi\sqrt{2n/3}}$. Furthermore, the degree of every spin character of G is at least $d_1 := 2^{\lfloor (n-2)/2 \rfloor}$, cf. [15]. Since g is unbreakable, by Lemma 3.3

$$\begin{aligned}
\sum_{\chi \in \mathrm{Irr}(G),\ z \notin \mathrm{Ker}(\chi)} |\chi(g)|^2 &= \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g)|^2 - \sum_{\chi \in \mathrm{Irr}(G/Z(G))} |\chi(g)|^2 \\
&= |C_G(g)| - |C_{\mathsf{A}_n}(\bar{g})| \\
&\leq |C_{\mathsf{A}_n}(\bar{g})| \\
&\leq (3/4) \cdot (n-3)^2.
\end{aligned}$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned}
E_1(g) &\leq f_1(n) := \frac{\sqrt{2p_2(n) \cdot (3/4) \cdot (n-3)^2}}{2^{\lfloor (n-2)/2 \rfloor}} \\
&< \frac{n-3}{2^{\lfloor (n-2)/2 \rfloor}} \cdot \sqrt{\frac{3}{2} \cdot e^{\pi \sqrt{2n/3}}} =: f_2(n).
\end{aligned}$$

Direct computation shows that $f_2(n) < 0.462$ when $n \geq 40$. If $30 \leq n \leq 39$, then $p_2(n) \leq p(n) \leq p(39) = 31185$, so $f_1(n) < 0.357$. Similarly, if $26 \leq n \leq 29$, then $p_2(n) \leq p(n) \leq p(29) = 4565$, so $f_1(n) < 0.465$. Another well known fact is that $p_2(n)$ is the number of partitions of n into odd parts. Using GAP and this observation to compute $p_2(n)$, we obtain $f_1(n) \leq 0.376$ for $20 \leq n \leq 25$.

For $14 \leq n \leq 19$, we must refine these estimates. By [15], G has one or two *basic* spin characters, i.e. spin characters of degree d_1, and all other spin characters have degree at least $d_2 \geq 2d_1$. We claim that for $n = 15$ or 17, $d_2 \geq 4d_1$. Indeed, assume that $n = 15$ and that $\chi \in \mathrm{Irr}(G)$ is a spin character of degree $< 4d_1 = 256$. Embedding $K := 2\mathsf{A}_{13}$ naturally in G, we see that every irreducible constituent θ of $\chi|_K$ is faithful at $Z(K) = Z(G)$ but of degree < 256. Inspecting [5], we conclude that θ must be a basic spin character of K, so $\theta(t) = -\theta(1)/2$, where $t \in K$ projects onto a 3-cycle in A_{13}. It follows that $\chi(t) = -\chi(1)/2$. By the main result of [25], this implies that χ is a basic spin character. In the case $n = 17$ and $\chi \in \mathrm{Irr}(G)$ is a spin character of degree $< 4d_1 = 512$, we can argue as before, embedding a double cover L of S_{14} in G and using the character table of L as supplied in GAP. Applying the Cauchy-Schwarz inequality separately to the basic spin and non-basic spin characters of G, we deduce that

$$E_1(g) \leq f_3(n) := \frac{(n-3)\sqrt{3/2}}{d_1} + \frac{(n-3)\sqrt{(3/2)p_2(n)}}{d_2}.$$

Direct computation shows that $f_3(n) < 0.484$ for $14 \leq n \leq 19$. ∎

Recall that the irreducible characters of S_n are labelled by partitions of n: $\lambda \vdash n$ corresponds to $\chi^\lambda \in \mathrm{Irr}(\mathsf{S}_n)$. For instance, $\chi^{(n)} = 1_{\mathsf{S}_n}$, the permutation character of S_n (acting on $\{1, 2, \ldots, n\}$) is $\rho = \chi^{(n)} + \chi^{(n-1,1)}$; furthermore,

$$\chi^{(n-2,2)} = \mathrm{Sym}^2(\rho) - 2\rho, \quad \chi^{(n-2,1^2)} = \wedge^2(\rho) - \rho + 1_{\mathsf{S}_n}. \tag{1}$$

We will need the following result on low-degree irreducible characters of A_n.

Lemma 3.5 *Let $n \geq 14$ and let $\theta \in \mathrm{Irr}(\mathsf{A}_n)$ be an irreducible character of degree $\chi(1) < n(n-1)(n-5)/6$. Then θ is the restriction to A_n of χ^λ for*

$$\lambda \in \{(n), (n-1,1), (n-2,2), (n-2,1^2)\}.$$

Proof. The statement can be checked directly for $n = 14$ using [8]. Assume $n \geq 15$ and let χ be an irreducible constituent of $\mathrm{Ind}_{\mathsf{A}_n}^{\mathsf{S}_n}(\theta)$. Since $\chi(1) < n(n-2)(n-4)/3$, by [21, Result 3], $\chi(1)$ must be one of

$$1, n-1, n(n-3)/2, (n-1)(n-2)/2, n(n-1)(n-5)/6, (n-1)(n-2)(n-3)/6.$$

Using [12] for instance, it is not hard to show that $\chi = \chi^\lambda$, where λ or its associated partition λ' is (n), $(n-1,1)$, $(n-2,2)$, $(n-2,1^2)$, $(n-3,3)$, or $(n-3,1^3)$, respectively. In all these cases, $\lambda \neq \lambda'$, whence χ is irreducible over A_n so $\theta(1) = \chi(1)$. The statement follows. ∎

Lemma 3.6 *Let $n \geq 14$ and let $g \in G = 2\mathsf{A}_n$ be unbreakable. Then*

$$E_2(g) := \sum_{\chi \in \mathrm{Irr}(G),\ \chi \neq 1_G,\ z \in \mathrm{Ker}(\chi)} \left| \frac{\chi(g)}{\chi(1)} \right| < 0.392.$$

Proof. Without loss of generality, we may identify G with A_n and g with $\bar{g}$. Observe that g is S_n-conjugate to one of the four permutations listed in Lemma 3.3.

1) Consider case (i) of Lemma 3.3. Assume that $g = (1, 2, \ldots, a)(a + 1, \ldots, a+b)(n-2, n-1, n)$, with $a, b \geq 2$ being even and $a + b = n - 3$ (so $n \geq 15$). Observe that $\chi(g) \in \mathbb{Z}$ for $\chi \in \mathrm{Irr}(\mathsf{A}_n)$; in particular, $|\chi(g)| \geq 1$ if $\chi(g) \neq 0$. (Indeed, it suffices to consider the case χ does not extend to S_n. In this case, there is some $\varphi \in \mathrm{Irr}(\mathsf{S}_n)$ such that $\varphi(g) = \chi(g) + \chi(xgx^{-1})$ for $x := (1, 2, \ldots, a)$ (recall that $2|a$). But x and g commute, hence $\chi(g) = \varphi(g)/2$ so the claim follows.) Hence the total number N of irreducible characters of A_n which do not vanish at g is at most $|C_{\mathsf{A}_n}(g)| \leq (3/4) \cdot (n-3)^2$. Among these, one is the principal character, another is (the restriction to A_n of) $\chi^{(n-1,1)}$ which takes value -1 at g. Next, (1) implies that

$$\{\chi^{(n-2,2)}(g), \chi^{(n-2,1^2)}(g)\} = \{0, 1\}.$$

Lemma 3.5 and the Cauchy-Schwarz inequality imply that

$$\begin{aligned} E_2(g) &\le \frac{1}{n-1} + \frac{2}{n(n-3)} + \frac{\sqrt{N \cdot |C_{\mathsf{A}_n}(g)|}}{n(n-1)(n-5)/6} \\ &\le \frac{1}{n-1} + \frac{2}{n(n-3)} + \frac{9(n-3)^2}{2n(n-1)(n-5)} \\ &\le 0.392 \end{aligned}$$

since $n \ge 15$.

The same argument applies to case (ii) of Lemma 3.3. Here we use the bound $N \le |C_{\mathsf{A}_n}(g)| \le n^2/4$, so

$$\begin{aligned} E_2(g) &\le \frac{1}{n-1} + \frac{2}{n(n-3)} + \frac{\sqrt{N \cdot |C_{\mathsf{A}_n}(g)|}}{n(n-1)(n-5)/6} \\ &\le \frac{1}{n-1} + \frac{2}{n(n-3)} + \frac{3n}{2(n-1)(n-5)} \\ &\le 0.308 \end{aligned}$$

since $n \ge 14$.

2) Consider case (iii) of Lemma 3.3. Assume that $g = (1, 2, \dots, n-3)(n-2, n-1, n)$. We claim that $|\chi(g)| \ge 1$ for $\chi \in \mathrm{Irr}(\mathsf{A}_n)$ with $\chi(g) \ne 0$. Indeed, it suffices to prove the claim when $\chi(g) \notin \mathbb{Q}$, in particular when χ does not extend to S_n. Now [13, Theorem 2.5.13] implies that χ is an irreducible constituent of the restriction of χ^α to A_n, where

$$\alpha = \left(\frac{n-2}{2}, 3, 2, 1^{\frac{n}{2}-4}\right).$$

Moreover,

$$\chi(g) = \frac{1}{2}\left((-1)^{\frac{n}{2}-1} \pm \sqrt{(-1)^{\frac{n}{2}-1} \cdot 3(n-3)}\right),$$

so the claim follows.

As in 1), we conclude that the total number N of irreducible characters of A_n which do not vanish at g is at most $|C_{\mathsf{A}_n}(g)| = 3(n-3)$. Using (1) one checks that $\chi^{(n-2,2)}(g) = 0$ and $\chi^{(n-2,1^2)}(g) = 1$. Lemma 3.5 and the Cauchy-Schwarz inequality imply that

$$\begin{aligned} E_2(g) &\le \frac{1}{n-1} + \frac{2}{(n-1)(n-2)} + \frac{\sqrt{N \cdot |C_{\mathsf{A}_n}(g)|}}{n(n-1)(n-5)/6} \\ &\le \frac{1}{n-1} + \frac{2}{(n-1)(n-2)} + \frac{18(n-3)}{n(n-1)(n-5)} \\ &\le 0.211 \end{aligned}$$

since $n \geq 14$.

The same argument applies to case (iv) of Lemma 3.3. Here $N \leq |C_{\mathsf{A}_n}(g)| = n$, and

$$\alpha = \left(\frac{n+1}{2}, 1^{\frac{n-1}{2}}\right), \quad \chi(g) = \frac{1}{2}\left((-1)^{\frac{n-1}{2}} \pm \sqrt{(-1)^{\frac{n-1}{2}} \cdot n}\right)$$

for those $\chi \in \mathrm{Irr}(\mathsf{A}_n)$ that are irrational at g. It follows that

$$\begin{aligned} E_2(g) &\leq \frac{1}{n-1} + \frac{2}{(n-1)(n-2)} + \frac{\sqrt{N \cdot |C_{\mathsf{A}_n}(g)|}}{n(n-1)(n-5)/6} \\ &\leq \frac{1}{n-1} + \frac{2}{(n-1)(n-2)} + \frac{6}{(n-1)(n-5)} \\ &\leq 0.126 \end{aligned}$$

since $n \geq 15$. ■

Proposition 3.7 *Every unbreakable $g \in 2\mathsf{A}_n$ with $n \geq 14$ is a commutator.*

Proof. By Lemmas 3.4 and 3.6,

$$\left|\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}\right| \leq E_1(g) + E_2(g) < 0.484 + 0.392 = 0.876,$$

whence the statement follows from Lemma 2.1. ■

Together with Lemma 2.4, Proposition 3.7 completes the proof of Theorem 1 for the double covers of alternating groups.

4 Spin groups

In this section we prove Theorem 1 for spin groups in odd characteristic. We recall some basic facts from spinor theory, cf. [4]. Let q be odd, and let $V = \mathbb{F}_q^m$ be endowed with a non-degenerate quadratic form Q. The *Clifford algebra* $\mathcal{C}(V)$ is the quotient of the tensor algebra $T(V)$ by the ideal $I(V)$ generated by $v \otimes v - Q(v)$, $v \in V$ (here we adopt the convention that $Q(v) = (v, v)$ if $(\cdot, \cdot)$ is the corresponding bilinear form on V). The natural grading on $T(V)$ passes over to $\mathcal{C}(V)$ and allows us to write $\mathcal{C}(V)$ as the direct sum of its even part $\mathcal{C}^+(V)$ and odd part $\mathcal{C}^-(V)$. We denote the identity element of $\mathcal{C}(V)$ by e. The algebra $\mathcal{C}(V)$ admits a canonical anti-automorphism α, which is defined via

$$\alpha(v_1 v_2 \dots v_r) = v_r v_{r-1} \dots v_1$$

for $v_i \in V$. The *Clifford group* $\Gamma(V)$ is the group of all invertible $s \in \mathcal{C}(V)$ such that $sVs^{-1} \subseteq V$. The action of $s \in \Gamma(V)$ on V defines a surjective homomorphism $\phi : \Gamma(V) \to GO(V)$ if m is even, and $\phi : \Gamma(V) \to SO(V)$ if m is odd, with $\mathrm{Ker}(\phi) \geq \mathbb{F}_q^\times e$. If $v \in V$ is nonsingular, then $-\phi(v) = \rho_v$, the reflection corresponding to v. The *special Clifford group* $\Gamma^+(V)$ is $\Gamma(V) \cap \mathcal{C}^+(V)$. Let $\Gamma_0(V) := \{s \in \Gamma(V) \mid \alpha(s)s = e\}$. The *reduced Clifford group*, or the *spin group*, is $Spin(V) = \Gamma^+(V) \cap \Gamma_0(V)$. The sequences

$$1 \longrightarrow \mathbb{F}_q^\times e \longrightarrow \Gamma^+(V) \xrightarrow{\phi} SO(V) \longrightarrow 1,$$

$$1 \longrightarrow \langle -e \rangle \longrightarrow Spin(V) \xrightarrow{\phi} \Omega(V) \longrightarrow 1$$

are exact.

If A is a non-degenerate subspace of V, then we denote by C_A the subalgebra of $\mathcal{C}(V)$ generated by all $a \in A$. We now clarify the relationship between C_A and the Clifford algebra $\mathcal{C}(A)$ of the quadratic space $(A, Q|_A)$. Decompose $V = A \oplus A^\perp$.

Lemma 4.1 *Let (V, Q) be a non-degenerate quadratic space over a field $\mathbb{F}_q$ of odd characteristic. Suppose A is a non-degenerate subspace of dimension ≥ 2 of V, and let C_A be the subalgebra of $\mathcal{C}(V)$ generated by all $a \in A$. Then there is a (canonical) algebra isomorphism $\psi : \mathcal{C}(A) \cong C_A$ which induces a group isomorphism $Spin(A) \cong C_A \cap Spin(V)$. Furthermore, ϕ projects $C_A \cap Spin(V)$ onto the subgroup*

$$\{h \in \Omega(V) \mid h|_{A^\perp} = 1_{A^\perp}\} \cong \Omega(A),$$

with kernel $\langle -e \rangle$.

Proof. 1) Since $\dim A \geq 2$, for $\lambda \in \mathbb{F}_q^\times$ we can find $w \in A$ with $Q(w) = \lambda$ so $w \cdot w = \lambda e$. Thus $C_A \supseteq \mathbb{F}_q^\times e$. Consider the natural embedding $f : A \to \mathcal{C}(V)$ that sends $u \in A$ to $u + I(V)$. The universal property of $\mathcal{C}(A)$ (cf. [4, II.1.1]) implies that f extends to an algebra homomorphism $\psi : \mathcal{C}(A) \to \mathcal{C}(V)$ which maps $\mathcal{C}(A)$ onto C_A. Now fix a basis $(v_1, \ldots, v_m)$ of the $\mathbb{F}_q$-space A and extend it to a basis $(v_1, \ldots, v_n)$ of the $\mathbb{F}_q$-space V. Then $\mathcal{C}(V)$ has a basis

$$(v_{j_1} v_{j_2} \ldots v_{j_r} \mid 0 \leq r \leq n,\ 1 \leq j_1 < j_2 < \ldots < j_r \leq n),$$

where we interpret $v_{j_1} v_{j_2} \ldots v_{j_r}$ with $r = 0$ as the identity element e. In particular, $\dim C_A \geq 2^m = \dim \mathcal{C}(A)$, so ψ is an isomorphism, and

$$(v_{j_1} v_{j_2} \ldots v_{j_r} \mid 0 \leq r \leq m,\ 1 \leq j_1 < j_2 < \ldots < j_r \leq m)$$

is a basis of C_A. Also, ψ maps even elements of $\mathcal{C}(A)$ to elements in $C_A \cap \mathcal{C}^+(V)$ so it maps $\mathcal{C}^+(A)$ into $C_A \cap \mathcal{C}^+(V)$. Observe that $C_A \cap \mathcal{C}^+(V)$ is spanned by $v_{j_1}v_{j_2}\dots v_{j_r}$ with even r and $1 \le j_1 < \dots < j_r \le m$, whence $\dim C_A \cap \mathcal{C}^+(V) = 2^{m-1} = \dim \mathcal{C}^+(A)$. Thus ψ induces an isomorphism $\mathcal{C}^+(A) \cong C_A \cap \mathcal{C}^+(V)$.

2) Abusing notation, we also denote by e the identity element of $\mathcal{C}(A)$, and by α the anti-isomorphism of $\mathcal{C}(A)$ that sends $y_1y_2\dots y_r$ to $y_ry_{r-1}\dots y_1$ for $y_i \in A$. Then ψ sends e to e and commutes with α. Now consider $h \in C_A \cap \mathit{Spin}(V)$. Then $h \in \mathcal{C}^+(V)$, h is invertible, $hVh^{-1} \subseteq V$, and $\alpha(h)h = e$. Since ψ maps $\mathcal{C}^+(A)$ onto $C_A \cap \mathcal{C}^+(V)$, there is some $g \in \mathcal{C}^+(A)$ such that $\psi(g) = h$. Notice that α preserves C_A. Hence $h^{-1} = \alpha(h) \in C_A \cap \mathit{Spin}(V)$. Thus we can also find $g' \in \mathcal{C}^+(A)$ such that $\psi(g') = h^{-1}$, so g' is the inverse of g in $\mathcal{C}(A)$. Also, $\psi(e) = e = \alpha(h)h = \psi(\alpha(g)g)$ which implies that $\alpha(g)g = e$. Using the aforementioned basis of $\mathcal{C}(V)$, we see that $C_A \cap V = A$. Hence,

$$\psi(gAg^{-1}) = hAh^{-1} = hA\alpha(h) \cap hVh^{-1} \subseteq C_A \cap V = A = \psi(A),$$

so $gAg^{-1} \subseteq A$. Thus $g \in \Gamma(A) \cap \mathcal{C}^+(A) \cap \Gamma_0(A) = \mathit{Spin}(A)$, i.e. $\psi(\mathit{Spin}(A))$ contains $C_A \cap \mathit{Spin}(V)$. In particular,

$$|\mathit{Spin}(A)| \ge |C_A \cap \mathit{Spin}(V)|. \tag{2}$$

3) Consider a non-singular $v \in A$. Then $-\phi(v) = \rho_v$ acts trivially on $A^\perp$ and it acts on A as the reflection ρ'_v in $SO(A)$. Recall that $SO(A)$ is generated by the products $\rho'_x\rho'_y$ where x and y run over all non-singular vectors of A. It follows that $\phi(C_A \cap \Gamma^+(V))$ contains the subgroup $SO(A) \times \langle 1_{A^\perp}\rangle$ of $SO(V)$. Similarly, $\Omega(A)$ consists of all the products $\prod_{i=1}^N \rho'_{x_i}$ where $2|N$, $x_i \in A$ is a non-singular vector, and $\prod_{i=1}^N Q(x_i)$ is a square in $\mathbb{F}_q^\times$, cf. [14, pp. 29–30]. Hence $\phi(C_A \cap \mathit{Spin}(V))$ contains the subgroup $\Omega(A) \times \langle 1_{A^\perp}\rangle$ of $\Omega(V)$. As mentioned in 1) we can find $u \in A$ with $Q(u) = -1$. Hence $-e = u^2 \in C_A \cap \mathcal{C}^+(V)$. Also, $\alpha(-e)(-e) = e$ and $(-e)V(-e)^{-1} = V$, so in fact $-e \in C_A \cap \mathit{Spin}(V)$ and $\phi(-e) = 1_V$. Thus we have shown that

$$|C_A \cap \mathit{Spin}(V)| \ge 2 \cdot |\Omega(A)| = |\mathit{Spin}(A)|.$$

Together with (2), this implies that $|C_A \cap \mathit{Spin}(V)| = |\mathit{Spin}(A)|$ so ψ induces a group isomorphism $\mathit{Spin}(A) \cong C_A \cap \mathit{Spin}(V)$. Also, $|C_A \cap \mathit{Spin}(V)| = 2 \cdot |\Omega(A)|$, whence ϕ maps $C_A \cap \mathit{Spin}(V)$ onto $\Omega(A) \times \langle 1_{A^\perp}\rangle$, with kernel $\langle -e\rangle$. ∎

We recall (and extend) the following definition from [17, §2.4].

Definition 4.2 *Let q be an odd prime power and V be a finite-dimensional vector space over $\mathbb{F}_q$ with a non-degenerate quadratic form.*

(i) *An element x of $\Omega(V)$ is breakable if there is a proper, nonzero, non-degenerate subspace W of V such that $x = (x_1, x_2) \in \Omega(W) \times \Omega(W^\perp)$, and one of the following holds:*

(a) *both factors* $\Omega(W)$ *and* $\Omega(W^\perp)$ *are perfect groups;*

(b) $\Omega(W)$ *is perfect, and* x_2 *is a commutator in* $\Omega(W^\perp)$.

Otherwise, x *is unbreakable.*

(ii) *Let* ϕ *be the projection* $Spin(V) \to \Omega(V)$. *Then* $g \in Spin(V)$ *is breakable (unbreakable) if its image* $\phi(g)$ *in* $\Omega(V)$ *is breakable (unbreakable).*

Our treatment of spin groups relies on the following.

Lemma 4.3 *Let* $V = \mathbb{F}_q^n$ *be a vector space over* $\mathbb{F}_q$ *with a non-degenerate quadratic form, where* q *is odd and* $n \geq 5$. *Suppose that, for every proper non-degenerate subspace* U *of* V, *if* $\Omega(U)$ *is perfect, then every element* $x \in Spin(U)$ *is a commutator in* $Spin(U)$. *Then every breakable element in* $Spin(V)$ *is a commutator in* $Spin(V)$.

Proof. Let $g \in Spin(V)$ be breakable and consider the corresponding decompositions $\phi(g) = (\bar{g}_1, \bar{g}_2)$ and $V = W \oplus W^\perp$ as in Definition 4.2(i). Since $\Omega(W)$ is perfect, $\dim W \geq 3$. We claim that either $\dim W^\perp \geq 3$, or $\bar{g}_2 = 1$. For, suppose that $\dim W^\perp \leq 2$. Then $\Omega(W^\perp)$ is not perfect and in fact it is a cyclic group, cf. [14, Prop. 2.9.1]. Hence $\bar{g}_2$ is a commutator in $\Omega(W^\perp)$ so it is 1.

Applying Lemma 4.1 to the subspace W of V, there is some $x \in C_W \cap Spin(V)$ such that $\phi(x) = \bar{g}_1$. If $\bar{g}_2 = 1$, set $s = t = e$, where e is the identity element in $Spin(V)$ as above. Assume $\bar{g}_2 \neq 1$. Then $\dim W^\perp \geq 3$, so Lemma 4.1 is applicable to the subspace $W^\perp$ of V; in particular, $C_{W^\perp} \cap Spin(V) \cong Spin(W^\perp)$. Hence in case (a) of Definition 4.2(i), we can find $y, s, t \in C_{W^\perp} \cap Spin(V)$ such that $y = [s, t]$ and $\phi(y) = \bar{g}_2$. Assume we are in case (b) of Definition 4.2(i). Then $\bar{g}_2 = [\bar{s}, \bar{t}]$ for some $\bar{s}, \bar{t} \in \Omega(W^\perp)$. Again applying Lemma 4.1 to $W^\perp$, we can find $s, t \in C_{W^\perp} \cap Spin(V)$ such that $\phi(s) = \bar{s}$ and $\phi(t) = \bar{t}$. Thus in all cases we have found $s, t \in C_{W^\perp} \cap Spin(V)$ such that $\phi([s, t]) = \bar{g}_2$.

Now $\phi(x \cdot [s, t]) = \bar{g}_1 \bar{g}_2 = \phi(g)$. Recall that ϕ projects $Spin(V)$ onto $\Omega(V)$, with kernel $Z := \langle -e \rangle$. It follows that there is some $z \in Z$ such that $g = zx \cdot [s, t]$. In case 3) of the proof of Lemma 4.1 we showed that $Z \leq C_W \cap Spin(V)$. Hence $zx \in C_W \cap Spin(V) \cong Spin(W)$ is a commutator in $C_W \cap Spin(V)$, i.e. $zx = [u, v]$ for some $u, v \in C_W \cap Spin(V)$. Observe that $C_W \cap Spin(V)$ is contained in $C_W \cap \mathcal{C}^+(V)$ so it commutes with $C_{W^\perp}$ by [23, Lemma 6.1]. Consequently, $g = zx \cdot [s, t] = [u, v] \cdot [s, t] = [us, vt]$ is a commutator in $Spin(V)$. ∎

By the main results of [2] and [6], we need to consider the non-central elements in spin groups over $\mathbb{F}_q$ only for $q = 3, 5$.

Proposition 4.4 *Let G be one of the spin groups $Spin_n^\epsilon(q)$ with $q = 3, 5$. Assume that $n \geq 12$ for $q = 3$, $n \geq 9$ for $q = 5$, and that $q = 3$ if $2|n$ and $\epsilon = +$. Then every unbreakable element in G is a commutator.*

Proof. Let $Z = \langle -e \rangle$ and $S = \Omega_n^\epsilon(q) = G/Z$ for $G = Spin(V) = Spin_n^\epsilon(q)$, and $\phi(g) = \bar{g}$. Then

$$|C_G(g)| \leq 2|C_S(\bar{g})|. \tag{3}$$

Upper bounds for $|C_S(\bar{g})|$ are given in [17, Prop. 5.15] for $n > 12$, and in [17, Prop. 5.16] for $n = 12$ (note that in the exceptional case $\bar{g} = \pm(J_2^6)$ of [17, 5.16(ii)], g is a commutator as it lies in a subgroup $Spin_4^+(3^3) = SL_2(27) \times SL_2(27)$).

We follow the proof of [17, Lemma 5.17] using this bound for $C_G(g)$. As usual, we will show that $|E(g)| < 1$ for $E(g) := E_1(g) + E_2(g)$, and

$$E_1(g) := \sum_{\chi \in \mathrm{Irr}(G),\ 1 < \chi(1) \leq d(G)} \frac{\chi(g)}{\chi(1)}, \quad E_2(g) := \sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) > d(G)} \frac{\chi(g)}{\chi(1)},$$

where $d(G)$ is chosen suitably. We use the better bounds of [7] for the number, $k(G)$, of conjugacy classes of G.

Case 1a: $G = Spin_{2n}^-(5)$ with $n \geq 6$.

By [7, Cor. 5.1], $k(G) \leq 5^n + 40 \cdot 5^{n-1} = 9 \cdot 5^n$, whereas in the proof of [17, Lemma 5.17] we used the weaker bound $k(S) \leq 116 \cdot 5^n$. Hence, in view of (3), the same arguments as in the proof of [17, Lemma 5.17] yields $|E_2(g)| < 0.09$ for $d(G) := 5^{4n-10}$. By [17, Cor. 5.8], all the characters χ in $E_1(g)$ are trivial at Z. Hence there is no change for $E_1(g)$ so $|E_1(g)| \leq 0.432$ and $|E(g)| < 0.522$.

Case 1b: $G = Spin_{10}^-(5)$.

As mentioned in the proof of [17, Lemma 5.17], $k(S) = 2633$ so $k(G) \leq 5266$; furthermore, $|C_G(g)| \leq 5^{10} \cdot 576$. Hence, if we choose $d(G) := 16 \cdot 5^9$, then the same arguments as in the proof of [17, Lemma 5.17] yields $|E_2(g)| < 0.35$. We break $E_1(g)$ into two sub-sums:

$$E_{11}(g) := \sum_{\chi \in \mathrm{Irr}(G),\ 1 < \chi(1) \leq 4 \cdot 5^9} \frac{\chi(g)}{\chi(1)}, \quad E_{12}(g) := \sum_{\chi \in \mathrm{Irr}(G),\ 4 \cdot 5^9 < \chi(1) \leq d(G)} \frac{\chi(g)}{\chi(1)}.$$

By [17, Prop. 5.3, 5.7], all 9 characters χ in $E_{11}(g)$ are trivial at Z. Hence, as in the proof of [17, Lemma 5.17], $|E_{11}(g)| \leq 0.432$. Using [20] one checks that E_{12} involves exactly 6 characters. By the Cauchy-Schwarz inequality,

$$|E_{12}(g)| \leq \sqrt{6 \cdot 5^{10} \cdot 576}/(4 \cdot 5^9) < 0.024.$$

It follows that $|E(g)| < 0.806$.

Case 2a: $G = Spin_{2n+1}(5)$ with $n \geq 5$.

By [7, Cor. 5.1], $k(G) \leq 5^n + 40 \cdot 5^{n-1} = 9 \cdot 5^n$, whereas in the proof of [17, Lemma 5.17] we used the weaker bound $k(S) \leq (14.76) \cdot 5^n$. Hence, in view of (3), the same arguments as in the proof of [17, Lemma 5.17] yields $|E_2(g)| < 0.02$ for $d(G) := 5^{4n-8}$. By [17, Cor. 5.8], all the characters χ in $E_1(g)$ are trivial at Z. Hence there is no change for $E_1(g)$, so $|E_1(g)| \leq 0.432$ and $|E(g)| < 0.452$.

Case 2b: $G = Spin_9(5)$.

By [7, Cor. 5.1], $k(S) \leq 9 \cdot 5^4$; furthermore, $|C_G(g)| \leq 2 \cdot 5^5$ by (3). Hence, if we choose $d(G) := 4^{10}$, then the same arguments as in the proof of [17, Lemma 5.17] yields $|E_2(g)| < 0.01$. Using [20] one checks that E_1 involves exactly 13 characters and each has degree at least 16276. By the Cauchy-Schwarz inequality,

$$|E_1(g)| \leq \sqrt{13 \cdot 2 \cdot 5^5}/16276 < 0.02.$$

It follows that $|E(g)| < 0.03$.

Case 3: $G = Spin_{2n+1}(3)$ with $n \geq 6$.

By [7, Cor. 5.1], $k(G) \leq 3^n + 40 \cdot 3^{n-1} < (14.34) \cdot 3^n$, whereas in the proof of [17, Lemma 5.17] we used the weaker bound $k(S) \leq (14.76) \cdot 3^n$. Hence, in view of (3), the same arguments as in the proof of [17, Lemma 5.17] yields $|E_2(g)| < 0.06$ for $d(G) := 3^{4n-8}$. As above, there is no change for $E_1(g)$, so $|E_1(g)| \leq 0.35$ and $|E(g)| < 0.41$.

Case 4a: $G = Spin^{\epsilon}_{2n}(3)$ with $n > 6$.

By [7, Cor. 5.1], $k(G) \leq 3^n + 40 \cdot 3^{n-1} < (14.34) \cdot 3^n$, whereas in the proof of [17, Lemma 5.17] we used the weaker bound $k(S) \leq 28 \cdot 3^n$. Hence, in view of (3), the same arguments as in the proof of [17, Lemma 5.17] yields $|E_2(g)| < 0.42$ for $d(G) := 3^{4n-10}$. As above, there is no change for $E_1(g)$, so $|E_1(g)| \leq 0.35$ and $|E(g)| < 0.77$.

Case 4b: $G = Spin^{\epsilon}_{12}(3)$.

By [7, Cor. 5.1], $k(S) < 14.34 \cdot 3^6$; furthermore, $|C_G(g)| \leq 3^{16} \cdot 2^7$ by (3). We will now break up $E(g)$ into four sub-sums

$$E_i(g) = \sum_{\chi \in \mathrm{Irr}(G),\ d_{i-1} < \chi(1) \leq d_i} \frac{\chi(g)}{\chi(1)},$$

where $1 \leq i \leq 4$, $d_0 = 1$, $d_1 = 3^{14}$, $d_2 = 11 \cdot 10^6$, $d_3 = 78 \cdot 10^6$, and $d_4 = \sqrt{|G|}$. Using the data of [20], we see that $E_1(g)$ involves exactly 7 characters listed in [17, Prop. 5.7], $E_2(g)$ involves at most 5 characters, and $E_3(g)$ involves at most 15 characters. As in the proof of [17, Lemma 5.17], $|E_1(g)| \leq 0.35$.

By the Cauchy-Schwarz inequality,

$$|E_2(g)| \leq \frac{\sqrt{5 \cdot 3^{17} \cdot 2^9}}{3^{14}} < 0.035, \quad |E_3(g)| \leq \frac{\sqrt{15 \cdot 3^{17} \cdot 2^9}}{11 \cdot 10^6} < 0.027,$$

and

$$|E_4(g)| \leq \frac{\sqrt{14.34 \cdot 3^6 \cdot 3^{17} \cdot 2^9}}{78 \cdot 10^6} < 0.098.$$

Consequently, $|E(g)| < 0.574$. ■

In view of Lemma 2.4, this completes the proof of Theorem 1 for the spin groups.

5 Simply connected groups of exceptional Lie type

In this section we prove Theorem 1 for simply connected groups of exceptional Lie type. Let G be such a group. By [17] we can assume that $Z(G) \neq 1$, so G is $E_7(q)$ with q odd or $E_6^{\epsilon}(q)$ with $3|q-\epsilon$, and $|Z(G)| = 2$ or 3 respectively.

By [2], every element of $Z(G)$ is a commutator; and by [6], the same holds for all non-central elements provided $q \geq 5$ (for $E_7(q)$), $q \geq 7$ (for $E_6(q)$) and $q \geq 8$ (for ${}^2E_6(q)$). Thus it remains to consider the groups $E_7(3)$, $E_6(4)$, ${}^2E_6(2)$ and ${}^2E_6(5)$. In fact ${}^2E_6(2)$ is covered by [17, 3.1]; so the proof of Theorem 1 is completed by the following result.

Lemma 5.1 *Every element of each of the simply connected groups $E_7(3)$, $E_6(4)$ and ${}^2E_6(5)$ is a commutator.*

Proof. The proof is similar to that in [17, Section 7], so we give just a sketch. Let G be one of the groups in the statement. We claim that G possesses semisimple subgroups M containing $Z(G)$, as in the following table.

G	M
$E_7(3)$	$D_6(3)$, $A_2^{\delta}(3)A_5^{\delta}(3)$ $(\delta = \pm)$
$E_6^{\epsilon}(q)$	$A_5^{\epsilon}(q)$, $A_2^{\epsilon}(q)^3$, $A_2(q^2)A_2^{-\epsilon}(q)$

The existence of these subgroups is given by [18]; that they contain $Z(G)$ can be seen by considering their actions on the minimal modules of dimensions 56 (for E_7) and 27 (for E_6) on which $Z(G)$ acts faithfully – see [19, 2.3].

By results in [17] (for groups of type SL, SU) and the previous section (for simply connected D_6), every element of each of the subgroups M is the above table is a commutator in M.

Recall [17, Lemma 7.2]: the group $G = E_7(q)$ (resp. $E_6^{\epsilon}(q)$) has one irreducible character of degree $q(q^{14}-1)(q^6+1)/(q^4-1)$ (resp. $q(q^4+$

$1)(q^6+\epsilon q^3+1))$, and all other nontrivial irreducible characters have degree at least q^{26} (resp. $q^{16}/2$); moreover $k(G) \le (2.5)q^7$ (resp. $(1.5)q^6$).

First consider $G = E_7(q)$ with $q = 3$. Let $\langle z\rangle = Z(G)$ and let $x \in G$. Define

$$E(x) = \sum_{1\neq\chi\in\mathrm{Irr}(G)} \frac{\chi(x)}{\chi(1)}.$$

We are done if we show that $|E(x)| < 1$.

Suppose that x or zx is a non-identity unipotent element. As in the first step of the proof of [17, Theorem 7.1] for $E_7(q)$,

$$|E(x)| \le \frac{3}{4} + \frac{|C_G(x)|^{1/2}k(G)^{1/2}}{q^{26}}.$$

Hence $|E(x)| < 1$ if $|C_G(x)| \le q^{45}/40$, so we can assume that $|C_G(x)| > q^{45}/40$. As in [17], this implies that the unipotent element x or zx is in one of the classes labelled $(A_3+A_1)'$, $(A_3+A_1)''$, A_3, $2A_2+A_1$, $2A_2$, A_2+3A_1, A_2+2A_1, A_2+A_1, A_2, $4A_1$, $(3A_1)'$, $(3A_1)''$, $2A_1$, A_1. In all cases we argue as in [17] that x lies in a subgroup $A_5^\delta(q)A_2^\delta(q)$ for some δ. This is one of the subgroups M in the table above, and it contains z; hence x and zx are commutators in M.

Now suppose $x = su$ has unipotent part u and semisimple part $s \notin Z$. As above, using the 19/20 bound for $|\chi(x)/\chi(1)|$ in [17, 7.2(ii)],

$$|E(x)| \le \frac{19}{20} + \frac{|C_G(x)|^{1/2}k(G)^{1/2}}{q^{26}}.$$

Hence we may assume that $|C_G(x)| > q^{45}/1000$, so $C_G(s)$ has a quasisimple normal subgroup $C = A_r^\epsilon(q)$ ($r = 5, 6$ or 7), $D_5^\epsilon(q)$, $D_6(q)$ or $E_6^\epsilon(q)$.

If $C = A_5^\epsilon(q)$, $D_5^\epsilon(q)$ or $E_6^\epsilon(q)$, then we argue as in the proof of [17, Theorem 7.1] that x lies in a subgroup $M = A_5^\delta(q)A_2^\delta(q)$, giving the conclusion as before. If $C = A_6^\epsilon(q)$ then either $\epsilon = +$ and $|s| = 2$, or $\epsilon = -$ and $|s|$ divides 4; neither of these is possible, since if $|s| = 2$ then $s = z \in Z(G)$, and if $|s| = 4$ then $C_G(s) \rhd A_7^-(3)$. If $C = A_7^\epsilon(q)$ then the bound on $|C_G(x)|$ forces the Jordan form of u on the 8-dimensional space for C to have at least 2 trivial blocks; hence $x = su$ centralizes a subgroup $A_1 = SL_2(q)$ in C corresponding to these 2 blocks, so $x \in C_G(A_1) = M = D_6(q)$, so is a commutator in M. Finally, consider the case where $C = D_6(q)$. Here $C_G(s) = D_6(q)A_1(q)$ (with $|s| = 2$ and $s \in Z(D_6(q))$) or $D_6(q) \circ 4$ (with $|s| = 4$). In the latter case, $u \in D_6(q)$ and $x = su$ is a commutator in $D_6(q)A_1(q)$ (as s is a commutator in $A_1(3)$). In the former case, we argue as in [17] that x lies in either $D_6(q)$ or $A_5^\delta(q)A_2^\delta(q)$, giving the conclusion as before. This completes the proof for $G = E_7(q)$.

We briefly consider $G = E_6^\epsilon(q)$. Recall that $(q,\epsilon) = (4,+)$ or $(5,-)$. As in the E_6^ϵ proof of [17, Theorem 7.1], we argue that $x \in G$ lies in one of the subgroups M in the above table, and hence x is a commutator in M. ■

This completes the proof of Theorem 1.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[2] H. Blau, A fixed-point theorem for central elements in quasisimple groups, *Proc. Amer. Math. Soc.* **122** (1994), 79–84.

[3] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[4] C. Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras. Collected works*, vol. **2**, Springer-Verlag, Berlin, 1997.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.

[6] E.W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671.

[7] J. Fulman and R. M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups, *Trans. Amer. Math. Soc.* (to appear).

[8] The GAP group, GAP - *Groups, Algorithms, and Programming*, Version 4.4, 2004, `http://www.gap-system.org`.

[9] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems, *Trans. Amer. Math. Soc.* **361** (2009), 4631–4651.

[10] R. Gow, Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* **32** (2000), 311–315.

[11] P. N. Hoffman and J. F. Humphreys, *Projective Representations of the Symmetric Group*, Clarendon Press, Oxford, 1992.

[12] G. D. James, On the minimal dimensions of irreducible representations of symmetric groups, *Math. Proc. Cam. Phil. Soc.* **94** (1983), 417–424.

[13] G. D. James and A. Kerber, *The Representation Theory of the Symmetric Group*, Addison-Wesley, 1981.

[14] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. no. 129, Cambridge University Press, 1990.

[15] A. S. Kleshchev and Pham Huu Tiep, On restrictions of modular spin representations of symmetric and alternating groups, *Trans. Amer. Math. Soc.* **356** (2004), 1971–1999.

[16] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups, and representation varieties, *Invent. Math.* **159** (2005), 317–367.

[17] M.W. Liebeck, E.A. O'Brien, A. Shalev and Pham Huu Tiep, The Ore Conjecture, *J. Europ. Math. Soc.*, **12** (2010), 939–1008.

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

[19] M.W. Liebeck and G.M. Seitz, Reductive subgroups of exceptional algebraic groups, *Mem. Amer. Math. Soc.*, Vol. 121, No. 580, 1996.

[20] F. Lübeck, Data for Finite Groups of Lie Type and Related Algebraic Groups. `www.math.rwth-aachen.de/~Frank.Luebeck/chev`

[21] R. Rasala, On the minimal degrees of characters of S_n, *J. Algebra* **45** (1977), 132–181.

[22] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, *Annals of Math.* **170** (2009), 1383–1416.

[23] Pham Huu Tiep and A. E. Zalesskii, Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), 291–315.

[24] W.R. Unger, Computing the character table of a finite group, *J. Symbolic Comput.* **41** (2006), 847–862.

[25] D. B. Wales, Some projective representations of S_n, *J. Algebra* **61** (1979), 37–57.