The Ore conjecture

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, posed in 1951, states that every element of every finite non-abelian simple group is a commutator. Despite considerable effort, it remains open for various infinite families of simple groups. In this paper we develop new strategies, combining character theoretic methods with other ingredients, and use them to establish the conjecture.

Liebeck acknowledges the support of a Maclaurin Fellowship from the New Zealand Institute of Mathematics and its Applications. O'Brien acknowledges the support of an LMS Visitor Grant, the Marsden Fund of New Zealand (grant UOA 0721), and the Mathematical Sciences Research Institute (Berkeley). Shalev acknowledges the support of an EPSRC Visiting Fellowship, an Israel Science Foundation Grant, and a Bi-National Science Foundation grant United States-Israel 2004-052. Tiep acknowledges the support of the NSF (grant DMS-0600967), and the Mathematical Sciences Research Institute (Berkeley).

1 Introduction

In 1951 Ore [40] conjectured that every element of every finite non-abelian simple group is a commutator. Much work on this conjecture has been done over the years. In the same paper, Ore established the conjecture for the alternating groups; in a series of papers, Thompson [44, 45, 46] established it for $PSL_n(q)$. Gow [22] proved that the conjecture holds for the symplectic groups $PSp_{2n}(q)$ if $q \equiv 1 \bmod 4$, and in [23] proved that every semisimple element of a finite simple group of Lie type is a commutator. The conjecture was established for the sporadic groups in [37]. Bonten [3] proved the conjecture for exceptional groups of Lie type of rank at most 4. An important breakthrough was made by Ellers and Gordeev [12], who showed that the conjecture holds for groups of Lie type over a finite field $\mathbb{F}_q$, provided q is not too small ($q \geq 8$ suffices).

Recently progress was made on probabilistic aspects of the conjecture. Shalev [41] proved that if g is a random element of a finite simple group G, then the probability that g is a commutator tends to 1 as $|G| \to \infty$. This implies that every element of a large finite simple group is a product of two commutators. In [19] it is shown that the commutator map on finite simple groups is almost measure-preserving, a result having applications to the product replacement algorithm [7].

In this paper we complete the proof of Ore's conjecture.

Theorem 1 *If G is a finite non-abelian simple group, then every element of G is a commutator.*

In fact we prove a little more for the classical groups, showing that in every quasisimple classical group $SL_n(q)$, $SU_n(q)$, $Sp_n(q)$, $\Omega_n^{\pm}(q)$, every element is a commutator (see Theorems 4.1, 5.1, 6.1 and Lemma 2.1). (Here, by a quasisimple group we mean a perfect group G such that $G/Z(G)$ is simple.) However it is *not* true that every element of every quasisimple group is a commutator: the smallest counterexample is $3.A_6$, where no element of order 12 is a commutator; other examples appear in [2].

Let us now describe the strategy of our proof, which combines three main ingredients: character theory, induction on the dimension, and certain computer calculations. Unlike previous methods, this strategy works well when the underlying field is small (which we are able to assume by the results of [12] mentioned above). In fact, using generic character tables of various low rank groups of Lie type, our approach could be used to handle groups over arbitrary underlying finite fields.

One of the connections with character theory is based on the classical result of Frobenius [16] that an element g of a finite group G is a commutator if and only if $\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)/\chi(1) \neq 0$, where the sum is over the set $\mathrm{Irr}(G)$ of irreducible characters of G. We use the character theory of

finite groups of Lie type to construct *explicitly* irreducible characters of relatively small degrees, and to derive information on their character values. Roughly speaking, we show that if g is an element with a small centralizer, then $|\chi(g)|/\chi(1)$ is small for $\chi \neq 1$, and the main contribution to the sum $\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)/\chi(1)$ comes from the trivial character $\chi = 1$. This enables us to deduce that this sum is positive, so elements with small centralizers are commutators. We use some of the Deligne-Lusztig theory, and also the theory of dual pairs and Weil characters of classical groups. We expect that our explicit construction of irreducible characters of relatively small degrees will be useful in other applications: it is already used in [36].

For elements whose centralizers are not small, our strategy is to reduce to groups of Lie type of lower dimension and use induction. In our proof for symplectic or orthogonal groups, this is usually possible since such elements have a Jordan decomposition into several Jordan blocks, and hence lie in a corresponding direct product of smaller symplectic or orthogonal groups; if we can (inductively) express each block as a commutator in the smaller classical group, then clearly the original element is itself a commutator. However, various technical difficulties have to be overcome to make this idea work. For instance, some blocks may lie in a symplectic or orthogonal group which is not perfect, such as $Sp_2(2)$, $Sp_2(3)$, $Sp_4(2)$, $\Omega_4^+(2)$, and so on; or in the orthogonal case they may have determinant -1. This inductive approach is phrased in terms of "unbreakable" elements, introduced in Section 2.4.

For exceptional groups, we adopt a similar approach: again the aim is to show that elements with reasonably large centralizer lie in suitable semisimple subsystem subgroups so that induction can be applied. This is achieved using a large amount of technical information on conjugacy classes and centralizers in these groups.

For the unitary groups, the inductive strategy does not work well, mainly because the Jordan blocks can have many different determinants (for example for $PSU_n(7)$ there are 8 possible values). We adopt a different approach, more in the spirit of Thompson's method for $PSL_n(q)$. Some of the ingredients are again character theoretic – but this time using characters to solve certain equations in unitary groups; and also computation to establish certain properties of unitary matrices in small dimensions.

Computation, performed using Magma [4], played a significant role in proving the theorem. Firstly, since the proofs are inductive, we need to establish various base cases. The conjecture is proved directly for a large number of such base cases by constructing the character table of the relevant group and using the character theoretic criterion for commutators discussed above. For various other groups which are too large to prove the entire conjecture by computation, such as symplectic groups of dimension at most 16 over $\mathbb{F}_3$, we explicitly construct certain elements with prescribed Jordan forms as commutators (see Lemma 4.14 for example). Secondly, our proof

of the conjecture for unitary groups is based on an ability to solve certain equations in such groups (see Section 6). For large dimensions the required properties are proved using character theory, but in small dimensions they do not always hold, and we use computation to establish precisely which unitary matrices have the properties; this information is fundamental to the proof. These are the most challenging computations, requiring careful organisation and various refinements to control the number of explicit equations to be solved. We emphasize that such calculations are *effective*: that the resulting matrices indeed enjoy these properties was verified directly in all cases. A rough estimate for the entire computation is about 150 weeks of CPU time, distributed over a number of machines.

The layout of the paper is as follows. In Section 2 we present some preliminary results, and in Section 3 computational methods are applied to provide the base for our inductive proofs. The symplectic, orthogonal, unitary and exceptional groups are then considered in turn.

Due to the length of this paper we shall discuss extensions of the Ore conjecture, as well as further applications of the method developed here, in a separate paper.

Notation The number of conjugacy classes of a finite group G is denoted by $k(G)$. By a group of simply connected Lie type we mean the fixed points of a Frobenius morphism on a simple algebraic group of simply connected type. For example, the families SL, SU, Sp and the spin groups are all of simply connected type. We use standard Lie theoretic notation for groups of Lie type. Moreover $A_n^\epsilon(q)$ ($\epsilon = \pm$) denotes $A_n(q)$ when $\epsilon = +$ and ${}^2A_n(q)$ when $\epsilon = -$, with similar notation for other types with twisted analogues. For $D_4^\epsilon(q)$ we extend this to allow $\epsilon \in \{+, -, 3\}$, so including ${}^3D_4(q)$.

For a vector space V over a field $\mathbb{F}$, $g \in GL(V)$ and $\lambda \in \overline{\mathbb{F}}$ (the algebraic closure of $\mathbb{F}$), we denote by $e(g, \lambda)$ the dimension of the kernel of $g - \lambda \cdot \mathrm{Id}$ on $V \otimes_{\mathbb{F}} \overline{\mathbb{F}}$; further, $d(g) := e(g, 1)$. The fixed point space of $g \in GL(V)$ is denoted by $C_V(g)$, and $\langle , \rangle$ is an inner product. Finally, J_i always denotes an $i \times i$ unipotent Jordan block matrix.

2 Preliminaries

2.1 Previous results on Ore's conjecture

Here we summarize some of the results on Ore's conjecture mentioned in the introduction.

Lemma 2.1 ([44, 45, 46]) *Every element of $SL_n(q)$ is a commutator, except when $(n, q) = (2, 2), (2, 3)$.*

Lemma 2.2 ([3]) *The Ore conjecture holds for all of the simple groups* ${}^2B_2(q)\,(q>2)$, $G_2(q)\,(q>2)$, ${}^2G_2(q)\,(q>3)$, ${}^3D_4(q)$, $F_4(q)$, ${}^2F_4(q)'$.

In [2], Blau proves that with a few specified exceptions, every central element of a finite quasisimple group is a commutator. Here is a particular instance of his result.

Lemma 2.3 ([2]) *If G is a quasisimple group of simply connected Lie type, then every element of $Z(G)$ is a commutator.*

Combining this with the results of Ellers and Gordeev (see [12, Theorem 2] and the remarks following it), we have the following.

Lemma 2.4 *Let G be one of the following groups, of simply connected type:*

$$\begin{array}{l} B_n(q)\,(q\geq 7)\\ C_n(q)\,(q\geq 4)\\ D_n(q)\,(n\geq 4, q\geq 5)\\ {}^2D_n(q)\,(n\geq 4, q\geq 7)\\ {}^2A_n(q)\,(q\geq 8)\\ E_6(q)\,(q\geq 7)\\ {}^2E_6(q)\,(q\geq 8)\\ E_7(q)\,(q\geq 5)\end{array}$$

Every element of G is a commutator.

2.2 Some character theory

In our proofs we use some of the Deligne-Lusztig theory of irreducible characters of groups of Lie type, as expounded in [10]. Let $G = G(q)$ be a finite group of Lie type, of simply connected type in characteristic p. The irreducible characters of G fall into Lusztig series $\mathcal{E}(G,s)$, one for each conjugacy class representative s in the dual group G^* (which is of adjoint type). Moreover there is a bijection $\chi \to \psi$ from $\mathcal{E}(G,s)$ to $\mathcal{E}(C_{G^*}(s),1)$, and the degree of χ is given by

$$\chi(1) = |G^* : C_{G^*}(s)|_{p'}\psi(1). \tag{1}$$

The characters in $\mathcal{E}(G,1)$ are the unipotent characters of G, and formulae for their degrees can be found in [6, 13.8-9].

Next we state for convenient reference the characterization of commutators mentioned in the introduction.

Lemma 2.5 *If G is a finite group and $g \in G$, then g is a commutator if and only if*

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

This lemma follows immediately from a well known result of Frobenius that the number of solutions (x, y) to the equation $[x, y] = g$ in a finite group G is equal to $|G| \sum_{\chi \in \ \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}$ (see [16, p. 13]).

Finally, we prove an elementary result which helps bound the character sums in Lemma 2.5 in terms of the number of conjugacy classes $k(G)$ and centralizer order $|C_G(g)|$.

Lemma 2.6 *Let G be a finite group and let $g \in G$. The following hold:*

(i) $\sum_{\chi \in \ \mathrm{Irr}(G)} |\chi(g)| \leq k(G)^{1/2} |C_G(g)|^{1/2}$;

(ii) *If $\chi_1, \ldots, \chi_k \in \ \mathrm{Irr}(G)$ are distinct characters of degree at least N, then $\sum_{i=1}^{k} |\chi_i(g)|/\chi_i(1) \leq (k|C_G(g)|)^{1/2}/N$. In particular,*

$$\sum_{\chi \in \ \mathrm{Irr}(G), \chi(1) \geq N} \frac{|\chi(g)|}{\chi(1)} \leq \frac{k(G)^{1/2} |C_G(g)|^{1/2}}{N}.$$

Proof Part (i) follows from the fact that $\sum_{\chi \in \ \mathrm{Irr}(G)} |\chi(g)|^2 = |C_G(g)|$, together with the Cauchy-Schwarz inequality. Part (ii) is proved in a similar manner. ∎

2.3 Conjugacy class numbers in classical groups

An important ingredient of our analysis is the following result of Fulman and Guralnick [17] that bounds the number $k(G)$ of conjugacy classes of finite classical groups G. Recall that $GO_n^\epsilon(q)$ denotes the full isometry group of some non-degenerate quadratic form on $\mathbb{F}_q^n$.

Proposition 2.7 ([17])

(i)
$$\begin{aligned} &k(SL_2(q)) \leq q + 4, \\ &k(SL_3(q)) \leq q^2 + q + 8, \\ &k(SL_n(q)) \leq q^n/(q-1) + q^{n/2+1} \text{ if } n \geq 4. \end{aligned}$$

(ii)
$$\begin{aligned} &k(SU_3(q)) \leq q^2 + q + 10, \\ &k(SU_n(q)) \leq 11.5((q^n/(q+1)) + ((q+1)q^{n/2+1}/(q-1)) \text{ if } n \geq 4. \end{aligned}$$

(iii) $k(Sp_{2n}(q)) \leq 12q^n$ *if q is odd, and* $k(Sp_{2n}(q) \leq 17q^n$ *if q is even.*

(iv) $k(GO^{\pm}_{2n}(q)) \leq 29q^n$ *if* q *is odd, and* $k(GO^{\pm}_{2n}(q)) \leq 17.5q^n$ *if* q *is even. Further,* $k(SO_{2n+1}(q)) \leq 7.38q^n$ *for* q *odd.*

The bound in Proposition 2.7 for $k(GO^{\pm}_{2n}(q))$ is too crude for our purposes when n is small. We now state precise values for these numbers.

Lemma 2.8 *Assume* q *is odd.*

$$k(GO^{\epsilon}_{10}(q)) = \frac{1}{2}\left(q^5 + 7q^4 + 25q^3 + \left\{ \begin{array}{l} 68q^2 + 144q + 171 \\ 70q^2 + 148q + 173 \end{array} \right)\right;$$

$$k(GO^{\epsilon}_{12}(q)) = \frac{1}{2}\left(q^6 + 7q^5 + 25q^4 + \left\{ \begin{array}{l} 71q^3 + 172q^2 + 320q + 326 \\ 69q^3 + 170q^2 + 316q + 324 \end{array} \right)\right;$$

$$k(GO^{\epsilon}_{14}(q)) = \frac{1}{2}\left(q^7 + 7q^6 + 25q^5 + 70q^4 + \left\{ \begin{array}{l} 177q^3 + 385q^2 + 640q + 593 \\ 179q^3 + 389q^2 + 646q + 595 \end{array} \right)\right;$$

in the formulae the first row is for $\epsilon = +$ *and the second row is for* $\epsilon = -$.

Proof By [50, p. 38], $k(GO^{+}_{2n}(q)) - k(GO^{-}_{2n}(q))$ is the coefficient of t^n in $\prod_{i=1}^{\infty}(1 - t^{2i-1})/(1 - qt^{2i})$, which is

$$\left\{ \begin{array}{ll} -q^2 - 2q - 1, & n = 5, \\ q^3 + q^2 + 2q + 1, & n = 6, \\ -q^3 - 2q^2 - 3q - 1, & n = 7. \end{array} \right.$$

Further, $k(GO^{+}_{2n}(q)) + k(GO^{-}_{2n}(q))$ is the coefficient of t^{2n} in $\prod_{i=1}^{\infty}(1 + t^{2i-1})^4/(1 - qt^{2i})$, which is

$$\left\{ \begin{array}{ll} q^5 + 7q^4 + 25q^3 + 69q^2 + 146q + 172, & n = 5, \\ q^6 + 7q^5 + 25q^4 + 70q^3 + 171q^2 + 318q + 325, & n = 6, \\ q^7 + 7q^6 + 25q^5 + 70q^4 + 178q^3 + 387q^2 + 643q + 594, & n = 7. \end{array} \right.$$

The statements follow. ∎

2.4 Unbreakable elements

As sketched in the introduction, our proof of Ore's conjecture for classical groups is inductive. We rephrase this inductive approach using the terminology of "unbreakable" elements, which we now define.

Definition Let $G = Cl(V) = Sp(V)$, $SU(V)$ or $\Omega(V)$, where V is a finite-dimensional vector space over $\mathbb{F}_q$ with a non-degenerate symplectic, unitary or quadratic form fixed by G. An element x of G is *breakable* if there is a proper, nonzero, non-degenerate subspace W of V such that $x = (x_1, x_2) \in Cl(W) \times Cl(W^{\perp})$, and one of the following holds:

(1) both factors $Cl(W)$ and $Cl(W^\perp)$ are perfect groups;

(2) $Cl(W)$ is perfect, and x_2 is a commutator in $Cl(W^\perp)$.

Otherwise, x is *unbreakable*.

Lemma 2.9 *Let $G = Cl(V) = Sp(V)$, $SU(V)$ or $\Omega(V)$, and assume that G is a perfect group. Suppose that whenever W is a non-degenerate subspace of V such that $Cl(W)$ is a perfect group, every unbreakable element of $Cl(W)$ is a commutator in $Cl(W)$. Then every element of G is a commutator.*

Proof The proof goes by induction on $\dim V$. The inductive hypothesis holds for all perfect subgroups of G of the form $Cl(X)$ with X a non-degenerate subspace of V.

If $x \in G$ is unbreakable, then it is a commutator by hypothesis. Otherwise x is breakable, so $x = (x_1, x_2) \in Cl(W) \times Cl(W^\perp)$ satisfies (1) or (2) in the above definition. In either case, by induction x_1, x_2 are commutators in $Cl(W)$, $Cl(W^\perp)$ respectively, and so x is a commutator, as required. ■

To show that unbreakable elements are commutators, we apply character theory and Lemma 2.6 in particular. An important step is to show that unbreakable elements have rather small centralizers.

3 Some low rank cases

In this section we establish Ore's conjecture for some groups of Lie type of small rank. These are base cases for our inductive proof of Ore's conjecture in the following sections.

Lemma 3.1 *Every element of each of the following groups is a commutator:*

(i) $Sp_{2n}(2)\,(3 \le n \le 6)$;

(ii) $Sp_{2n}(3)\,(2 \le n \le 5)$;

(iii) $SU_3(q)\,(3 \le q \le 7)$, $SU_4(q)\,(q \le 7)$, $SU_5(q)\,(q \le 4)$ *or* $SU_6(q)\,(q \le 4)$, $SU_7(2)$;

(iv) $\Omega_n^\pm(2)\,(8 \le n \le 12)$, $\Omega_n^\pm(3)\,(7 \le n \le 11)$, $\Omega_7(5)$;

(v) *simply connected* $D_4(q)\,(q \le 4)$ *or* ${}^2D_4(q)\,(q \le 5)$;

(vi) $E_6(2)$ *or simply connected* ${}^2E_6(2)$.

Proof With two exceptions, we proved these results by applying Lemma 2.5 to the character table of the relevant group. Some of these character tables are available in the Character Table Library of GAP [18]; the remainder were constructed directly using the MAGMA implementation of the algorithm of Unger [49].

It was not possible, using available memory and time resources, to construct the character tables of either $Sp_{10}(3)$ or $\Omega_{11}(3)$. Instead, for each group, its conjugacy classes were computed using the algorithm of [5]; by constructing random commutators in the group and deciding their conjugacy classes, we exhibited a commutator in each conjugacy class, and so verified the conjecture directly. ■

Combining this with Lemmas 2.1 and 2.4, we obtain the following.

Corollary 3.2 *Every element of each of the following groups of simply connected Lie type is a commutator: $A_2^\epsilon(q)$, $A_3^\epsilon(q)$, $D_4^\epsilon(q)$ (excluding $A_2^-(2) = SU_3(2)$).*

4 Symplectic groups

In this section we prove the following result, which implies Ore's conjecture for the symplectic groups.

Theorem 4.1 *Every element of the symplectic group $Sp_{2m}(q)$ is a commutator, excluding $Sp_2(2), Sp_2(3)$ and $Sp_4(2)$.*

By Lemma 2.4, the only cases requiring proof are $q = 2$ or 3. For convenience we handle these separately.

4.1 Proof of Theorem 4.1 for $q = 2$

This is mainly based on character theory, using Lemma 2.5. We use the following "gap" result for irreducible characters of symplectic groups in even characteristic, taken from [24, 6.2].

Lemma 4.2 *Let $G = Sp_{2n}(q)$ with q even, $n \geq 4$. There is a collection $\mathcal{W}$ of $q + 3$ irreducible characters of G, such that*

(i) $\chi(1) \geq \frac{(q^n-1)(q^n-q)}{2(q+1)}$ *if* $\chi \in \mathcal{W}$, *and*

(ii) $\chi(1) \geq \frac{1}{2}(q^{2n}-1)(q^{n-1}-1)(q^{n-1}-q^2)/(q^4-1)$ *for* $1 \neq \chi \in \mathrm{Irr}(G)\backslash\mathcal{W}$.

The proof of Theorem 4.1 when $q = 2$

Let $G = Sp_{2n}(2)$ with $n \geq 3$, and let $V = V_{2n}(2)$ be the natural module for G. For $x \in G$, define

$$E_1(x) = \sum_{\chi\in\mathcal{W}} \frac{\chi(x)}{\chi(1)}, \quad E_2(x) = \sum_{1\neq\chi\in\ \mathrm{Irr}(G)\backslash\mathcal{W}} \frac{\chi(x)}{\chi(1)}, \tag{2}$$

where $\mathcal{W}$ is the set of characters in Lemma 4.2. Since

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)}{\chi(1)} = 1 + E_1(x) + E_2(x),$$

Lemma 2.5 gives the following.

Lemma 4.3 *If $|E_1(x)| + |E_2(x)| < 1$, then x is a commutator in G.*

We now bound $E_1(x)$ and $E_2(x)$.

Lemma 4.4 *Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|E_2(x)| < 0.6$.*

Proof In the definition of $E_2(x)$ the sum is over at most $k(G)$ characters, each of which, by Lemma 4.2, has degree at least

$$\frac{1}{30}(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4).$$

Lemma 2.6(ii) and Proposition 2.7(iii) imply that

$$|E_2(x)| < \frac{30\sqrt{17} \cdot 2^{n/2}|C_G(x)|^{1/2}}{(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4)}.$$

This is less than 0.6 when $|C_G(x)| < 2^{2n+15}$ and $n \geq 7$. ∎

Lemma 4.5 *Suppose that $n \geq 7$ and $x \in G$ is such that $\dim C_V(x) \leq n$. Then $|E_1(x)| < 0.2$.*

Proof This is based on a detailed analysis of the characters in $\mathcal{W}$, taken from [24, Section 3]. We have

$$\mathcal{W} = \{\zeta_n^1, \rho_n^1, \rho_n^2, \alpha_n, \beta_n\},$$

with degrees as follows:

χ	ζ_n^1	ρ_n^1	ρ_n^2	α_n	β_n
$\chi(1)$	$\frac{2^{2n}-1}{3}$	$\frac{(2^n+1)(2^n-2)}{2}$	$\frac{(2^n-1)(2^n+2)}{2}$	$\frac{(2^n-1)(2^n-2)}{6}$	$\frac{(2^n+1)(2^n+2)}{6}$

Moreover,

$$\rho_n^1(x) + \rho_n^2(x) = |C_V(x)| - 2, \tag{3}$$

and, via the embedding $G = Sp_{2n}(2) < SU_{2n}(2)$, taking $\bar{V} := V_{2n}(4)$ to be the unitary space, we see that both $|\zeta_n^1(x)|$ and $|\alpha_n(x) + \beta_n(x)|$ are at most

$$\frac{1}{3}(2^{\dim C_{\bar{V}}(x)} + 2^{\dim C_{\bar{V}}(\omega x)} + 2^{\dim C_{\bar{V}}(\omega^2 x)}), \tag{4}$$

where $\omega \in \mathbb{F}_4$ is a cube root of unity.

Now we estimate the contributions of the characters in $\mathcal{W}$ to $E_1(x)$. Since $x \in G = Sp_{2n}(2)$ and $\dim C_V(x) \leq n$ by hypothesis, the dimensions of $C_{\bar{V}}(x)$, $C_{\bar{V}}(\omega x)$ and $C_{\bar{V}}(\omega^2 x)$ are all at most n, and hence

$$|\zeta_n^1(x)| \leq 2^n, \;\; |\alpha_n(x) + \beta_n(x)| \leq 2^n.$$

Therefore

$$|\tfrac{\alpha_n(x)}{\alpha_n(1)} + \tfrac{\beta_n(x)}{\beta_n(1)}| \leq \tfrac{|\alpha_n(x)+\beta_n(x)|}{\beta_n(1)} + \tfrac{\beta_n(1)-\alpha_n(1)}{\beta_n(1)} \leq \tfrac{2^n \cdot 12}{(2^n+1)(2^n+2)}.$$

As $n \geq 7$ this gives

$$|\frac{\alpha_n(x)}{\alpha_n(1)} + \frac{\beta_n(x)}{\beta_n(1)}| < 0.1. \tag{5}$$

Similarly

$$|\frac{\zeta_n^1(x)}{\zeta_n^1(1)}| \leq \frac{2^n \cdot 3}{2^{2n}-1} < 0.03. \tag{6}$$

Finally

$$|\frac{\rho_n^1(x)}{\rho_n^1(1)} + \frac{\rho_n^2(x)}{\rho_n^2(1)}| \leq \frac{|\rho_n^1(x) + \rho_n^2(x)|}{\rho_n^2(1)} + \frac{\rho_n^2(1) - \rho_n^1(1)}{\rho_n^2(1)},$$

and since $\rho_n^1(x) + \rho_n^2(x) = |C_V(x)| - 2 \leq 2^n - 2$, and $n \geq 7$, this yields

$$|\frac{\rho_n^1(x)}{\rho_n^1(1)} + \frac{\rho_n^2(x)}{\rho_n^2(1)}| < 0.04. \tag{7}$$

The conclusion now follows from (5), (6) and (7). ■

Recall the definition of an unbreakable element of G given in Section 2.4.

Lemma 4.6 *Assume $n \geq 4$. Let $x \in Sp(V) = Sp_{2n}(2)$, and suppose one of the following holds:*

(i) *x fixes a non-degenerate subspace W of V with $6 \leq \dim W \leq n$;*

(ii) *$C_V(x)$ contains a nonzero non-degenerate subspace.*

Then x is breakable.

Proof If (i) holds then $x \in Sp(W) \times Sp(W^\perp)$, and both factors are perfect since W and $W^\perp$ have dimension at least 6. In case (ii), let W be a non-degenerate 2-space in $C_V(x)$. Then $x = (1_W, x_2) \in Sp(W) \times Sp(W^\perp)$. Obviously 1_W is a commutator in $Sp(W)$, and $Sp(W^\perp)$ is perfect as $\dim W^\perp \geq 6$. Hence x is breakable in either case. ■

Lemma 2.9 shows that it suffices to prove that every unbreakable element of G is a commutator. The following is a key step towards this goal.

Lemma 4.7 *Assume $n \geq 7$, and let x be an unbreakable element of $G = Sp(V) = Sp_{2n}(2)$. Then $|C_G(x)| < 2^{2n+15}$.*

Proof Since x is unbreakable, by Lemma 4.6 every non-degenerate subspace of V fixed by x has dimension either at most 4, or at least $2n-4$; and $C_V(x)$ is totally singular.

First assume that x is unipotent, and let $x = (J_i^{m_i})$ be the Jordan form of x, where J_i denotes a unipotent Jordan block of dimension i. By [25, p. 172], any minimal non-degenerate $\langle x \rangle$-submodule of V is either a single Jordan block, or a sum of two Jordan blocks of equal size. By the first paragraph, the following hold:

(a) $m_1 = 0$;

(b) if $m_i = 1$, then i is even, and either $i \geq 2n-4$ or $i \leq 4$;

(c) if $m_i \geq 2$, then either $i \leq 2$, or $i \geq n-2$.

It follows that the possible Jordan forms for x are

$$(J_{n-2}^2, J_4 \text{ or } J_2^2),\ (J_{n-1}^2, J_2),\ (J_n^2),\ (J_{2n-4}, J_4 \text{ or } J_2^2),\ (J_{2n-2}, J_2),\ J_{2n}.$$

We refer to [50, p. 60] (see also [30]) for the structure of $C_G(x)$. From this we see that

$$|C_G(x)| \leq 2^{k+f} \prod |Sp_{m_i - \delta_i}(2)|, \tag{8}$$

where k is the number of "big component sets", δ_i is 0 if m_i is even and is 1 if m_i is odd, and

$$f = \sum_{i<j} i m_i m_j + \frac{1}{2} \sum (i-1) m_i^2 + \frac{1}{2} \sum m_i.$$

From the definition, k is certainly no more than the total number of Jordan blocks, so it is clear that the largest centralizer occurs for $x = (J_{n-2}^2, J_2^2)$. For this class, (8) gives

$$|C_G(x)| < 2^{2n+15},$$

as in conclusion (i). This completes the proof when x is unipotent.

The general case is similar. Write $x = su$, where $s \neq 1$ is the semisimple part of x and u is the unipotent part. Then

$$C_G(s) = Sp_{2r}(2) \times \prod GL_{a_i}^{\epsilon_i}(2^{b_i}),$$

where each $\epsilon_i = \pm 1$, $2r = \dim C_V(s)$, and $r + \sum a_i b_i = n$; and $C_G(x) = C_{C_G(s)}(u)$. By the first paragraph of the proof, each of the quantities $r, a_i b_i$ is either at most 2, or at least $n-2$; and not all of them are at most 2. Hence either $2r \geq 2n-4$, or there exists i with $2a_i b_i \geq 2n-4$. In the former case, we apply the above analysis to the unipotent element u acting on the non-degenerate $2r$-dimensional space $C_V(s)$ to deduce that $|C_G(x)| <$

2^{2n+15}, giving the conclusion (i). In the latter case, write $a = a_i, b = b_i$, so $2ab \geq 2n-4$ and in its action on the appropriate non-degenerate $2ab$-subspace, u gives a unipotent element u_0 of $GL_a^\epsilon(2^b)$. Each Jordan block J_k of u_0 gives an x-invariant non-degenerate $2bk$-subspace of V, so it follows that the Jordan decomposition of u_0 is one of

$$(J_{a-2}, J_2 \text{ or } J_1^2),\ (J_{a-1}, J_1).$$

The size of the centralizer of u in $C_G(s)$ is given by [50, p. 34]. The centralizer of maximal size occurs when $b = 1$, $\epsilon = -$, $a = n$ and $u = u_0 = (J_{n-2}, J_1^2)$. In this case

$$|C_G(x)| = |C_{GU_n(2)}(u)| < 2^{2n+4}.$$

Conclusion (i) follows. This completes the proof. ■

Lemma 4.8 *For $n \geq 3$, every unbreakable element of $Sp_{2n}(2)$ is a commutator.*

Proof Let $G = Sp(V) = Sp_{2n}(2)$ with $n \geq 3$, and let $x \in G$ be unbreakable. If $3 \leq n \leq 6$ then x is a commutator by Lemma 3.1(i). Now assume that $n \geq 7$.

As x is unbreakable, $\dim C_V(x) \leq n$ by 4.6, and $|C_G(x)| < 2^{2n+15}$ by Lemma 4.7. It follows from Lemma 4.4 that $|E_2(x)| < 0.6$, and from Lemma 4.5 that $|E_1(x)| < 0.2$. Lemma 4.3 implies that x is a commutator, as required. ■

Lemmas 4.8 and 2.9 now imply that every element of G is a commutator, completing the proof of Theorem 4.1 for $q = 2$.

4.2 Proof of Theorem 4.1 for $q = 3$

As before, we start with a "gap" result for characters, this time for symplectic groups in odd characteristic, taken from [47, 5.2].

Lemma 4.9 *Let $G = Sp_{2n}(q)$ with q odd, $n \geq 2$. Then G has a collection $\mathcal{W}$ of 4 irreducible characters of degree $\frac{1}{2}(q^n \pm 1)$, such that $\chi(1) \geq (q^n - 1)(q^n - q)/2(q+1)$ for $1 \neq \chi \in Irr(G)\backslash\mathcal{W}$.*

We require more detailed information about character degrees and conjugacy class numbers of $Sp_{20}(3)$.

Lemma 4.10 *Let $G = Sp_{20}(3)$.*

(i) *G has a collection $\mathcal{X}$ of 4 irreducible characters such that if $\chi \in Irr(G)\backslash(1 \cup \mathcal{W} \cup \mathcal{X})$, then $\chi(1) > 3^{19}/2$. The degrees of the characters in $\mathcal{X}$ are $3(3^9 - \epsilon)(3^{10} - \epsilon)/8$ ($\epsilon = \pm 1$) and $(3^{20} - 1)/8$.*

(ii) *$k(G) = 602929$.*

Proof (i) This goes a little beyond [47, Theorem 5.2], and is proved by the same method, using some of the Deligne-Lusztig theory described in Section 2.2. Here $G = Sp_{20}(3)$ and the dual group is $G^* = SO_{21}(3)$. Formulae for the degrees of the unipotent characters of G can be found in the proof of [47, 5.1]; following that proof, we find that there are just two unipotent characters of degree at most $3^{19}/2$, and these have degree $3(3^9 - \epsilon)(3^{10} - \epsilon)/8$ with $\epsilon = \pm 1$.

For the non-unipotent characters of degree at most $3^{19}/2$, by (1) these must occur in Lusztig series $\mathcal{E}(G, s)$ with $|G^* : C_{G^*}(s)|_{3'} \leq 3^{19}/2$, and it follows that $C_{G^*}(s)$ must be $SO^{\pm}_{20}(3).2$ or $(SO_{19}(3) \times SO^-_2(3)).2$; moreover the corresponding unipotent character of $C_{G^*}(s)$ must be a linear character. The first possibility for $C_{G^*}(s)$ gives the characters in $\mathcal{W}$, and the second gives two further characters of degree $(3^{20} - 1)/8$.

(ii) The number of conjugacy classes of G is given by [50, p. 36]: it is the coefficient of t^{20} in the infinite product $\prod_{l=1}^{\infty}(1 + t^{2l})^4/(1 - 3t^{2l})$. ■

We need the following result about the values of the characters in $\mathcal{W}$.

Lemma 4.11 *Let $G = Sp_{2n}(q)$ with $n \geq 3$ and q odd. Let $x \in G$ with $|C_G(x)| \leq q^e$. If $\chi \in \mathcal{W}$ then $|\chi(x)| \leq q^{\sqrt{e/2}}$.*

Proof We know (see for example [31, p. 79]) that for $\chi \in \mathcal{W}$ there are complex numbers a, b of modulus 1 such that

$$\chi(x) = \frac{1}{2}(a \cdot |C_V(x)|^{1/2} + b \cdot |C_V(-x)|^{1/2}), \tag{9}$$

where $V = V_{2n}(q)$ is the natural module.

Consider first the case where x is unipotent. Let the Jordan form of x be $(J_i^{n_i})$. By [50, p. 34],

$$|C_G(x)| = q^k \prod_{i \text{ odd}} Sp_{n_i}(q) \prod_{i \text{ even}} q^{n_i/2} O_{n_i}(q),$$

where $k = \sum_{i<j} i n_i n_j + \sum_i (i-1) n_i^2/2$. Since $|Sp_{n_i}(q)| > \frac{1}{2} q^{n_i(n_i+1)/2}$ and $|O_{n_i}(q)| > \frac{1}{2} q^{n_i(n_i-1)/2}$, it follows that

$$|C_G(x)| > q^{f/2} \cdot 2^{-g}, \tag{10}$$

where $g = |\{i : n_i \neq 0\}|$ and

$$f = 2 \sum_{i<j} i n_i n_j + \sum_i i n_i^2 + \sum_{i \text{ odd}} n_i.$$

Let $l = \dim C_V(x)$. Then $l = \sum_i n_i$, so

$$f = (\sum n_i)^2 + \sum (i-1)n_i^2 + 2\sum (i-1)n_i n_j + \sum_{i \text{ odd}} n_i \geq l^2 + l.$$

Also $g \leq l/2$ (recall that $n \geq 3$ by hypothesis). Hence (10) implies that

$$|C_G(x)| > q^{l^2/2}.$$

By hypothesis, $|C_G(x)| \leq q^e$ and so $l < \sqrt{2e}$; hence from (9), $|\chi(x)| \leq \frac{1}{2}q^{l/2} < \frac{1}{2}q^{\sqrt{e/2}}$ for $\chi \in \mathcal{W}$, as required. This completes the proof where x is unipotent.

Now consider the general case, $x = su$ with s, u the semisimple and unipotent parts of x. For $\epsilon = \pm$ let $V_\epsilon = C_V(\epsilon s)$, and set $l_\epsilon = \dim V_\epsilon$. Then $C_G(s)$ contains $Sp(V_+) \times Sp(V_-)$, and we see as above that

$$|C_{Sp(V_\epsilon)}(u)| > q^{l_\epsilon^2/2}.$$

Hence $e \geq \frac{1}{2}(l_+^2 + l_-^2)$ (where $|C_G(x)| \leq q^e$), and so it follows from (10) that for $\chi \in \mathcal{W}$,

$$|\chi(x)| \leq \frac{1}{2}(q^{l_+/2} + q^{l_-/2}) \leq q^{\sqrt{e/2}}.$$

This completes the proof. ■

The proof of Theorem 4.1 for $q = 3$

Let $G = Sp_{2n}(3)$ with $n \geq 2$, let $x \in G$, and define $E_1(x), E_2(x)$ as in (2) (where $\mathcal{W}$ is as in 4.9).

Lemma 4.12 *If $n \geq 3$ and $|C_G(x)| < 3^{3n-8}$ then $|E_2(x)| < 1/2$.*

Proof Now $E_2(x)$ is a sum over at most $k(G)$ characters, each of which, by Lemma 4.9, has degree at least $(3^n - 1)(3^n - 3)/8$. Moreover $k(G) \leq 12 \cdot 3^n$ by Proposition 2.7(iii). Hence Lemma 2.6 yields

$$|E_2(x)| < \frac{8\sqrt{12} \cdot 3^{n/2}|C_G(x)|^{1/2}}{(3^n - 1)(3^n - 3)}.$$

This is less than $1/2$ when $|C_G(x)| < \frac{1}{3072}(3^n - 1)^2(3^n - 3)^2/3^n$, which holds if $|C_G(x)| < 3^{3n-8}$. ■

Lemma 4.13 *If $n \geq 4$ and $|C_G(x)| < 3^{3n-8}$ then $|E_1(x)| < 1/2$.*

Proof Suppose $|C_G(x)| < 3^{3n-8}$. Lemma 4.11 implies that $|\chi(x)| \leq 3^{\sqrt{(3n-8)/2}}$ for $\chi \in \mathcal{W}$, so

$$|E_1(x)| < \frac{8 \cdot 3^{\sqrt{(3n-8)/2}}}{3^n - 1},$$

and this is less than $1/2$ if $n \geq 4$. ■

We need the following technical result concerning various elements in symplectic groups of low dimension over $\mathbb{F}_3$. In the statements, J_i denotes an $i \times i$ unipotent Jordan block matrix.

Lemma 4.14 (i) *For even $n \leq 12$, the elements of G with Jordan form $\pm(J_{n-1}^2, J_2)$ are commutators.*

(ii) *For even $n \leq 8$, the elements of G with Jordan form $\pm(J_{n-1}^2, -J_2)$ are commutators.*

(iii) *For $n = 7$, the elements of G with Jordan form $\pm(J_7^2)$ are commutators.*

Proof (i) For $n \leq 8$ we proved this by computational methods, as follows. For each of the two Jordan forms, there are precisely two conjugacy classes of elements in $Sp_{2n}(3)$ having this form, and these can be distinguished using the criterion of Wall [50, p. 36]. We proved the result by explicit computation using MAGMA: for each Jordan form, by random search in the corresponding group $Sp_{2n}(3)$, we constructed explicit commutators having this form until we found two that were not conjugate.

For $n \geq 10$ the group $Sp_{2n}(3)$ is too large to be handled by random search, and a theoretical argument is required. Let $x = \pm(J_{n-1}^2, J_2)$. From [50, p. 36],

$$|C_G(x)| = 3^{2n+1} \cdot |Sp_2(3)| \cdot |O_1(3)| = 3^{2n+1} \cdot 48.$$

Suppose $n = 12$. As in the proof of Lemma 4.13 we have $|E_1(x)| < \frac{1}{2}$. Also, as in the proof of Lemma 4.12,

$$|E_2(x)| < \frac{8\sqrt{12} \cdot 3^6 |C_G(x)|^{1/2}}{(3^{12}-1)(3^{12}-3)} \leq \frac{8\sqrt{12} \cdot 3^6 \cdot 3^{25/2} \cdot \sqrt{48}}{(3^{12}-1)(3^{12}-3)} < \frac{1}{2},$$

and hence x is a commutator.

Now suppose $n = 10$, so that $G = Sp_{20}(3)$. For this case we need a rather more detailed argument using Lemma 4.10. First, $|C_G(x)| = 3^{21} \cdot 48 < 3^{25}$, so as in Lemma 4.13,

$$|E_1(x)| < \frac{8 \cdot 3^{\sqrt{25/2}}}{3^{10} - 1} < 0.011. \tag{11}$$

Next, by Lemma 4.10, $Irr(G) = \{1\} \cup \mathcal{W} \cup \mathcal{X} \cup \mathcal{Y}$, where $\mathcal{X}$ consists of 4 characters of degree at least $3(3^9-1)(3^{10}-1)/8 = 435818526$, and the characters in $\mathcal{Y}$ have degree at least $3^{19}/2$. Moreover $k(G) = 602929$ and $|C_G(x)| = 3^{21} \cdot 48$. Hence

$$\begin{aligned} E_2(x) &< \tfrac{4|C_G(x)|^{1/2}}{435818526} + \tfrac{2(k(G)\cdot|C_G(x)|)^{1/2}}{3^{19}} \\ &= (3^{21}\cdot 48)^{1/2}(\tfrac{4}{435818526} + \tfrac{2\sqrt{602929}}{3^{19}}) < 0.954. \end{aligned} \tag{12}$$

The conclusion follows from (11) and (12).

(ii) For $n \leq 6$ we prove this computationally by random search as in part (i), so assume $n = 8$. Let $x = \pm(J_7^2, -J_2) \in G$. By [50, p. 36],

$$|C_G(x)| = |C_{Sp_{14}(3)}(J_7^2)| \cdot |C_{Sp_2(3)}(J_2)| = 3^{14} \cdot 16.$$

As usual $|E_1(x)|$ is small, and

$$|E_2(x)| < \frac{8\sqrt{12}\cdot 3^4 |C_G(x)|^{1/2}}{(3^8-1)(3^8-3)} < \frac{1}{2},$$

giving the conclusion.

(iii) Let $G = Sp_{14}(3)$. As in the proof of Lemma 4.10(ii) we see that $k(G) = 19952$. Let $x = \pm(J_7^2) \in G$. By [50, p. 36], $|C_G(x)| = 3^{12} \cdot |Sp_2(3)| < 3^{15}$, so

$$|E_2(x)| < \frac{8(k(G)|C_G(x)|)^{1/2}}{(3^7-1)(3^7-3)} < 0.85.$$

Also, as in the proof of Lemma 4.13,

$$|E_1(x)| < \frac{8\cdot 3^{\sqrt{15/2}}}{3^7-1} < 0.1.$$

The result follows. ∎

Now we consider unbreakable elements of G (defined in Section 2.4).

Lemma 4.15 *Assume $n \geq 3$. Let $x \in Sp(V) = Sp_{2n}(3)$, and suppose one of the following holds:*

(i) *x fixes a non-degenerate subspace W of V with $4 \leq \dim W \leq n$;*

(ii) *$C_V(\epsilon x)$ contains a nonzero non-degenerate subspace for $\epsilon \in \{+,-\}$.*

Then x is breakable.

Proof If (i) holds this is clear. In case (ii), let W be a non-degenerate 2-space in $C_V(\epsilon x)$. Then $x = (\pm 1_W, x_2) \in Sp(W) \times Sp(W^\perp)$. Since -1_W is a commutator in $Sp(W) \cong Sp_2(3)$, and $Sp(W^\perp)$ is perfect as $\dim W^\perp \geq 4$, x is breakable. ∎

Lemma 4.16 *Let $G = Sp(V) = Sp_{2n}(3)$ with $n \geq 6$, and let x be an unbreakable element of G. One of the following holds:*

(i) $|C_G(x)| < 3^{3n-8}$;

(ii) *x is a commutator in G.*

Proof The proof is similar to that of Lemma 4.7. Assume first that x or $-x$ is unipotent, with Jordan form $(J_i^{m_i})$. Since x is unbreakable, and an even block J_{2i} fixes a non-degenerate subspace, the possibilities for this Jordan form are

$$J_{2n},\ (J_{2n-2}, J_2),\ (J_n^2)\ (n \text{ odd}),\ (J_{n-1}^2, J_2)\ (n \text{ even}).$$

We summarise the order of $C_G(x)$ given in [50, p. 36]:

$\pm x$	$\lvert C_G(x)\rvert$
J_{2n}	$3^n \cdot 2$
(J_{2n-2}, J_2)	$3^{n+2} \cdot 4$
(J_n^2)	$3^{2n-2} \cdot 24$
(J_{n-1}^2, J_2)	$3^{2n+1} \cdot 48$

For the first two cases, $|C_G(x)| < 3^{3n-8}$ (recall that $n \geq 6$ by hypothesis), giving (i). In the third case, (i) holds if $n \geq 9$; since n is odd, we may assume that $n = 7$. Then x is a commutator by Lemma 4.14(iii), so (ii) holds. Finally, in the last case $\pm x = (J_{n-1}^2, J_2)$ (n even), (i) holds if $n \geq 13$, so we may take $n \leq 12$, and x is a commutator by Lemma 4.14(i). This proves the result when $\pm x$ is unipotent.

Now assume that $\pm x$ is not unipotent. Then $x = su$, where s, u are the semisimple and unipotent parts, and $s \neq \pm 1$. We have

$$C_G(s) = Sp_{2a}(3) \times Sp_{2b}(3) \times \prod GL_{c_i}^{\epsilon_i}(3^{d_i}),$$

where $2a, 2b$ are the dimensions of the 1- and -1-eigenspaces of s, and $a + b + \sum c_i d_i = n$. As x fixes all the eigenspaces of s and is unbreakable, one of the following must hold:

(1) $2a$ or $2b$ is equal to $2n - 2$;

(2) $2c_i d_i \geq 2n - 2$ for some i.

In case (1), $C_G(s) = Sp_{2n-2}(3) \times Sp_2(3)$. Write $u = u_1 u_2$, where u_1, u_2 are the projections of u into the factors of $C_G(s)$. As x is unbreakable, we must have $u_2 = J_2$ and $u_1 = J_{2n-2}$ or (J_{n-1}^2) (n even). When $u_2 = J_{2n-2}$, we have $|C_G(x)| = 3^n \cdot 4$, so conclusion (i) holds. When $u_2 = (J_{n-1})^2$, we have $|C_G(x)| = 3^{2n-2} \cdot 48$. Hence (i) holds if $n > 8$, and if $n \leq 8$ then (ii) holds, by Lemma 4.14(ii).

In case (2), either $C_G(s) = GL_c^\epsilon(3^d)$ with $cd = n$, $d \geq 2$, or $C_G(s) = Sp_2(3) \times GL_c^\epsilon(3^d)$ with $cd = n - 1$, $d \geq 2$. Since each Jordan block J_k of

u in the $GL_c^\epsilon(3^d)$ factor corresponds to a non-degenerate $2kd$-space fixed by x, the projection of u in this factor must be a single Jordan block J_c. Hence when $cd = n$ we have $|C_G(x)| = 3^{d(c-1)}(3^d - \epsilon)$, so (i) holds. When $cd = n - 1$ we have $|C_G(x)| = 6 \cdot 3^{d(c-1)}(3^d - \epsilon)$, and again (i) holds. ∎

Lemma 4.17 *For $n \geq 2$, every unbreakable element of $Sp_{2n}(3)$ is a commutator.*

Proof Let $G = Sp(V) = Sp_{2n}(3)$ with $n \geq 2$, and let $x \in G$ be unbreakable. If $n \leq 5$ then x is a commutator by Corollary 3.2. If $n \geq 6$, then we may assume that $|C_G(x)| < 3^{3n-8}$ by Lemma 4.16, and hence x is a commutator by Lemmas 4.12 and 4.13. ∎

Lemmas 4.17 and 2.9 imply that every element of G is a commutator, completing the proof of Theorem 4.1 for $q = 3$.

5 Orthogonal groups

In this section we prove the following result, which implies Ore's conjecture for the orthogonal groups.

Theorem 5.1 *Let G be one of the orthogonal groups $\Omega_{2n+1}(q)$ ($n \geq 1$, q odd) or $\Omega^\pm_{2n}(q)$ ($n \geq 2$), excluding the groups $\Omega_3(3), \Omega_4^+(2), \Omega_4^+(3)$. Then every element of G is a commutator.*

Lemma 2.4 implies that we may assume that $q < 7$, and that $q < 5$ if $G = \Omega^+_{2n}(q)$. Further, by Lemma 3.1(iv), writing $G = \Omega(V)$, we may assume that $\dim V \geq 14$ if $q = 2$, $\dim V \geq 12$ if $q = 3$, and $\dim V \geq 10$ if $q = 4, 5$.

Our proof of Theorem 5.1 follows the same conceptual lines as the proof for symplectic groups, but requires a great deal more effort. In particular, we first prove some new character theoretic results for orthogonal groups in Section 5.1. We next establish some centralizer bounds in Section 5.2, and finally prove the theorem in Section 5.3.

5.1 Character theory of orthogonal groups

The main results of this section are Corollary 5.8 and Propositions 5.12 and 5.14, which identify values of irreducible characters of small degree for orthogonal groups. Their proof requires some substantial results and methods in the character theory of orthogonal groups, in particular the use of dual pairs and Weil characters in Proposition 5.7.

First we collect some results from [38] on complex irreducible characters of relatively small degrees for orthogonal groups.

Proposition 5.2 ([38]) *Let $G := Spin_{2n+1}(q)$ with $n \geq 5$ and q an odd prime power. Assume $\chi \in \mathrm{Irr}(G)$ and $1 < \chi(1) \leq q^{4n-8}$. Then χ is one of $q+4$ characters, of the following degrees:*

(i) $(q^{2n}-1)/(q^2-1)$ *(1 character),*

(ii) $q(q^{2n}-1)/(q^2-1)$ *(1 character),*

(iii) $(q^n+\alpha_1)(q^n+\alpha_2 q)/2(q+\alpha_1\alpha_2)$ *(4 characters, where each of α_1, α_2 is ± 1),*

(iv) $(q^{2n}-1)/(q-\alpha)$ *($q-2$ characters in total: $(q-\alpha-2)/2$ characters for $\alpha = \pm 1$).*

Proposition 5.3 ([38]) *Let $G := Spin^{\epsilon}_{2n}(q)$ with $n \geq 5$ and q an odd prime power, and let $\chi \in \mathrm{Irr}(G)$.*

(A) *Assume that $n \geq 6$ and $1 < \chi(1) \leq q^{4n-10}$. Then χ is one of $q+4$ characters, of the following degrees:*

(i) $(q^n-\epsilon)(q^{n-1}+\epsilon q)/(q^2-1)$ *(1 character),*

(ii) $(q^{2n}-q^2)/(q^2-1)$ *(1 character),*

(iii) $(q^n-\epsilon)(q^{n-1}+\epsilon\alpha)/2(q-\alpha)$ *(4 characters, two for each $\alpha = \pm 1$),*

(iv) $(q^n-\epsilon)(q^{n-1}+\epsilon\alpha)/(q-\alpha)$ *($q-2$ characters in total: $(q-\alpha-2)/2$ characters for $\alpha = \pm 1$).*

Further, $Spin^{\epsilon}_{12}(3)$ has at most 22 irreducible characters of degree at most $4 \cdot 3^{15}$.

(B) *Assume that $n = 5$, and $1 < \chi(1) \leq q^{10}$ if $\epsilon = +$, and $1 < \chi(1) < (q-1)(q^2+1)(q^3-1)(q^4+1)$ if $\epsilon = -$. Then χ is one of the $q+4$ characters listed in* (A)(i)–(iv).

Proposition 5.4 ([38]) *Let $G := \Omega^{\epsilon}_{2n}(q)$ with $n \geq 5$ and q an even prime power. Assume $\chi \in \mathrm{Irr}(G)$ and $1 < \chi(1) \leq q^{4n-10}$.*

(A) *If $n \geq 6$, then χ is one of $q+1$ characters, of the following degrees:*

(i) $(q^n-\epsilon)(q^{n-1}+\epsilon q)/(q^2-1)$ *(1 character),*

(ii) $(q^{2n}-q^2)/(q^2-1)$ *(1 character),*

(iii) $(q^n-\epsilon)(q^{n-1}+\epsilon\alpha)/(q-\alpha)$ *($q-1$ characters in total: $(q-\alpha-1)/2$ characters for $\alpha = \pm 1$).*

(B) *Assume $n = 5$ and $\epsilon = +$. If $q \geq 4$, then χ is one of $q+1$ characters listed in* (A)(i) – (iii). *If $q = 2$, then there is one more character of degree* 868.

(C) *Assume $n = 5$ and $\epsilon = -$. Then χ is one of $2q+2$ characters: $q+1$ characters listed in* (A)(i) – (iii), *and $q+1$ characters of the following degrees:*

(iv) $q^2(q^4+1)(q^5+1)/(q+1)$ *(1 character),*

(v) $(q-1)(q^2+1)(q^3-1)(q^4+1)$ *(q characters).*

Next we study some dual pairs to find the explicit values of small characters of finite orthogonal groups over fields of odd characteristic. Our consideration is based on the following well known formula.

Lemma 5.5 *Let ω be a character of the direct product $S \times G$ of finite groups S and G. For $s \in S$ and $g \in G$,*

$$\omega(sg) = \sum_{\alpha \in \ \mathrm{Irr}(S)} \alpha(s) \cdot D_\alpha(g),$$

where

$$D_\alpha(g) = \frac{1}{|S|} \sum_{x \in S} \overline{\alpha(x)} \omega(xg).$$

Proof By the orthogonality relations, $\sum_{\alpha \in \ \mathrm{Irr}(S)} \alpha(s)\overline{\alpha(x)}$ is equal to 0 if $x \notin s^S$ and $|S|/|s^S|$ otherwise. Hence

$$\sum_{\alpha \in \ \mathrm{Irr}(S)} \alpha(s) \cdot D_\alpha(g) = \frac{1}{|S|} \sum_{x \in S} \omega(xg) \left(\sum_{\alpha \in \ \mathrm{Irr}(S)} \alpha(s)\overline{\alpha(x)} \right) = \omega(sg).$$

■

Let q be an odd prime power. The dual pair we have in mind is $S \times G$ inside $\Gamma := Sp_{2n}(q)$, where $S = Sp_2(q)$ and $G \in \{\Omega_n(q), SO_n(q), GO_n(q)\}$, and ω_n is one of the two *reducible* Weil characters of $Sp_{2n}(q)$, of degree q^n (see [48]). More precisely, we view S as $Sp(U)$, where $U = \langle e, f \rangle_{\mathbb{F}_q}$ is endowed with the symplectic form $(\cdot,\cdot)$, and Gram matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in the basis $\{e, f\}$. Fix $\gamma \in \mathbb{F}_q^\times$. Next, $GO_n(q)$ means $GO(W)$, where $W = \langle v_1, \dots, v_n \rangle_{\mathbb{F}_q}$ is endowed with the orthogonal form $(\cdot,\cdot)$, and Gram matrix $\mathrm{diag}(1, 1, \dots, 1, \gamma)$ in the basis $\{v_1, \dots, v_n\}$. Now we consider $V = U \otimes W$ with the symplectic form $(\cdot,\cdot)$ defined via $(u \otimes w, u' \otimes w') = (u, u') \cdot (w, w')$ for $u \in U$ and $w \in W$, which has Gram matrix $\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ in the basis

$$\left\{ e \otimes v_1, e \otimes v_2, \dots, e \otimes v_n, f \otimes v_1, f \otimes v_2, \dots, f \otimes v_{n-1}, f \otimes \gamma^{-1} v_n \right\}.$$

The action of $S \times G$ on V induces a homomorphism $S \times G \to \Gamma := Sp(V)$.

Lemma 5.6 *Under the above assumptions, assume that $n \geq 6$. Then*

$$(\omega_n|_G, \omega_n|_G)_G = (q+1)(q^2+1).$$

Further, $(\omega_n|_G, 1_G)_G = q+1$ if $G = \Omega_n(q)$ or $SO_n(q)$.

Proof Let A be the matrix of $g \in G$ in the basis $\{v_1, \ldots, v_n\}$ of W. Then g has matrix $\mathrm{diag}\left(A, (A^T)^{-1}\right)$ in the basis of V listed above. In particular, G embeds in the Levi subgroup $GL_n(q)$ of the parabolic subgroup

$$Stab_\Gamma\left(\langle e \otimes v_1, e \otimes v_2, \ldots, e \otimes v_n\rangle_{\mathbb{F}_q}\right)$$

of Γ. Let ν denote the unique nontrivial character of order 2 of $\mathbb{F}_q^\times$. By [20, Theorem 3.3], the restriction of ω_n to $GL_n(q)$ is $h \mapsto \tau(h) \cdot \nu(h)$, where

$$\tau(h) := q^{\dim_{\mathbb{F}_q} \mathrm{Ker}(h-1)},$$

and we take the fixed point subspace of h on the natural module $\mathbb{F}_q^n$ of $GL_n(q)$. It follows that for any $g \in G$,

$$|\omega_n^2(g)| = q^{2\dim_{\mathbb{F}_q} \mathrm{Ker}(g-1)},$$

where we take the fixed point subspace of g on W. In other words, $|\omega_n^2(g)|$ is just the number of g-fixed points on the set $W \times W$. Hence $(\omega_n|_G, \omega_n|_G)_G$ equals the number of G-orbits on $W \times W$. Using Witt's theorem and the assumption $n \geq 6$, one can show that G has exactly $(q+1)(q^2+1)$ orbits on $W \times W$, with the following representatives: $(0,0)$, $(v, \lambda v)$ where $\lambda \in \mathbb{F}_q$, $0 \neq v \in V$ and $(v,v) = \mu \in \mathbb{F}_q$, $(0, v)$ where $0 \neq v \in V$ and $(v,v) = \mu \in \mathbb{F}_q$, and (u, v) where $u, v \in V$ are linearly independent and $(\cdot, \cdot)$ has Gram matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ with $a, b, c \in \mathbb{F}_q$. Similarly, if $G \leq SO_n(q)$, then $(\omega_n|_G, 1_G)_G$ is just the number of G-orbits on W, which is $q+1$. ■

Remark The first statement of Lemma 5.6 also holds for $G = GO_5(q)$ or $SO_5(q)$. However, the number of G-orbits on W, and so $(\omega_5|_G, \omega_5|_G)_G$, equals $(q+1)(q^2+1)+1$, since G has two orbits on the pairs (u, v) such that $\langle u, v\rangle_{\mathbb{F}_q}$ is a totally singular 2-space. This explains the fact that an $SO_5(q)$-irreducible constituent of degree q^2+1 of ω_5 splits into two $\Omega_5(q)$-irreducible constituents of degree $(q^2+1)/2$.

Proposition 5.7 *Assume that $G = \Omega_n^\epsilon(q)$ and $S = Sp_2(q)$, where $n \geq 6$ and q is an odd prime power.*

The restriction $\omega_n|_{S \times G}$ of a reducible Weil character of degree q^n of $Sp_{2n}(q)$ decomposes as $\sum_{\alpha \in \mathrm{Irr}(S)} \alpha \otimes D_\alpha$, where $k_\alpha \in \{0, 1\}$, and the characters $D_\alpha^\circ := D_\alpha - k_\alpha \cdot 1_G$ are all irreducible and distinct.

Further, $k_\alpha = 1$ if and only if one of the following holds:

(i) *n is odd, and α is one of the two irreducible Weil characters of degree $(q+1)/2$ of S;*

(ii) *n is even, and α is either the trivial character, or the Steinberg character (of degree q) of S.*

Moreover, each D_α° extends to $GO_n(q)$.

Proof We present the proof in various steps.

1) Apply Lemma 5.5 to the character $\omega = \omega_n$, and define $l_\alpha := (D_\alpha, 1_G)_G$ and $D^\circ_\alpha := D_\alpha - l_\alpha \cdot 1_G$. By Lemma 5.6, $\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) l_\alpha = q+1$,

$$\omega_n|_G = (q+1) \cdot 1_G + \sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) D^\circ_\alpha,$$

and $(D^\circ_\alpha, 1_G)_G = 0$ for all α. Again by Lemma 5.6,

$$\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1)^2 = |S| = q(q^2-1) = \left(\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) D^\circ_\alpha, \sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) D^\circ_\alpha \right)_G .$$

It follows that all D°_α, $\alpha \in \mathrm{Irr}(S)$, must be irreducible and distinct, if all of them have positive degrees. Set $\delta := (-1)^{(q-1)/2}$.

2) We consider the case where n is odd, or n is even and $\epsilon = \delta^{n/2}$. In the above construction we can choose $\gamma = 1$ (or any square in $\mathbb{F}_q^\times$). If $s \in S$ is represented by the matrix B in the basis $\{e, f\}$ of U, then it has matrix $\mathrm{diag}(B, B, \ldots, B)$ in the basis

$$\{e \otimes v_1, f \otimes v_1, e \otimes v_2, f \otimes v_2, \ldots, e \otimes v_n, f \otimes v_n\}$$

of V, and in fact V is the orthogonal sum of the n non-degenerate 2-spaces $\langle e \otimes v_i, f \otimes v_i \rangle_{\mathbb{F}_q}$, $i = 1, \ldots, n$. Thus S acts on V via the embeddings

$$Sp_2(q) \hookrightarrow Sp_2(q) \times Sp_2(q) \ldots \times Sp_2(q) \hookrightarrow Sp_{2n}(q),$$

where the first embedding is the diagonal embedding. It follows by [48] that $\omega_n|_S = (\omega_1)^n$. The character table of S is well known, see e.g. [11, p. 228]. We use the same labelling for the irreducible characters: 1_S, St (of degree q), χ_i (of degree $q+1$), θ_j (of degree $q-1$), Weil characters ξ_1 and ξ_2 (of degree $(q+1)/2$), and Weil characters η_1 and η_2 (of degree $(q-1)/2$), where $\omega_1 = \xi_1 + \eta_1$ (a total of $q+4$ characters in all). It is straightforward to compute $D_\alpha(1) = (\omega_n|_S, \alpha)_S$. In particular, $D_\alpha(1) > q+1$ and so $D^\circ_\alpha(1) > 0$ for all $\alpha \in \mathrm{Irr}(S)$. Hence the D°_α are all irreducible and distinct. It remains to prove that $l_\alpha = k_\alpha$, where the integers k_α are defined in the statement.

The degrees of D_α and the integers k_α are listed in Table I for $n = 2m+1$, and in Table II for $n = 2m$. Observe that $|D_\alpha(1) - D_\beta(1)| \geq q+1$ if α and β belong to different rows of the Tables. Also, notice that $\omega_n|_G$ contains the rank 3 permutation character of $G = \Omega^\epsilon_n(q)$ (on singular 1-spaces of W). The degrees of the irreducible constituents of the latter are well known (see e.g. [42]). It follows in particular that, when $n = 2m+1$, some D°_α have degrees $D_{\xi_i}(1) - 1$ for each $i = 1, 2$. Thus $|D_\alpha(1) - D_{\xi_i}(1)| = |l_\alpha - 1| \leq q$ and so $\alpha = \xi_i$. We have shown that $l_{\xi_1} = l_{\xi_2} = 1$. Since $l_\beta \geq 0$ for all β and $\sum_\beta \beta(1) l_\beta = q+1$, we must have $l_\beta = 0$ for all $\beta \neq \xi_1, \xi_2$.

Next we assume that $n = 2m$. Then some D°_α have degrees $D_\xi(1) - 1$ for each $\xi \in \{1_S, St\}$. Thus $|D_\alpha(1) - D_\xi(1)| = |l_\alpha - 1| \leq q$ and so $\alpha = \xi$. We have shown that $l_{1_S} = l_{St} = 1$. Since $l_\beta \geq 0$ for all β and $\sum_\beta \beta(1) l_\beta = q+1$, we must have $l_\beta = 0$ for all $\beta \neq 1_S, St$.

TABLE I. Degrees of D_α, $n = 2m+1$

α	$\alpha(1)$	$D_\alpha(1)$	k_α
1_S	1	$(q^{2m}-1)/(q^2-1)$	0
St	q	$(q^{2m+1}-q)/(q^2-1)$	0
χ_i	$q+1$	$(q^{2m}-1)/(q-1)$	0
θ_j	$q-1$	$(q^{2m}-1)/(q+1)$	0
ξ_1	$(q+1)/2$	$(q^m-\delta^{m+1})(q^m+\delta^{m+1}q)/2(q-1) \ +1$	1
ξ_2	$(q+1)/2$	$(q^m+\delta^{m+1})(q^m-\delta^{m+1}q)/2(q-1) \ +1$	1
η_1	$(q-1)/2$	$(q^m+\delta^{m+1})(q^m+\delta^{m+1}q)/2(q+1)$	0
η_2	$(q-1)/2$	$(q^m-\delta^{m+1})(q^m-\delta^{m+1}q)/2(q+1)$	0

TABLE II. Degrees of D_α, $n = 2m$

α	$\alpha(1)$	$D_\alpha(1)$	k_α
1_S	1	$(q^m-\epsilon)(q^{m-1}+\epsilon q)/(q^2-1) \ +1$	1
St	q	$(q^{2m}-q^2)/(q^2-1) \ +1$	1
χ_i	$q+1$	$(q^m-\epsilon)(q^{m-1}+\epsilon)/(q-1)$	0
θ_j	$q-1$	$(q^m-\epsilon)(q^{m-1}-\epsilon)/(q+1)$	0
ξ_1, ξ_2	$(q+1)/2$	$(q^m-\epsilon)(q^{m-1}+\epsilon)/2(q-1)$	0
η_1, η_2	$(q-1)/2$	$(q^m-\epsilon)(q^{m-1}-\epsilon)/2(q+1)$	0

3) Next we consider the case where n is even but $\epsilon = -\delta^{n/2}$. In the above construction we can choose γ to be any non-square in $\mathbb{F}_q^\times$. If $s \in S$ is represented by the matrix B in the basis (e, f) of U, then it has matrix $\mathrm{diag}(B, B, \ldots, B, CBC^{-1})$ in the basis

$$\left\{e \otimes v_1, f \otimes v_1, e \otimes v_2, f \otimes v_2, \ldots, e \otimes v_{n-1}, f \otimes v_{n-1}, e \otimes v_n, \gamma^{-1} f \otimes v_n\right\}$$

of V, where $C = \mathrm{diag}(1, \gamma)$ and so it induces a non-inner diagonal automorphism of S which interchanges ξ_1 and ξ_2, and also η_1 and η_2. Also, V is the orthogonal sum of the n non-degenerate 2-spaces $\langle e \otimes v_i, f \otimes v_i \rangle_{\mathbb{F}_q}$ $(i = 1, \ldots, n-1)$, and $\langle e \otimes v_n, \gamma^{-1} f \otimes v_n \rangle_{\mathbb{F}_q}$. Thus S acts on V via the embeddings

$$Sp_2(q) \hookrightarrow Sp_2(q) \times Sp_2(q) \ldots \times Sp_2(q) \hookrightarrow Sp_{2n}(q),$$

where the first embedding is the diagonal embedding composed with a non-inner diagonal automorphism on the last $Sp_2(q)$ factor. It follows by [48] that

$\omega_n|_S = (\xi_1+\eta_1)^{n-1}(\xi_2+\eta_2)$. Direct computations yield $D_\alpha(1) = (\omega_n|_S, \alpha)_S$ as listed in Table II. In particular, $D_\alpha(1) > q+1$ and so $D^\circ_\alpha(1) > 0$ for all $\alpha \in \mathrm{Irr}(S)$. Hence D°_α are all irreducible and distinct. Arguing as in 2), we obtain $l_\alpha = k_\alpha$.

4) Finally, the extendibility of D°_α to $GO_n(q)$ follows from the fact that $(\omega_n|_G, \omega_n|_G)_G$ are the same for both $G = \Omega_n(q)$ and $G = GO_n(q)$. ■

Note that $|\mathrm{Irr}(S)| = q+4$ (see [11, p. 228]). Propositions 5.2, 5.3, and 5.7 immediately imply:

Corollary 5.8 *Let $G = Spin^\epsilon_n(q)$, where $n \geq 11$ and q is an odd prime power. Assume $\chi \in \mathrm{Irr}(G)$ with $1 < \chi(1) \leq q^{2n-10}$. Then χ is one of the $q+4$ characters D°_α listed in Theorem 5.7.*

To estimate the character values for D°_α, we need the following well known fact (see [24, Lemma 2.4]).

Lemma 5.9 *Let ω_n be a reducible Weil character of $\Gamma := Sp_{2n}(q)$. For $g \in \Gamma$, let $d(g)$ denote the dimension of the g-fixed point subspace on the natural module $V = \mathbb{F}_q^{2n}$ of Γ. Then $|\omega_n(g)| \leq q^{d(g)/2}$.*

Next we consider the dual pair $S \times G$ inside Γ and estimate $D_\alpha(g)$ for an unbreakable $g \in G$.

Lemma 5.10 *Let $G := \Omega^\epsilon_n(q)$ with natural module $W = \mathbb{F}_q^n$ and q an odd prime power. Assume $n \geq 10$ if $q \geq 5$ and $n \geq 12$ if $q = 3$. For $g \in G$ and $\lambda \in \overline{\mathbb{F}}_q^\times$, let $e(g,\lambda)$ denote the dimension of the eigenspace of g on $W \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ corresponding to λ. If g is unbreakable, then $e(g,\lambda) \leq n/2$ if $\lambda \neq -1$ and $e(g,-1) \leq n-3$.*

Proof 1) If λ is an eigenvalue for g then so is λ^{-1}, and moreover $e(g,\lambda) = e(g,\lambda^{-1})$. Hence the statement is obvious if $\lambda \neq \pm 1$.

Next, let W_λ denote the eigenspace for g on W corresponding to λ; in particular, $e(g,\lambda) = \dim W_\lambda$ if $\lambda \in \mathbb{F}_q^\times$. Assume $e(g,1) > n/2$. Then the subspace W_1 cannot be totally singular, whence it contains a vector v with $(v,v) \neq 0$. Thus $g \in Stab_G(v) = 1_{\langle v\rangle} \times \Omega(\langle v\rangle^\perp) \simeq \Omega_{n-1}(q)$ and so g is breakable, a contradiction. In general, the unbreakability of g implies that g cannot fix any nonsingular vector $v \in W$.

2) Now we assume that $e(g,-1) \geq n-2$. First we consider the case $e(g,-1) = n$, i.e. $g = -1_W$; in particular, $2|n$ and $\epsilon = (-1)^{n(q-1)/4}$. We claim that g is breakable in this situation. Indeed, if $q \geq 5$, then $g \in \Omega^+_4(q) \times \Omega^\epsilon_{n-4}(q)$ and hence g is breakable. If $q = 3$, then $g \in \Omega^-_6(q) \times \Omega^{-\epsilon}_{n-6}(q)$ and so g is breakable.

Thus we may assume $g \neq -1_W$. Let s be the semisimple part of g. Then $e(s,-1) \geq e(g,-1) \geq n-2$ and so $e(s,1) \leq 2$. Let W_+, resp. W_-, denote the eigenspace of s on W corresponding to the eigenvalue 1, resp. -1; in particular, $W_+ \supseteq W_1$ and $W_- \supseteq W_{-1}$. Assume $e(s,1) = 1$. Then $W_+ = \langle v \rangle_{\mathbb{F}_q}$ and v is nonsingular. Clearly, g fixes v and so g is breakable as in 1). Assume $e(s,1) = 2$. Then $\dim W_+ = 2$ and so $W = W_+ \oplus W_-$. In particular, W_+ is non-degenerate and is stabilized by g. In fact, g acts on W_+ as a unipotent transformation. If this action is trivial, then g fixes some nonsingular vector of W_+ and so it is breakable. If this action is nontrivial, then $g(u) = u$ and $g(v) = u + v$ for some basis $\{u, v\}$ of W_+. In this case, $(u,u) = (u,v) = 0$, i.e. W_+ is degenerate, a contradiction.

We have shown that $e(s,1) = 0$. Notice that the eigenvalues other than ± 1 of s come in pairs, so either $W = W_- \oplus A$, where $\dim A = 2$ and s has no eigenvalue ± 1 on $A \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$, or $s = -1_W$. Consider the former case. Then W_- has dimension $n - 2 \geq 8$ and is non-degenerate; also $g|_{W_-} = -1_{W_-}$. Hence, we can find a 6-dimensional non-degenerate subspace B of type $\delta = (-1)^{6(q-1)/4} = (-1)^{(q-1)/2}$, inside W_- and fixed by g; in fact, $g|_B = -1_B \in \Omega(B)$. Now

$$g \in \Omega(B) \times \Omega(B^\perp) \simeq \Omega_6^\delta(q) \times \Omega_{n-6}^{\epsilon\delta}(q)$$

is breakable, since $n - 6 \geq 4$ if $q \geq 5$ and $n - 6 \geq 6$ if $q = 3$.

Finally, we consider the case $s = -1_W$, i.e. -1 is the only eigenvalue of g. Observe that n is even, as $g \in SO(W)$. Since $n - 1 \geq e(g,-1) \geq n - 2$, we have the orthogonal decomposition $W = C \oplus D$, where $g|_C = -1_C$, and $-g$ acts on D as a unipotent transformation with matrix J_3, J_2^2, or J_2. In any case, $\dim(C) \geq n - 4$. Now if $q \geq 5$, then $\dim(C) \geq 6$, and we can find a 4-dimensional non-degenerate subspace B of type $+$, inside C and fixed by g; in fact, $g|_B = -1_B \in \Omega(B)$ and it is a commutator in B. It follows that

$$g \in \Omega(B) \times \Omega(B^\perp) \simeq \Omega_4^+(q) \times \Omega_{n-4}^\epsilon(q)$$

and so g is breakable. If $q = 3$, then $\dim(C) \geq 8$, and we can find a 6-dimensional non-degenerate subspace B of type $-$, inside C and fixed by g; in fact, $g|_B = -1_B \in \Omega(B)$. In this case,

$$g \in \Omega(B) \times \Omega(B^\perp) \simeq \Omega_6^-(q) \times \Omega_{n-6}^{-\epsilon}(q)$$

and so g is breakable. ■

Proposition 5.11 *Consider the dual pair $S \times G$ inside $\Gamma := Sp_{2n}(q)$ (q odd), where $S = Sp_2(q)$ and $G = \Omega_n^\epsilon(q)$. Assume $n \geq 10$ if $q \geq 5$ and $n \geq 12$ if $q = 3$. For any unbreakable $g \in G$ and any $\alpha \in \mathrm{Irr}(S)$,*

$$|D_\alpha(g)| \leq \frac{\alpha(1)}{q(q^2-1)} \cdot \left\{ \left(q(q^2-1) - 1\right) q^{n/2} + q^{n-3} \right\}.$$

If $q = 3$, then $|D_\alpha(g)| < 4q^{n-5}\alpha(1)/(q^2-1) - 1$.

Proof We apply Lemma 5.5 to this dual pair and obtain $D_\alpha(g) = \sum_{x\in S}\overline{\alpha(x)}\omega(xg)/|S|$, where $\omega = \omega_n$. Next we use Lemmas 5.9 and 5.10 to estimate $\omega(xg)$.

1) If $x = 1_U$, then $d(xg) = 2e(g,1) \le n$. If x is conjugate (in $Sp_2(\overline{\mathbb{F}}_q)$) to $\mathrm{diag}(\lambda,\lambda^{-1})$ for some $\pm 1 \ne \lambda \in \overline{\mathbb{F}}_q^\times$, then $d(xg) \le e(g,\lambda) + e(g,\lambda^{-1}) \le n$. Next assume that x is conjugate in S to $a\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix}$ for some $a = \pm 1$ and $b \in \mathbb{F}_q^\times$. Direct computation shows that $|\mathrm{Ker}(xg - 1_V)|$ equals the number of pairs $(u,v) \in W^2$, where $W = \mathbb{F}_q^n$ is the natural module for G, $v \in \mathrm{Ker}(g - a\cdot 1_W) \cap \mathrm{Im}(g - a\cdot 1_W)$, and $(g - a\cdot 1_W)u = abv$, which is at most $|\mathrm{Im}(g - a\cdot 1_W)|\cdot|\mathrm{Ker}(g - a\cdot 1_W)| = |W| = q^n$. Hence $d(xg) \le n$ in this case as well. Finally, if $x = -1_U$, then $d(xg) = 2e(g,-1) \le 2(n-3)$, and the first claim of the proposition follows since $|\alpha(x)| \le \alpha(1)$.

2) Now consider the case $q = 3$; in particular, $n \ge 12$. Recall that $e(g,-1) \le n-3$ by Lemma 5.10. Also, the calculations in 1) show that $d(xg) \le n$ if $x \ne -1_U$. Hence, if $e(g,-1) \le n-4$, then

$$|D_\alpha(g)| \le \left(q^{n-4} + 23q^{n/2}\right)\alpha(1)/q(q^2-1) < 4q^{n-5}\alpha(1)/(q^2-1) - 1.$$

Assume $e(g,-1) = n-3$. For any $\lambda \ne -1$, $e(g,\lambda) \le 3$. It follows that $d(xg) \le 6$ if $x = 1_U$ (one element), or if $x \in S$ has order 4 (6 elements). If x is one of the 8 elements of order 3, then the calculations in 1) show that $|\mathrm{Ker}(xg - 1_V)| \le |\mathrm{Ker}(g - 1_W)|^2 \le q^6$ and so $d(xg) \le 6$ again. Thus

$$\begin{aligned} |D_\alpha(g)| &\le \left(q^{n-3} + 8q^{n/2} + (1+6+8)q^3\right)\alpha(1)/q(q^2-1) \\ &< 4q^{n-5}\alpha(1)/(q^2-1) - 1. \end{aligned}$$

■

Proposition 5.12 *Let χ be any irreducible character of $G = \Omega_n^\epsilon(q)$, where q is an odd prime power, $n \ge 10$ if $q \ge 5$ and $n \ge 12$ if $q = 3$. Assume that $1 < \chi(1) \le q^{2n-10}$ if $n > 10$, or χ is one of the characters D_α° listed in Proposition 5.7 if $n = 10$. For unbreakable $g \in G$,*

$$|\chi(g)/\chi(1)| \le \begin{cases} (q+1)/q^3, & \text{if } q \ge 5, \\ 1/20, & \text{if } q = 3. \end{cases}$$

Proof Consider the dual pair $S\times G$ inside $\Gamma := Sp_{2n}(q)$, where $S = Sp_2(q)$. By Corollary 5.8, if $n > 10$ then $\chi = D_\alpha^\circ$ for some $\alpha \in \mathrm{Irr}(S)$. Thus in any case, $\chi = D_\alpha^\circ$ for some α. The degrees of D_α° are given in Theorem 5.7 and Tables I, II. Direct calculations show that

$$\frac{D_\alpha^\circ(1)}{q^{n-1}\alpha(1)/(q^2-1)} > 1 - \frac{1}{q^{m-2}}$$

where $m := \lfloor n/2 \rfloor$. Assume $q \geq 5$. Now $n \geq 10$, whence $n/2 \leq n-5$. Proposition 5.11 implies

$$|D_\alpha^\circ(g)| \leq |D_\alpha(g)| + 1 \leq \frac{\alpha(1)\left(q(q^2-1)q^{n-5} + q^{n-3}\right)}{q(q^2-1)}$$

$$= \frac{q^{n-4}(q+1)\alpha(1)}{q^2-1} \cdot \left(1 - \frac{1}{q^2+q}\right),$$

and so $|D_\alpha^\circ(g)/D_\alpha^\circ(1)| < (q+1)/q^3$.

Next, assume that $q = 3$; in particular $n \geq 12$ and $m \geq 6$. Hence

$$\frac{D_\alpha^\circ(1)}{q^{n-1}\alpha(1)/(q^2-1)} > \frac{80}{81}.$$

On the other hand, by Proposition 5.11,

$$|D_\alpha^\circ(g)| \leq |D_\alpha(g)| + 1 \leq 4q^{n-5}\alpha(1)/(q^2-1),$$

whence $|D_\alpha^\circ(g)/D_\alpha^\circ(1)| < 1/20$. ■

Now we estimate the character values for the three small irreducible characters δ^1, δ^2 and γ of $K := \Omega_{2n}^{\pm}(2)$ ($n \geq 7$) given by Proposition 5.4, where $\delta^1(1) = (2^n - \epsilon)(2^{n-1} + 2\epsilon)/3$, $\delta^2(1) = (2^n - \epsilon)(2^{n-1} - \epsilon)/3$, and $\gamma(1) = (2^{2n}-4)/3$. To do this, we consider the three *unitary-Weil* characters of $H := Sp_{2n}(2)$ as described in [24]: α_n of degree $(2^n-1)(2^{n-1}-1)/3$, β_n of degree $(2^n+1)(2^{n-1}+1)/3$, and ζ_n^1 of degree $(2^{2n}-1)/3$.

Lemma 5.13 *Assume $n \geq 5$ and consider the natural embedding of $K := \Omega_{2n}^{\epsilon}(2)$ in $H := Sp_{2n}(2)$. If $\epsilon = +$, then*

$$\alpha_n|_K = \delta^2, \quad \beta_n|_K = 1_K + \delta^1, \quad \zeta_n^1|_K = 1_K + \gamma.$$

If $\epsilon = -$, then

$$\alpha_n|_K = 1_K + \delta^1, \quad \beta_n|_K = \delta^2, \quad \zeta_n^1|_K = 1_K + \gamma.$$

Proof When $n = 5$ the statements can be verified directly using [8], so we assume $n \geq 6$. Recall that the reducible Weil character ζ_n of $SU_{2n}(q)$ restricts to H as $\alpha_n + \beta_n + 2 \cdot \zeta_n^1$ (see [24, §3]). We consider the permutation character τ_n of H on the point set of the natural module $V = \mathbb{F}_2^{2n}$. By [24, Lemma 5.8], the restrictions of τ_n and ζ_n to K are equal. All the nontrivial irreducible constituents of $\tau_n|_K = \zeta_n|_K$ have degree less than $2^{2n} \leq 2^{4n-10}$ and so they must be among the characters δ^1, δ^2, and γ listed in Proposition 5.4. Notice that $\tau_n|_K - 1_K$ contains the rank 3 permutation character of K on the singular 1-spaces of V. Reading off the degrees of the nontrivial

irreducible constituents of the latter from [42, Table I], we see that they are δ^1 and γ. Further, $(\tau_n|_K, 1_K)_K$ equals the number of K-orbits on V, which is 3. Thus

$$\alpha_n|_K + \beta_n|_K + 2 \cdot \zeta_n^1|_K = \zeta_n|_K = \tau_n|_K$$

contains $3 \cdot 1_K + \delta^1 + \gamma$. But $\gamma(1) = \zeta_n^1(1) - 1 > \beta_n(1) > \alpha_n(1)$. It follows that $\zeta_n^1|_K = 1_K + \gamma$.

First we assume that $\epsilon = +$. Here $\delta^2(1) = \alpha_n(1)$ is the smallest degree of nontrivial irreducible characters of K (see [47]). Hence $\alpha_n|_K = \delta^2$. This forces $\beta_n|_K = 1_K + \delta^1$.

Now we assume that $\epsilon = -$. Clearly, δ^1 must be a constituent of $\alpha_n|_K$ or $\beta_n|_K$. Assume that δ^1 is a constituent of $\beta_n|_K$. Now $\beta_n(1) - \delta^1(1) = 2^n + 1$ is less than the smallest degree of nontrivial irreducible characters of K (see [47]). It follows that $\beta_n|_K - \delta^1 = (2^n + 1) \cdot 1_K$ and so $\tau_n|_K$ contains 1_K with multiplicity at least $2^n + 1$, a contradiction. Thus δ^1 is a constituent of $\alpha_n|_K$. Since $\alpha_n(1) - \delta^1(1) = 1$, we must have $\alpha_n|_K = 1_K + \delta^1$. In this situation, $(\beta_n|_K, 1_K) = 0$ and $\beta_n(1)$ is less than twice the smallest degree of nontrivial irreducible characters of K. Hence $\beta_n|_K$ is irreducible and so $\beta_n|_K = \delta^2$. ■

Proposition 5.14 *Let $K := \Omega_{2n}^{\epsilon}(2)$ with $n \geq 6$. For unbreakable $g \in K$,*

$$\sum_{\chi \in \ \mathrm{Irr}(K),\ 1 < \chi(1) \leq 2^{4n-10}} |\frac{\chi(g)}{\chi(1)}| \leq \frac{7}{2^{n-2}}.$$

Proof Recall that χ is one of the characters δ^1, δ^2, or γ. For any $\lambda \in \overline{\mathbb{F}}_2^{\times}$, let $e(g, \lambda)$ denote the dimension of the eigenspace of g on $V \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$ corresponding to the eigenvalue λ, where $V = \mathbb{F}_2^{2n}$ is the natural module for $H := Sp_{2n}(2) > K$, with an H-invariant symplectic form $(\cdot, \cdot)$. We claim that the unbreakability of g implies that $e(g, 1) \leq n$. Assume instead that $e(g, 1) > n$. Then the fixed point subspace U of g on V has dimension greater than n and so it cannot be totally isotropic. Hence we can find $u, v \in U$ such that $(u, v) \neq 0$. Now $g \in \Omega(\langle u, v \rangle^{\perp}) \simeq \Omega_{2n-2}^{\pm}(2)$ and so g is breakable.

Abusing notation, we use ω to denote a primitive cube root of unity in both $\mathbb{C}$ and $\overline{\mathbb{F}}_2$. By the formulae (4) and (6) of [24],

$$\zeta_n^1(G) = \sum_{i=0}^{2} \omega^i (-2)^{e(g,\omega^i)}/3, \quad \alpha_n(g) + \beta_n(g) = \sum_{i=0}^{2} (-2)^{e(g,\omega^i)}/3.$$

We have shown above that $a := e(g, 1) \leq n$. Also, $e(g, \omega) = e(g, \omega^{-1}) =: b$, hence $b \leq n$. Since $a + 2b \leq 2n$ and $0 \leq a, b \leq n$, it is easy to check that $2^a + 2 \cdot 2^b \leq 2^{n+1} + 1$. Hence

$$|\zeta_n^1(g)| \leq (2^{n+1} + 1)/3, \quad |\alpha_n(g) + \beta_n(g)| \leq (2^{n+1} + 1)/3.$$

By Lemma 5.13,

$$|\gamma(g)| = |\zeta_n^1(g) - 1| \leq |\zeta_n^1(g)| + 1 \leq (2^{n+1} + 4)/3.$$

Also, if ρ denotes the rank 3 permutation character of K on the singular 1-spaces of V, then $0 \leq \rho(g) - 1 \leq 2^{e(g,1)} - 1 \leq 2^n - 1$, whence

$$|\delta^1(g) + \gamma(g)| = |\rho(g) - 1| \leq 2^n - 1.$$

It follows that

$$|\delta^1(g)| \leq (2^n - 1) + |\gamma(g)| \leq (5 \cdot 2^n + 1)/3.$$

Again, by Lemma 5.13, $\delta^1(g) + \delta^2(g) + 1 = \alpha_n(g) + \beta(g)$, and so

$$|\delta^2(g)| \leq 1 + |\delta^1(g)| + |\alpha_n(g) + \beta_n(g)| \leq (7 \cdot 2^n + 5)/3.$$

The degrees of δ^1, δ^2, and γ are listed before Lemma 5.13, and the conclusion now follows. ■

5.2 Centralizer bounds

In this section we obtain centralizer bounds for unbreakable elements of orthogonal groups.

Proposition 5.15 *Let $G = \Omega(V) = \Omega^\epsilon_{2n}(q)\,(q < 7)$ or $\Omega_{2n+1}(q)\,(q = 3, 5)$. Assume that $\dim V \geq 9$, and also that $\dim V \geq 13$ if $q \leq 3$.*

If $x \in G$ is unbreakable, then $|C_G(x)| \leq N$, where N is listed in the following table.

G	q	N
$\Omega^\epsilon_{2n}(q)$	2	$2^{2n+6} \cdot 3$
	3	$3^{2n+4} \cdot 2^{10}$
	4	$4^{2n-3} \cdot 60$
	5	$5^{2n} \cdot 288$
$\Omega_{2n+1}(q)$	3	$3^{2n+3} \cdot 16$
	5	5^{n+1}

Proof (1) *The case $q = 2$.* Here we assume that $G = \Omega^\epsilon_{2n}(2)$ with $n \geq 7$.

Let $x \in G$ be unbreakable, and assume first that x is unipotent. We use the classification of unipotent elements of orthogonal groups in characteristic 2 given by [25] (see also [30]). According to this, $V|x$ is a perpendicular sum of non-degenerate subspaces of the following types:

$V(2k)$: a single Jordan block $J_{2k} \in O^\epsilon_{2k}(2) \backslash \Omega^\epsilon_{2k}(2)$
$W(k)$: two Jordan blocks $J_k^2 \in \Omega^+_{2k}(2)$.

(These are not unique up to conjugacy, but that does not concern us.) Moreover, the only non-perfect groups $\Omega^\epsilon_{2k}(2)$ are $\Omega^\epsilon_2(2)$ and $\Omega^+_4(2)$. Hence for the unbreakable element x, $V|x$ is listed in the following table. The table also gives $\dim \bar{C}$ and $\bar{C}/R_u(\bar{C})$, where $\bar{C}$ is the centralizer of x in the algebraic group $O_{2k}(\bar{F}_2)$. The formula for $\dim \bar{C}$ is given in [25, 4.4]: if $u = (J_{n_i})_i$ with $n_1 \geq n_2 \geq \cdots$, then $\dim \bar{C} = \sum in_i - \chi(n_i)$, where $\chi(n_i) = n_i/2 + 1$ for a summand $V(n_i)$ and $\chi(n_i) = [(n_i + 1)/2]$ for a summand $W(n_i)$. The groups $\bar{C}/R_u(\bar{C})$ are given in [30].

$V\|x$	$\dim \bar{C}$	$\bar{C}/R_u(\bar{C})$
$W(n)$	$2n - 2 + (n, 2)$	$Sp_2\,(n \text{ even}), O_2\,(n \text{ odd})$
$W(2) + W(n-2)$	$2n + 6\,(n \text{ even})$	$Sp_2 \times Sp_2\,(n \text{ even})$
	$2n + 5\,(n \text{ odd})$	$Sp_2 \times O_2\,(n \text{ odd})$
$W(2) + V(2n - 2k - 4) + V(2k)$	$\leq 2n + 4$	$Sp_2 \times 2^a$, $a \leq 2$
$V(2)^2 + W(n-2)$	$2n + 6\,(n \text{ even})$	$Sp_2 \times 2\,(n \text{ even})$
	$2n + 5\,(n \text{ odd})$	$O_2 \times 2\,(n \text{ odd})$
$V(2n - 2k) + V(2k)$	$\leq 2n - 2$	2^a, $a \leq 2$

Applying Lang's Theorem (see [43, I, 3.4]) to the corresponding possibilities for $|C_G(x)|$, we see that the maximum possible value of this occurs for $V(2)^2 + W(n-2)$ with n odd, so that

$$|C_G(x)| \leq 2^{2n+4} \cdot |O^-_2(2) \times 2| = 2^{2n+6} \cdot 3, \tag{13}$$

the claimed bound.

Now assume that x is non-unipotent, and write $x = su$ with semisimple part $s \neq 1$ and unipotent part u. We have

$$C_G(s) = \Omega^\delta_{2k}(2) \times \prod_i GL^{\epsilon_i}_{a_i}(2^{b_i}),$$

where $k + \sum a_i b_i = n$. As each $GL^{\epsilon_i}_{a_i}(2^{b_i}) \leq \Omega_{2a_ib_i}(2)$ and x is unbreakable, it must be the case that either $2k \geq 2n - 4$, or $2a_ib_i \geq 2n - 4$ for some i.

Let $V_{2k} = C_V(s)$, of dimension $2k$. If $2k \geq 2n - 4$, then $V_{2k}|u$ must be $W(k)$ (otherwise x is breakable), so $\dim \bar{C} \leq 2k + 1$ and the bound (13) holds.

Assume now that $2a_ib_i \geq 2n - 4$ for some i. Each Jordan block J_r of u in $GL^{\epsilon_i}_{a_i}(2^{b_i})$ fixes a non-degenerate subspace of dimension $2rb_i$, so for all such r, either $2rb_i \geq 2n-4$ or $2rb_i \leq 4$. It follows that the possibilities with the largest centralizers are:

(a) $k = 0$, $C_G(s) = GU_n(2)$, $u = (J_{n-2}, J_1^2) \in GU_n(2)$

(b) $k = 1$, $C_G(s) = \Omega^-_2(2) \times GU_{n-1}(2)$, $u = (J_{n-2}, J_1) \in GU_{n-1}(2)$.

In case (a), $|C_G(x)| = 2^{n+1}.(GU_2(2) \times GU_1(2))$, which is much smaller than the bound in (13), and in case (b), $|C_G(x)|$ is even smaller.

This completes the proof for $q = 2$.

(2) *The case* $q = 4$. Here we assume that $G = \Omega^{\epsilon}_{2n}(4)$ with $n \geq 5$. This case is similar to the previous one, except that $\Omega^{+}_{4}(q)$ is perfect, so unbreakable elements cannot lie in a subgroup $\Omega(W) \times \Omega(W^{\perp})$ where $\dim W \geq \dim W^{\perp}$ and $\dim W > 2$.

For x unipotent, $V|x$ must be either $W(n)$ or $V(2n-2k)+V(2k)$. The formula for $\dim \bar{C}$ is as in the $q = 2$ case. For $W(n)$ we have $\dim \bar{C} = 2n$, $\bar{C}/R_u(\bar{C}) = Sp_2$ if n is even, and $\dim \bar{C} = 2n-1$, $\bar{C}/R_u(\bar{C}) = O_2$ if n is odd. Thus the largest possibility for $|C_G(x)|$ is $4^{2n-3} \cdot |Sp_2(4)|$.

For x non-unipotent write $x = su$ again, and

$$C_G(s) = \Omega^{\delta}_{2k}(4) \times \prod_i GL^{\epsilon_i}_{a_i}(4^{b_i}),$$

where $k + \sum a_i b_i = n$. As x is unbreakable, either $2k \geq 2n-4$, or $2a_ib_i \geq 2n-4$ for some i, and arguing as for the $q = 2$ case, we see that $|C_G(x)| \leq 4^{2n-3} \cdot 60$.

(3) *The case* $q = 3$. Here we assume that $G = \Omega^{\epsilon}_{2n}(3)$ with $n \geq 7$, or $\Omega_{2n+1}(3)$ with $n \geq 6$. The non-perfect groups $\Omega(W)$ are $\Omega_1(3)$, $\Omega^{\pm}_2(3)$, $\Omega_3(3)$ and $\Omega^{+}_4(3)$.

By [25], if x is unipotent, then $V|x$ is a perpendicular sum of non-degenerate subspaces of the following types:

$$W(2k) \,:\, J^2_{2k} \in \Omega^{+}_{4k}(q)$$
$$V(2k+1) \,:\, J_{2k+1} \in \Omega_{2k+1}(q).$$

The possibilities for $V|x$ are listed in the following table. The formula for $\dim \bar{C}$ is given in [25, 4.4]: if $x = (J_{n_i})_i$ where $n_1 \geq n_2 \geq \cdots$, then

$$\dim \bar{C} = \sum i n_i - \chi(n_i)$$

where $\chi(n_i) = (n_i+1)/2$ for a summand $V(n_i)$ and $\chi(n_i) = n_i/2$ for a summand $W(n_i)$.

$V\|x$	$\dim \bar{C}$	$\bar{C}/R_u(\bar{C})$
$W(n)$	$2n$	Sp_2
$W(2)+W(n-2)$	$2n+8$	$Sp_2 \times Sp_2$
$V(3)+V(2n-3)$	$n+2$	2^2
$V(3)+W(n-1)$	$2n+5$	$Sp_2 \times 2$

(Here we used the assumption that $\dim V \geq 13$ to avoid the configurations $W(2)^3 \in \Omega^{+}_{12}(q)$ and $V(3)+W(2)^2 \in \Omega_{11}(q)$.) Hence, if $G = \Omega^{\epsilon}_{2n}(3)$, then $|C_G(x)| \leq 3^{2n+2} \cdot |Sp_2(3)^2|$; if $G = \Omega_{2n+1}(3)$, then $|C_G(x)| \leq 3^{2n+2} \cdot 2|Sp_2(3)|$.

Now assume x is non-unipotent and write $x = su$ as usual. We have

$$C_G(s) = (O_a(3) \times O_b(3) \times \prod GL^{\epsilon_i}_{a_i}(3^{b_i})) \cap G,$$

where $a = \dim C_V(s)$ and $b = \dim C_V(-s)$. Since $GL^\epsilon_r(q) \leq SO_{2r}(q)$ in general, it follows that b is even since $\det(s) = 1$.

Write $U = C_V(-s)$. Consider $U|u$. This is a sum of spaces of type $W(2k)$ and $V(2k+1)$. Since $-1 \in \Omega^+_{4k}(3)$ (see [26, 2.5.13]), if u_0 is a unipotent element of type $W(2k)$, then

$$-u_0 = -(J^2_{2k}) \in \Omega^+_{4k}(3).$$

Moreover, for a unipotent element of type $\sum_{i=1}^m V(2r_i+1)$ with $m \geq 4$, there exist i, j such that the discriminant of the space $V(2r_i+1) + V(2r_j+1)$ is a square; so if u_1 is the corresponding unipotent element, then $-u_1 = -(J_{2r_i+1}, J_{2r_j+1}) \in \Omega_{2r_i+2r_j+2}(3)$ (again by [26, 2.5.13]).

It follows from these observations that for $\dim V = 2n$, the largest possibility for $|C_G(x)|$ arises when $U = V$ (i.e. $s = -1$) and $V|u$ is $V(1)^4 + W(n-2)$, in which case $\dim \bar{C} = 2n+10$ and $\bar{C}/R_u(\bar{C}) = Sp_2 \times O_4$, so that $|C_G(x)| \leq 3^{2n+1} \cdot |Sp_2(3) \times SO^+_4(3)| = 3^{2n+4} \cdot 2^{10}$, as in the conclusion. When $\dim V = 2n+1$, the maximum is achieved when $a = 3$, $\dim U = b = 2n-2$, $U^\perp|u = V(3)$ and $U|u = W(n-1)$, in which case $\dim \bar{C} = 2n-1$, giving an upper bound for $|C_G(x)|$ which is smaller than that for the unipotent case.

(4) *The case* $q = 5$. Here we assume that $G = \Omega^\epsilon_{2n}(q)$ or $\Omega_{2n+1}(5)$ with $n \geq 4$. The only non-perfect groups $\Omega(W)$ are $\Omega_1(q)$ and $\Omega^\pm_2(q)$.

Assume that $\dim V = 2n$. For unipotent x, the indecomposables are $W(2k)$ and $V(2k+1)$ as in the $q = 3$ case, and the only possibility for $V|x$ with x unbreakable is $W(n)$, in which case $\dim \bar{C} = 2n$, $\bar{C}/R_u(\bar{C}) = Sp_2$ and $|C_G(x)| \leq q^{2n-3} \cdot |Sp_2(q)|$. For $x = su$ non-unipotent, the maximum value of $|C_G(x)|$ occurs when $s = -1$ and $V|u = V(1)^2 + W(n-1)$, in which case $|C_G(x)| \leq q^{2n-1} \cdot |Sp_2(q) \times O^-_2(q)|$, which is the bound in the conclusion.

For $\dim V = 2n+1$ the only unbreakable unipotent class is the regular class (corresponding to the indecomposable $V(2n+1)$), which has centralizer of order 5^n. For $x = su$ non-unipotent and unbreakable, $C_V(s)$ is a non-degenerate subspace of odd dimension on which x acts as a unipotent element. Hence the unbreakability of x forces $\dim C_V(s) = 2n-1$ and $C_V(s)|x = V(2n-1)$, whence $|C_G(x)| \leq 5^{n-1} \cdot O^-_2(5) < 5^{n+1}$, as required.

This completes the proof of the proposition. ∎

We also need a version of Proposition 5.15 for the 12-dimensional orthogonal groups over $\mathbb{F}_3$.

Lemma 5.16 *Let $G = \Omega^\epsilon_{12}(3)$ and let $x \in G$ be unbreakable. Then one of the following holds:*

(i) $|C_G(x)| \leq 3^{16}.2^6$;

(ii) $\epsilon = +$, $x = (J_2^6)$ *or* $-(J_2^6)$, *and x is a commutator in G.*

Proof The proof runs along similar lines to that of 5.15: the bound in (i) is achieved by unipotent $u \in \Omega^+_{12}(3)$ with $V|u = W(2) + W(4)$ and centralizer $3^{14}.(Sp_2(3)^2)$; and the exceptional elements in (ii) come from the decomposition $W(2)^3$. (Note that $x = -(I_4, J_4^2)$ with $\epsilon = +$, arising from the decomposition $-(V(1)^4 + W(4))$, has larger centralizer than the bound in (i); but this element is in fact breakable, since $-I_4$ is a commutator in $\Omega^+_4(3)$.) Finally, the elements in (ii) are commutators since they lie in a subgroup $\Omega^+_4(3^3) \cong SL_2(27) \circ SL_2(27)$, and every element in $SL_2(27)$ is a commutator. ∎

5.3 Proof of Theorem 5.1

The main step in the proof of Theorem 5.1 is the following.

Lemma 5.17 *Let G be one of the orthogonal groups $\Omega_{2n+1}(q)$ ($n \geq 1$, q odd, $q < 7$), $\Omega^+_{2n}(q)$ ($n \geq 2$, $q < 5$) or $\Omega^-_{2n}(q)$ ($n \geq 2$, $q < 7$), excluding the groups $\Omega_3(3), \Omega^+_4(2), \Omega^+_4(3)$. Every unbreakable element of G is a commutator.*

Proof We first sketch the structure of our proof, which is similar to that of Section 4 for symplectic groups.

Let $G = \Omega^\epsilon_n(q)$ and let $g \in G$ be unbreakable. By Lemma 3.1(iv), we may assume that $n \geq 14$ if $q = 2$, $n \geq 12$ if $q = 3$, and $n \geq 9$ if $q = 4, 5, 7$.

We want to show that

$$|\sum_{\chi \in \ \mathrm{Irr}(G),\ \chi(1)>1} \frac{\chi(g)}{\chi(1)}| < 1,$$

which implies that $\sum_{\chi \in \ \mathrm{Irr}(G)} \chi(g)/\chi(1) \neq 0$ and so g is a commutator in G by Lemma 2.5. We usually break this sum into two sub-sums:

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

where $d(G)$ is chosen suitably. We use the results of Section 5.1 to show that $|E_1(g)|$ is small. We frequently use the bound

$$|E_2(g)| < \frac{\sqrt{k(G) \cdot |C_G(g)|}}{d(G)}, \tag{14}$$

which follows from Lemma 2.6. In applying (14), we use the bound on $|C_G(g)|$ from Section 5.2; we also use the crude bound $k(G) \leq 4k(GO^\epsilon_n(q))$, where $k(GO^\epsilon_n(q))$ is bounded by Proposition 2.7.

Case 1: $G = \Omega^-_{2n}(5)$, and $n \geq 5$.

First we assume that $n \geq 6$. Then $k(G) \leq 116 \cdot 5^n$ by 2.7, and $|C_G(g)| \leq 5^{2n} \cdot 288 \leq (2.304)5^{2n+3}$ by 5.15, whence $k(G) \cdot |C_G(g)| < 268 \cdot 5^{3n+3} < 5^{3n+7}$. We choose $d(G) = 5^{4n-10}$. It follows using (14) that

$$|E_2(g)| < 5^{(3n+7)/2-(4n-10)} = 5^{(27-5n)/2} \leq 5^{-3/2} < 0.09.$$

By Proposition 5.3, $E_1(g)$ involves $q + 4 = 9$ terms, and each has absolute value at most $(q+1)/q^3$ by Proposition 5.12. Hence

$$|E_1(g)| \leq (q+1)(q+4)/q^3 \leq 0.432,$$

and so $|E_1(g) + E_2(g)| < 0.522$.

Next we consider the case $n = 5$ so $G = \Omega^-_{10}(5)$. The degrees of the irreducible complex characters of $SO^-_{10}(q)$ are available in [33]. Specializing to $q = 5$, we obtain that $k(SO^-_{10}(5)) = 5266$, whence $k(G) = 2633$ as $SO^-_{10}(5) = C_2 \times \Omega^-_{10}(5)$. By 5.15, $|C_G(g)| \leq 5^{10} \cdot 288$. Choosing $d(G) = 4 \cdot 5^9$, we get

$$|E_2(g)| < \sqrt{5^{10} \cdot 288 \cdot 2633}/(4 \cdot 5^9) < 0.35.$$

By Propositions 5.3 and 5.12, $E_1(g)$ involves 9 terms, and each has absolute value at most $6/125$, whence $|E_1(g)| < 54/125$ and so $|E_1(g)| + |E_2(g)| < 0.79$.

Case 2: $G = \Omega_{2n+1}(5)$, and $n \geq 4$.

Here $k(G) \leq 2k(SO_{2n+1}(5)) \leq 5^n \cdot (14.76)$ by 2.7, and $|C_G(g)| \leq 5^{n+1}$ by 5.15. First suppose that $n \geq 5$ and choose $d(G) = 5^{4n-8}$. It follows that

$$|E_2(g)| < 5^{(2n+1)/2-(4n-8)} \cdot \sqrt{(14.76)} < 0.01.$$

By Theorem 5.3, $E_1(g)$ involves 9 terms, and each has absolute value at most $6/125$ by Theorem 5.12. Hence $|E_1(g)| \leq 54/125$ and so $|E_1(g) + E_2(g)| < 0.5$.

Next we assume that $n = 4$ and choose $d(G) = 4^{10}$. By 5.15, $|C_G(g)| \leq 5^5$. It follows that

$$|E_2(g)| < \sqrt{5^5 \cdot 5^4 \cdot (14.76)}/4^{10} < 0.01.$$

The degrees of the irreducible complex characters of $Spin_9(5)$ are available in [33]. Using this list, it is straightforward to check that G has at most 13 nontrivial irreducible characters of degree at most 4^{10}, and all have degree at least 16276. Hence $|E_1(g)| \leq \sqrt{5^5 \cdot 13}/16276 < 0.02$, and so $|E_1(g) + E_2(g)| < 0.03$.

Case 3: $G = \Omega_{2n+1}(3)$, and $n \geq 6$.

Here $k(G) \leq 2k(SO_{2n+1}(3)) \leq 3^n \cdot (14.76)$ by 2.7, and $|C_G(g)| \leq 3^{2n+3} \cdot 16$ by 5.15, whence $k(G) \cdot |C_G(g)| < 3^{3n+3} \cdot 237 < q^{3n+8}$. We choose $d(G) = q^{4n-8}$. It follows that

$$|E_2(g)| < q^{(3n+8)/2-(4n-8)} = q^{(24-5n)/2} \leq q^{-3} < 0.04.$$

By Proposition 5.3, $E_1(g)$ involves 7 terms, and each has absolute value at most 1/20 by Proposition 5.12. Hence $|E_1(g)| \leq 7/20$ and so $|E_1(g) + E_2(g)| < 0.39$.

Case 4a: $G = \Omega^{\pm}_{2n}(3)$, and $n \geq 7$.

We choose $d(G) = 3^{4n-10}$. By Proposition 5.3, $E_1(g)$ involves 7 terms, and each has absolute value at most 1/20 by Proposition 5.12. Hence $|E_1(g)| \leq 7/20$.

Assume $n \geq 8$. Then $k(G) \leq 3^n \cdot 116$ by 2.7, and $|C_G(g)| \leq 3^{2n+4} \cdot 2^{10}$ by 5.15, whence $k(G) \cdot |C_G(g)| < 3^{3n+4} \cdot 2^{10} \cdot 116 < q^{3n+15}$. It follows that

$$|E_2(g)| < q^{(3n+15)/2-(4n-10)} = q^{(35-5n)/2} \leq q^{-5/2} < 0.07,$$

and so $|E_1(g) + E_2(g)| < 0.42$.

Assume $n = 7$. Then $k(GO^{\pm}_{2n}(3)) < 3^n \cdot 7$ by Lemma 2.8, and so $k(G) < 3^n \cdot 28$. Thus

$$|E_2(g)| < \frac{\sqrt{3^{3n+4} \cdot 2^{10} \cdot 28}}{3^{4n-10}} < 0.41,$$

whence $|E_1(g) + E_2(g)| < 0.76$.

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

We choose $d(G) = 3^{14}$. As in Case 4a, $E_1(g)$ involves 7 terms, and each has absolute value at most 1/20 by Proposition 5.12. Hence $|E_1(g)| \leq 7/20$.

We break $E_2(g)$ into two sub-sums:

$$E_3(g) = \sum_{\chi \in \ \mathrm{Irr}(G),\ 3^{14} < \chi(1) \leq 3^{15}} \frac{\chi(g)}{\chi(1)}, \quad E_4(g) = \sum_{\chi \in \ \mathrm{Irr}(G),\ \chi(1) > 3^{15}} \frac{\chi(g)}{\chi(1)}.$$

By (14), $|E_4(g)| < \sqrt{k(G) \cdot |C_G(g)|}/3^{15}$. By Lemma 2.8, $k(GO^{\pm}_{12}(3)) < 3^6 \cdot (6.4)$, and so $k(G) < 3^6 \cdot (25.6)$. By Lemma 5.16 we may assume that $|C_G(g)| \leq 3^{16} \cdot 2^6$. It follows that

$$|E_4(g)| < \frac{\sqrt{3^{22} \cdot 2^6 \cdot (25.6)}}{3^{15}} < 0.5.$$

On the other hand, by Proposition 5.3 there are at most 15 terms in $E_3(g)$. The Cauchy-Schwarz inequality yields $|E_3(g)| < \sqrt{15 \cdot |C_G(g)|}/3^{14} < 0.05$. Consequently,

$$|E_1(g) + E_2(g)| \leq |E_1(g)| + |E_3(g)| + |E_4(g)| < 0.9.$$

Case 5: $G = \Omega^{\pm}_{2n}(4)$, and $n \geq 5$.

Here $k(G) \leq 2k(GO^{\pm}_{2n}(4)) \leq 4^n \cdot 35$ by 2.7, and $|C_G(g)| \leq 4^{2n-3} \cdot 60$ by 5.15, whence $k(G) \cdot |C_G(g)| < 4^{3n-3} \cdot 2100$. We choose $d(G) = 2^{4n-10}$. It follows that

$$|E_2(g)| < 4^{(3n-3)/2-(4n-10)} \cdot \sqrt{2100} = q^{(17-5n)/2} \cdot \sqrt{2100} < 0.18.$$

By Proposition 5.4, $E_1(g)$ involves at most 10 characters, and each has degree $> 4^{2n-3}$. The Cauchy-Schwarz inequality yields

$$|E_1(g)| < \sqrt{10 \cdot |C_G(g)|}/4^{2n-3} = \sqrt{600}/2^{2n-3} < 0.2.$$

Consequently $|E_1(g) + E_2(g)| < 0.38$.

Case 6: $G = \Omega^{\pm}_{2n}(2)$, and $n \geq 7$.

Here $k(G) \leq 2k(GO^{\pm}_{2n}(2)) \leq 2^n \cdot 35$ by 2.7, and $|C_G(g)| \leq 2^{2n+6} \cdot 3$ by 5.15, whence $k(G) \cdot |C_G(g)| < 2^{3n+6} \cdot 105$. We choose $d(G) = 2^{4n-10}$. It follows that

$$|E_2(g)| < 2^{(3n+6)/2-(4n-10)} \cdot \sqrt{105} = 2^{(26-5n)/2} \cdot \sqrt{105} < 0.46.$$

By Proposition 5.14, $|E_1(g)| \leq 7/2^5 < 0.22$, whence $|E_1(g) + E_2(g)| < 0.68$.

In all cases, we have shown that $|\sum_{\chi \in \mathrm{Irr}(G)\setminus\{1_G\}} \chi(g)/\chi(1)| < 1$, and hence that g is a commutator. ■

Theorem 5.1 now follows from Lemmas 5.17 and 2.9.

6 Unitary groups

In this section we prove the following result, which together with Lemma 2.4, implies Ore's conjecture for the unitary groups.

Theorem 6.1 *Let $G = SU_n(q)$ with $n \geq 3$, excluding $SU_3(2)$. Then every element of G is a commutator.*

Our proof differs from that for the symplectic and orthogonal groups: the bounds for centralizers of unbreakable elements in unitary groups are much weaker than for the other types, making the character theoretic part of that approach unworkable.

Instead, we use a more direct approach. Given $X \in G = SU_n(q)$, we find $B, C \in G$ such that $XB = C$ and B, C are conjugate. This obviously implies that X is a commutator. Here is a rough sketch of our approach to

solving the equation $XB = C$. We write $X = \mathrm{diag}(X_1, \ldots, X_k)$ in diagonal block form, where the blocks X_i are indecomposable matrices in $GU_{n_i}(q)$ (indecomposable meaning that each X_i does not fix a proper non-degenerate subspace of the unitary n_i-space). We then attempt to solve equations of the form $X_iB_i = C_i$, where B_i and C_i are both matrices in $GU_{n_i}(q)$ with diagonal block form $\mathrm{diag}(b, J_{n_i-1})$ with b a scalar (and of course we require $\det(C_i) = \det(X_i)\det(B_i)$). If we can solve such an equation, we say that X_i has the (b, J)-*property*. Taking B, C to be the block diagonal sum of the resulting matrices B_i, C_i, we obtain a solution to our original equation $XB = C$.

The approach hinges on establishing both the (b, J)-property for indecomposable matrices in $GU_n(q)$, and also a variant called the (a, b, J)-property which ensures that the determinants of the final matrices B, C are 1. We prove these properties for $n \geq 7$ in Section 6.2, and some variants for $q = 2$ and 3 in Sections 6.3 and 6.4. The proofs are character theoretic, based on a substantial amount of new information about characters of unitary groups of low degree obtained in Section 6.1. For dimensions $n < 7$ we study the (b, J)- and (a, b, J)-properties using computational methods. This is a manageable task, since we can assume that $q \leq 7$ by Lemma 2.4. To complicate matters, however, it turns out that for small n, q, there are many elements of $GU_n(q)$ which do not have the (b, J)- or (a, b, J)-properties. This leads to several technical complications in the proof of Theorem 6.1, which is finally completed in Section 6.5.

6.1 Characters of small degree

In this section, we study irreducible complex characters of relatively small degrees of the unitary groups $GU_n(q)$, $n \geq 7$. The main result is Proposition 6.6.

Our approach uses the theory of dual pairs in similar fashion to the proofs for orthogonal groups in Section 5.1. We consider the dual pair $S \times G$ inside $\Gamma := GU_{2n}(q)$, where $S = GU_2(q)$ and $G \in \{SU_n(q), GU_n(q)\}$, and

$$\omega(g) = \zeta_{2n,q}(g) = (-q)^{\dim \mathrm{Ker}_{\mathbb{F}_{q^2}}(g-1)} \tag{15}$$

is a *reducible* Weil character of $GU_{2n}(q)$, of degree q^{2n} (see [48]). More precisely, we view S as $GU(U)$, where $U = \langle e, f \rangle_{\mathbb{F}_{q^2}}$ is endowed with the Hermitian form $(\cdot, \cdot)$, and Gram matrix $\mathrm{diag}(1, 1)$ in the basis $\{e, f\}$. Next, $GU_n(q)$ means $GU(W)$, where $W = \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_{q^2}}$ is endowed with the Hermitian form $(\cdot, \cdot)$, and Gram matrix $\mathrm{diag}(1, 1, \ldots, 1)$ in the basis $\{v_1, \ldots, v_n\}$. Now we consider $V = U \otimes W$ with the Hermitian form $(\cdot, \cdot)$ defined via $(u \otimes w, u' \otimes w') = (u, u') \cdot (w, w')$ for $u \in U$ and $w \in W$. The action of $S \times G$ on V induces a homomorphism $S \times G \to \Gamma := GU(V)$.

Lemma 6.2 *Let $n \geq 4$ if $G = GU_n(q)$ and $n \geq 5$ if $G = SU_n(q)$. Under the above assumptions,*

$$(\omega|_G, \omega|_G)_G = (q+1)(q^3+1).$$

Further, $(\omega|_G, 1_G)_G = q+1$.

Proof Let A be the matrix of $g \in G$ in the basis $\{v_1, \ldots, v_n\}$ of W. Then g has matrix $\mathrm{diag}(A, A)$ in the basis $\{e \otimes v_i, f \otimes v_i\}$ of V. It follows that $\omega(g)$ is the number of g-fixed points on W, and $\omega^2(g)$ is the number of g-fixed points on the set $W \times W$. Hence $(\omega|_G, 1_G)_G$ is the number of G-orbits on W, which is $q+1$. Next, $(\omega|_G, \omega|_G)_G$ equals the number of G-orbits on $W \times W$. Using Witt's theorem and the assumptions on n, one can show that G has exactly $(q+1)(q^3+1)$ orbits on $W \times W$, with the following representatives: $(0,0)$, $(v, \lambda v)$ where $\lambda \in \mathbb{F}_{q^2}$, $0 \neq v \in V$ and $(v,v) = \mu \in \mathbb{F}_q$, $(0, v)$ where $0 \neq v \in V$ and $(v,v) = \mu \in \mathbb{F}_q$, and (u, v) where $u, v \in V$ are linearly independent and $(\cdot, \cdot)$ has Gram matrix $\begin{pmatrix} a & b \\ b^q & c \end{pmatrix}$ with $a, c \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q^2}$. ■

Proposition 6.3 *Assume that $S = GU_2(q)$, q any prime power, and $G = GU_n(q)$ with $n \geq 4$ or $G = SU_5(q)$ with $n \geq 5$. Then the restriction $\zeta_{2n,q}|_{S \times G}$ of the reducible Weil character $\zeta_{2n,q}$ of degree q^{2n} of $GU_{2n}(q)$ decomposes as $\sum_{\alpha \in \mathrm{Irr}(S)} \alpha \otimes D_\alpha$, where the characters $D^\circ_\alpha := D_\alpha - k_\alpha \cdot 1_G$ are all irreducible and distinct, for some $k_\alpha \in \{0, 1\}$. Further, $k_\alpha = 1$ precisely when $\alpha = 1_S$ or α is the Steinberg character St of S.*

Proof 1) Apply Lemma 5.5 to the character $\omega = \zeta_{2n,q}$, and define $l_\alpha := (D_\alpha, 1_G)_G$ and $D^\circ_\alpha := D_\alpha - l_\alpha \cdot 1_G$. By Lemma 6.2, $\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) l_\alpha = q+1$,

$$\omega|_G = (q+1) \cdot 1_G + \sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) D^\circ_\alpha,$$

and $(D^\circ_\alpha, 1_G)_G = 0$ for all α. Again by Lemma 6.2,

$$\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1)^2 = |S| = (q+1)(q^3-q) = \left(\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) D^\circ_\alpha, \sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1) D^\circ_\alpha \right)_G.$$

It follows that all D°_α, $\alpha \in \mathrm{Irr}(S)$, must be irreducible and distinct, if all of them have positive degrees.

2) The character table of S is well known, see e.g. [13]. We use the same labelling for the irreducible characters: $\chi_1^{(t)}$ of degree 1 (where $1 \leq t \leq q+1$; in particular, $\chi_1^{(q+1)} = 1_S$), $\chi_q^{(t)}$ of degree q (where $1 \leq t \leq q+1$; in particular, $\chi_q^{(q+1)}$ is the Steinberg character), $\chi_{q-1}^{(t,u)}$ of degree $q-1$ (where

$1 \le t \ne u \le q+1$ and $\chi_{q-1}^{(t,u)} = \chi_{q-1}^{(u,t)}$), and $\chi_{q+1}^{(t)}$ of degree $q+1$ (where $1 \le t \ne u \le q^2-2$ and $t \notin (q-1)\mathbb{Z}$). It is straightforward to compute $D_\alpha(1) = (\omega|_S, \alpha)_S$. In particular, $D_\alpha(1) > q+1$ and so $D_\alpha^\circ(1) > 0$ for all $\alpha \in \mathrm{Irr}(S)$. Hence the D_α° are all irreducible and distinct. It remains to prove that $l_\alpha = k_\alpha$, where the integers k_α are defined in the statement.

The degrees of D_α and the integers k_α are listed in Table III. Observe that $\omega|_G$ contains the rank 3 permutation character of G (on singular 1-spaces of W). The degrees of the irreducible constituents of the latter are well known (see e.g. [42]). It follows in particular that for each $\beta \in \{1_S, St\}$ there is some α such that D_α° has degree $D_\beta(1)-1$. Thus $|D_\alpha(1) - D_\beta(1)| = |l_\alpha - 1| \le q$. First we assume that $\beta = St$. It is easy now to check that $|D_\alpha(1) - D_\beta(1)| > q+1$ for $\alpha \ne St$, whence $\alpha = St$. Next we assume that $\beta = 1_S$. Since $l_{St} = 1$ and $\sum_{\gamma \in \mathrm{Irr}(S)} l_\gamma \gamma(1) = q+1$, we conclude that $\alpha(1) = 1$. A short computation reveals that $\alpha = 1_S$. ∎

TABLE III. Degrees of D_α for $G = SU_n(q)$

α	$\alpha(1)$	$D_\alpha(1)$	k_α
1_S	1	$(q^n-(-1)^n)(q^{n-1}+(-1)^n q^2)/(q+1)(q^2-1)+1$	1
$\chi_1^{(t)}$, $t \ne q+1$	1	$(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q+1)(q^2-1)$	0
St	q	$(q^n+(-1)^n q)(q^n-(-1)^n q^2)/(q+1)(q^2-1)+1$	1
$\chi_q^{(t)}$, $t \ne q+1$	q	$(q^n-(-1)^n)(q^n+(-1)^n q)/(q+1)(q^2-1)$	0
$\chi_{q-1}^{(q+1,u)}$, $u \ne q+1$	$q-1$	$(q^n-(-1)^n)(q^{n-1}+(-1)^n q)/(q+1)^2$	0
$\chi_{q-1}^{(t,u)}$, $t,u \ne q+1$	$q-1$	$(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q+1)^2$	0
$\chi_{q+1}^{(t)}$	$q+1$	$(q^n-(-1)^n)(q^{n-1}+(-1)^n)/(q^2-1)$	0

Direct computation yields the following.

Lemma 6.4 *In the notation of Proposition* 6.3*, for any* $\alpha \in \mathrm{Irr}(GU_2(q))$*,*

$$D_\alpha^\circ(1) > \kappa \cdot \frac{q^{2n-1}\alpha(1)}{(q+1)(q^2-1)}$$

where $\kappa > 1 - 1/q^{n-3}$*.*

For completeness and future reference, we prove (in the notation of the proof of Proposition 6.3):

Proposition 6.5 *Let q be any prime power and consider the subgroup $K = SU_4(q)$ of $G = GU_4(q)$. Consider the irreducible constituents D_α° of $\zeta_{8,q}|_G$ as in Proposition* 5.8*. The following statements hold.*

(i) $(\zeta_{8,q}|_K, \zeta_{8,q}|_K)_K = (q+1)(q^3+1)+q$.

(ii) $D^\circ_\alpha|_K = D^\circ_\beta|_K$ *if and only if* $\{\alpha,\beta\} = \{\chi_1^{(t)}, \chi_1^{(q+1-t)}\}$ *for some* $t \in \{1,\dots q\} \setminus \{(q+1)/2\}$.

(iii) *All* D°_α *restrict irreducibly to* K, *except when* q *is odd and* $\alpha = \chi_1^{((q+1)/2)}$. *In the exceptional case,* $D^\circ_\alpha|_K$ *is the sum of two distinct irreducible characters of degree* $(q+1)(q^2+1)/2$.

Proof 1) The proof of Lemma 6.2 yields that $(\omega|_K, 1_K)_K = q+1$. However the number of K-orbits on $W \times W$, and so $(\omega|_K, \omega|_K)_K$, equals $(q+1)(q^3+1)+q$, since the single G-orbit on the pairs (u,v), where $\langle u,v\rangle_{\mathbb{F}_{q^2}}$ is a totally singular 2-space, splits into $q+1$ K-orbits. Thus (i) is proved.

Since ω is real-valued, the formula for D_α in Lemma 5.5 implies that $\overline{D}_\alpha = D_{\overline{\alpha}}$. Notice that $D_\alpha = D^\circ_\alpha$ has degree $(q^2+1)(q^2-q+1)$ for $\alpha = \chi_1^{(t)}$ with $1 \le t \le q$. Assume in addition that $q = 2$. Then (iii) obviously holds, as $G = K \times \mathbb{Z}_3$. Further, for the aforementioned α, $D_\alpha(1) = 15$ and so it is real-valued by [8], whence $D_\alpha = D_{\overline{\alpha}}$. Together with (i), this implies (ii). Henceforth we assume $q > 2$.

2) Again we focus on $D_\alpha = D^\circ_\alpha$, where $\alpha = \chi_1^{(t)}$ with $1 \le t \le q$. Since $D_\alpha(1) = (q^2+1)(q^2-q+1)$ and $q > 2$, D_α must be one of the irreducible characters $\chi_{22}(k,l)$ of $G = GU_4(q)$, $1 \le k \ne l \le q+1$, listed in [39]. Hence

$$D_{\overline{\alpha}} = \overline{D}_\alpha = \overline{\chi}_{22}(k,l) = \chi_{22}(q+1-k, q+1-l).$$

But, in the notation of [39], $\chi_{22}(k,l) = \chi_{22}(q+1-k, q+1-l)\cdot\chi_1(k+l)$, where $\chi_1(k+l)$ has degree 1 and so it is trivial on K. We have shown that $D_\alpha|_K = \overline{D}_\alpha|_K$ when $\alpha(1) = 1$ but $\alpha \ne 1_S$. Let $\rho_1,\dots,\rho_s$ be all the distinct characters among $D_\alpha|_K$ with $\alpha \ne \overline{\alpha}$ and $\alpha(1) = 1$, each appearing with multiplicity $m_1,\dots,m_s$, respectively. In particular, $m_i \ge 2$ for all i.

3) Assume q is even and > 2. Then $\sum_{i=1}^s m_i = q$, while (i) implies that

$$\left(\sum_{i=1}^s m_i\rho_i, \sum_{i=1}^s \rho_i\right)_K \le 2q.$$

Hence $s \le q/2$, and

$$2q \ge \sum_{i=1}^s m_i^2 \ge (\sum_{i=1}^s m_i)^2/s \ge q^2/(q/2)$$

by the Cauchy-Schwarz inequality. It follows that $s = q/2$, $m_i = 2$ for all i, and so (ii) and (iii) follow.

4) Now assume that q is odd. Then $\sum_{i=1}^s m_i = q-1$, while (i) implies

$(\sum_{i=1}^s m_i\rho_i, \sum_{i=1}^s \rho_i)_K \le 2q-1$. Hence $s \le (q-1)/2$, and

$$2q-1 \ge \sum_{i=1}^s m_i^2 \ge (\sum_{i=1}^s m_i)^2/s \ge (q-1)^2/((q-1)/2) = 2q-2$$

by the Cauchy-Schwarz inequality. It follows that $s=(q-1)/2$, and $m_i=2$ for all i. If some ρ_i is reducible, then

$$\left(\sum_{i=1}^s m_i\rho_i, \sum_{i=1}^s m_i\rho_i\right)_K \ge 4\cdot\frac{q-3}{2} + 4\cdot 2 = 2q+2,$$

violating (i). The same happens if $(\rho_i,\rho_j)_K \ne 0$ for some $i\ne j$. Thus all the characters ρ_i, $1\le i\le (q-1)/2$, are distinct and irreducible. Together with (i), this also implies that $D^\circ_\alpha|_K$ is irreducible for all α with $\alpha(1)>1$. Recall that $D^\circ_{1_S}$, one of the two nontrivial irreducible constituents of the rank 3 permutation character of G, restricts irreducibly to K.

Let $\gamma = \chi_1^{((q+1)/2)}$. We claim that $D_\gamma|_K$ is the sum of two distinct irreducible characters of degree $(q+1)(q^2+1)/2$ (and so (ii) and (iii) follow). It suffices to show that $D_\gamma|_K$ is reducible. Assume the contrary. If $D_\gamma|_K = D^\circ_\beta|_K$ for some $\beta\ne\gamma$, then $(\omega|_K,\omega|_K) > (q+1)(q^3+1)+q$, which contradicts (i). If $D_\gamma|_K \ne D^\circ_\beta|_K$ for any $\beta\ne\gamma$, then $(\omega|_K,\omega|_K) \ne (q+1)(q^3+1)+q$, which also contradicts (i). ■

Recall (see [48]) that, for $n\ge 3$, $GU_n(q)$ has $(q+1)^2$ irreducible Weil characters, each of which is a product of a character of degree 1 of $GU_n(q)$ and one of the following characters

$$\zeta^i_{n,q}(g) = \frac{(-1)^n}{q+1}\sum_{j=0}^q \tilde\xi^{ij}(-q)^{\dim_{\mathbb{F}_{q^2}}\mathrm{Ker}(g-\xi^j)}, \tag{16}$$

with $0\le i\le q$. We fix a primitive $(q+1)^{\text{th}}$-root $\tilde\xi$ of unity in $\mathbb{C}$ and a primitive $(q+1)^{\text{th}}$-root ξ of unity in $\mathbb{F}_{q^2}$, and take the dimension of the ξ^j-eigenspace of g acting on the natural module $\mathbb{F}_{q^2}^n$ for $GU_n(q)$.

The main result of this section is the following:

Proposition 6.6 *Let $n\ge 7$, $q=p^f$, $G:=GU_n(q)$, and let*

$$D := \begin{cases} \frac{(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})(q^{n-2}-(-1)^{n-2})}{(q+1)(q^2-1)(q^3+1)}, & n \text{ even},\\ \frac{(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})(q^{n-2}+(-1)^n q^3)}{(q+1)(q^2-1)(q^3+1)}, & n \text{ odd}. \end{cases}$$

Assume that $\chi\in \mathrm{Irr}(G)$ and $\chi(1)<D$. Then one of the following holds.

(i) *χ is one of $q+1$ irreducible characters of degree 1 of G;*

(ii) χ *is one of* $(q+1)^2$ *irreducible Weil characters of* G*;*

(iii) $\chi = \lambda\tau$*, where* $\lambda \in \mathrm{Irr}(G)$ *has degree* 1*, and* τ *is one of the irreducible characters* D°_α *defined in Proposition* 6.3 *for* G*.*

Proof This goes a little beyond [47, Theorem 4.1] and is proved by the same method, using Lusztig's classification of irreducible characters of $GU_n(q)$ (see [10]). We omit the details. Comparing with Proposition 6.3, we see that the characters $\chi \in \mathrm{Irr}(G)$ with $\chi(1) < D$ are precisely those listed in (i) and (ii), plus $q+1$ characters of degree $D^\circ_\alpha(1)$ for each $\alpha \in \mathrm{Irr}(GU_2(q))$. On the other hand, since $n \geq 7$, Proposition 6.3 also implies that the restrictions of D°_α to $SU_n(q)$, where $\alpha \in \mathrm{Irr}(GU_2(q))$, are all distinct and irreducible. By Clifford theory for cyclic extensions, the characters τD°_α, where $\tau \in \mathrm{Irr}(GU_n(q)/SU_n(q))$ and $\alpha \in \mathrm{Irr}(GU_2(q))$, are all distinct and irreducible. The result follows. ■

6.2 The (b, J)- and (a, b, J)-properties for $GU_n(q)$ with large n

Define $X \in GU_n(q) = GU(V)$ to be *indecomposable* if X cannot be embedded in any natural subgroup $GU_m(q) \times GU_{n-m}(q)$ with $1 \leq m \leq n-1$; namely, X is indecomposable if it does not fix a proper non-degenerate subspace of V.

Write $F_0 = \{a \in \mathbb{F}_{q^2} : a^{q+1} = 1\}$.

Definition (1) For $A \in GU_n(q)$ and $b \in F_0$, we say that A has the (b, J)-*property* if there are matrices $B, C \in GU_n(q)$ such that $AB = C$, B is conjugate (in $GU_n(q)$) to the block diagonal matrix $\mathrm{diag}(b, J_{n-1})$, and C is conjugate to $\mathrm{diag}(b|A|, J_{n-1})$.

(2) For $A \in GU_n(q)$ and $a, b \in F_0$, we say that A has the (a, b, J)-*property* if there are matrices $B, C \in GU_n(q)$ such that $AB = C$, B is conjugate to $\mathrm{diag}(a, b, J_{n-2})$, and C is conjugate to $\mathrm{diag}(a|A|, b, J_{n-2})$.

We now use the results of Section 6.1 to establish the (b, J)- and (a, b, J)-properties for indecomposable elements of $GU_n(q)$.

A. Preliminaries

Let $V = \mathbb{F}_{q^2}^n$ denote the natural module for $G = GU_n(q)$. For $\alpha \in \mathbb{F}_{q^2}^\times$, let $e(g, \alpha)$ denote $\dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(g - \alpha)$, the dimension of the α-eigenspace of g acting on $V \otimes_{\mathbb{F}_{q^2}} \overline{\mathbb{F}}_q$.

We begin with the following observation.

Lemma 6.7 *If* $g \in G := GU_n(q)$ *is indecomposable, then* $|C_G(g)| \leq (q+1)q^{n-1}$*. For* $\alpha \in \mathbb{F}_{q^2}^\times$*, exactly one of the following holds.*

(i) $e(g,\alpha)=0$, *except possibly for one value of* α*: in this exceptional case* $\alpha\in F_0$ *and* $e(g,\alpha)=1$.

(ii) $e(g,\alpha)=0$, *except possibly for two values* $\alpha\in\{\lambda,\lambda^{-q}\}$ *with* $\lambda\notin F_0$, *for which* $e(g,\alpha)=1$.

Proof Write $g=su$ with s the semisimple part and u the unipotent part. For irreducible polynomial $f(t)\in\mathbb{F}_{q^2}[t]$ with nonzero root λ, denote by $\check{f}$ the unique irreducible polynomial with root λ^{-q}. The indecomposability of g implies that one of the following two cases must occur.

(a) s has characteristic polynomial f^k on V, for some irreducible polynomial $f\in\mathbb{F}_{q^2}[t]$ of odd degree r, with $f(0)\neq 0$ and $f=\check{f}$. In this case, $C_G(s)=GU_k(q^r)$. Further, considered as an element of $GU_k(q^r)$, u has only one Jordan block J_k of size k. It follows that

$$C_G(g)=C_{C_G(s)}(u)=C_{GU_k(q^r)}(J_k)$$

has order $q^{r(k-1)}(q^r+1)\leq(q+1)q^{n-1}$ (since $n=kr$). Let λ be a root of f. Then all the eigenvalues of g on V are $\lambda^{q^{2i}}$ with $i\geq 0$. Since $\deg(f)=r$ and $f=\check{f}$, $\lambda^{q^r+1}=1$ but $\lambda\notin\mathbb{F}_{q^{2j}}$ for any $1\leq j<r$. Therefore $e(g,\alpha)$ can be nonzero only when $r=1$ and $\alpha=\lambda$, in which case it equals 1.

(b) s has characteristic polynomial $f^k\check{f}^k$ on V, for some irreducible polynomial $f\in\mathbb{F}_{q^2}[t]$ of degree r, with $f(0)\neq 0$ and $f\neq\check{f}$. In this case, $C_G(s)=GL_k(q^{2r})$. Further, considered as an element of $GL_k(q^{2r})$, u has only one Jordan block J_k of size k. It follows that

$$C_G(g)=C_{C_G(s)}(u)=C_{GL_k(q^{2r})}(J_k)$$

has order $q^{2r(k-1)}(q^{2r}-1)<q^n$ (since $n=2kr$). Let λ be a root of f. Then all the eigenvalues of g on V are $\lambda^{(-q)^i}$ with $i\geq 0$. Since $\deg(f)=r$, $\lambda\notin\mathbb{F}_{q^{2j}}$ for any $1\leq j<r$. Therefore $e(g,\alpha)$ can be nonzero only when $r=1$ and $\alpha\in\{\lambda,\lambda^{-q}\}$, in which case it equals 1. In the exceptional case, $\lambda^{q+1}\neq 1$ since $f\neq\check{f}$. ∎

We aim to show that, for any indecomposable $X\in G=GU_n(q)$, one can find B_1 and C_1, such that $XB_1=C_1$ where B_1, resp. C_1, is G-conjugate to a fixed element B, resp. to a fixed element C. It is well known that this is equivalent to showing that

$$\sum_{\chi\in\ \mathrm{Irr}(G)}\frac{\chi(X)\chi(B)\overline{\chi(C)}}{\chi(1)}\neq 0. \tag{17}$$

If $n\geq 7$, then Proposition 6.6 implies that we can break the sum on the left hand side of (17) into 4 sub-sums:

- $\sum^1$ involving only χ with $\chi(1) = 1$ (case (i) of Proposition 6.6),
- $\sum^2$ involving the $(q+1)^2$ irreducible Weil characters of G (case (ii) of Proposition 6.6),
- $\sum^3$ involving precisely the characters χ belonging to case (iii) of Proposition 6.6, and
- $\sum^4$ involving only χ with $\chi(1) \geq D$, where D is defined in Proposition 6.6.

Since B and C are chosen so that $\det(X)\det(B) = \det(C)$, we have $\chi(X)\chi(B)\overline{\chi(C)} = 1$ whenever $\chi(1) = 1$, and so $\sum^1 = q+1$. Thus it suffices to show

$$|\sum^2| + |\sum^3| + |\sum^4| < q + 1 \ . \tag{18}$$

Observe that $|\chi(X)| \leq \sqrt{|C_G(X)|}$; on the other hand, by the Cauchy-Schwarz inequality,

$$\sum_{\chi \in \ \mathrm{Irr}(G)} |\chi(B)| \cdot |\chi(C)| \leq \sqrt{\sum_{\chi} |\chi(B)|^2 \cdot \sum_{\chi} |\chi(C)|^2} = \sqrt{|C_G(B)| \cdot |C_G(C)|}.$$

Hence we deduce that

$$|\sum^4| \leq \tfrac{|C_G(X)| \cdot |C_G(B)| \cdot |C_G(C)|)^{1/2}}{D}. \tag{19}$$

B. Character estimates

Throughout the rest of this section, the elements B, C are chosen to be G-conjugate to elements of the form

$$\mathrm{diag}(a, J_{n-1})\,(a \in F_0) \text{ or } \mathrm{diag}(a, b, J_{n-2})\,(a, b \in F_0, (a, b) \neq (1, 1)).$$

For brevity, we refer to all such conjugates (including $\mathrm{diag}(a, J_{n-1})$) as (a, b, J)-*elements.*

Lemma 6.8 *Let $n \geq 4$ and let $g \in G := GU_n(q)$ be an (a, b, J)-element. Then $|C_G(g)| \leq (q+1)^3 q^{n-1}$. If $\alpha \in \mathbb{F}_{q^2}^\times$, then $e(g, \alpha) > 0$ for at most three values of α. In fact, if $e(g, \alpha) > 0$ for some $\alpha \in \mathbb{F}_{q^2}^\times$, then $\alpha \in F_0$ and one of the following holds.*

(i) *$e(g, \alpha) = 2$ for at most one value of α (which may depend on g). Further, $\dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g - \alpha) \cap \mathrm{Ker}(g - \alpha)) \leq 1$.*

(ii) *$e(g, \alpha) \leq 1$.*

Proof It is obvious that $e(g,\alpha)=0$ if $\alpha\notin F_0$, since all eigenvalues of g belong to F_0. In what follows we assume that $\alpha\in F_0$.

First we consider the case where g is conjugate to $\mathrm{diag}(a,J_{n-1})$ with $a\in F_0$. Then $|C_G(g)|$ is $(q+1)^2q^n$ if $a=1$ and $(q+1)^2q^{n-2}$ if $a\neq 1$. Next, $e(g,\alpha)$ equals 2 if $\alpha=a=1$, and is at most 1 otherwise. Further, $\dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-\alpha)\cap\mathrm{Ker}(g-\alpha))=1$ in the former case.

Now we consider the case where g is conjugate to $\mathrm{diag}(a,b,J_{n-2})$ with $a,b\in F_0$ but $(a,b)\neq(1,1)$. Then $|C_G(g)|$ is $(q+1)^2q^{n-2}(q^2-1)$ if $a=b\neq 1$, $(q+1)^3q^{n-1}$ if $1\in\{a,b\}$, and $(q+1)^3q^{n-3}$ if $1\neq a\neq b\neq 1$. Next, $e(g,\alpha)$ equals 2 if $\alpha=a=b\neq 1$ or if $\alpha=1\in\{a,b\}$, and is at most 1 otherwise. Further, $\dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-\alpha)\cap\mathrm{Ker}(g-\alpha))\leq 1$ in the two former cases. ■

We now estimate the characters D_α° introduced in Proposition 6.3 and the Weil characters at $g\in\{X,B,C\}$. Set

$$Q:=(q+1)(q^2-1).$$

Proposition 6.9 *Let $n\geq 5$, let $g\in G:=GU_n(q)$ be indecomposable, and let $\chi\in\ \mathrm{Irr}(G)$.*

(i) *If χ is a Weil character, then $|\chi(g)|\leq 2q/(q+1)$.*

(ii) *If $\chi=D_\alpha^\circ$ for some $\alpha\in\ \mathrm{Irr}(GU_2(q))$, then*

$$\frac{|D_\alpha^\circ(g)|}{\alpha(1)}\leq\begin{cases} f(q)/Q, & \alpha\neq 1_S,\\ 1+f(q)/Q, & \alpha=1_S,\end{cases}$$

where $f(q):=3q^3-q^2-q$.

Proof If $\chi=\zeta_{n,q}^i$ (see (16)), then $e(g,\xi^j)\leq 1$, and it can equal 1 for at most one ξ^j by Lemma 6.7. Hence $|\chi(g)|\leq 2q/(q+1)$.

Now we may assume that $\chi=D_\alpha^\circ$ for some $\alpha\in\ \mathrm{Irr}(GU_2(q))$. We begin by estimating $\omega(xg)$ for $x\in S:=GU_2(q)$, where ω is defined by (15). We distinguish the following cases.

1) $x=aI_2$ for some $a\in F_0$. Then $|\omega(xg)|=q^{2e(g,a^{-1})}$, and so by Lemma 6.7 it is 1 except possibly for one element x for which $|\omega(xg)|=q^2$.

2) x is conjugate to $\begin{pmatrix}a&1\\0&a\end{pmatrix}$ for some $a\in F_0$. Arguing as in part 1) of the proof of Proposition 5.11, we see that

$$|\omega(xg)|=q^{\dim_{\mathbb{F}_{q^2}}\mathrm{Ker}(g-a^{-1})+\dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-a^{-1})\cap\mathrm{Ker}(g-a^{-1}))}.$$

Lemma 6.7 implies that $|\omega(xg)|$ equals 1 except possibly for one value of a (giving q^2-1 elements x of S) for which $|\omega(xg)|\leq q^2$.

3) x is conjugate to $\mathrm{diag}(a,b)$ for some $a \neq b \in F_0$. Then $|\omega(xg)| = q^{e(g,a^{-1})+e(g,b^{-1})}$, and so by Lemma 6.7 it is 1 except possibly for q pairs (a,b) (giving $q^2(q-1)$ elements x) for which $|\omega(xg)| = q$.

4) x is conjugate to $\mathrm{diag}(a,a^{-q})$ for some $a \in \mathbb{F}_{q^2}^\times \setminus F_0$. Again $|\omega(xg)| = q^{e(g,a^{-1})+e(g,a^q)}$, and so by Lemma 6.7 it is 1 except possibly for one pair (a,a^{-q}) (giving $q(q+1)$ elements x) for which $|\omega(xg)| = q^2$.

First assume that the exception in 4) does not occur. Lemma 5.5 and the obvious estimate $|\alpha(x)| \leq \alpha(1)$ imply that

$$|D_\alpha(g)| \leq \frac{\alpha(1)\cdot\left(q^2\cdot q^2 + q\cdot q^2(q-1) + (|S|-q^3)\right)}{|S|} \leq \frac{\alpha(1)(3q^3-q^2-q)}{(q+1)(q^2-1)}.$$

Next assume the exception in 4) occurs. Notice that the cases (i) and (ii) in Lemma 6.7 are mutually exclusive. In particular, the exception in 4) cannot occur in conjunction with any of the exceptions in 1) – 3). Now we can use the same arguments as before and arrive at a better estimate for $|D_\alpha(g)|$.

Thus we have finished if $\alpha \neq 1_S$ or St, since in these cases $D_\alpha^\circ = D_\alpha$. We have also finished if $\alpha = 1_S$, since $|D_\alpha^\circ(g)| \leq |D_\alpha(g)| + 1$. Finally, we consider the case $\alpha = St$: now $|\alpha(x)| \leq 1$ unless $x \in Z(S)$. Since in the above estimates we used the crude bound $|\alpha(g)| \leq \alpha(1) = q$, we can easily improve the upper bound for $|D_\alpha(g)|$ by 1 to get the stated bound. ∎

Proposition 6.10 *Let $n \geq 5$, let $g \in G := GU_n(q)$ be an (a,b,J)-element, and let $\chi \in \mathrm{Irr}(G)$.*

(i) *If χ is a Weil character, then $|\chi(g)| \leq (q^2+3q-2)/(q+1)$.*

(ii) *If $\chi = D_\alpha^\circ$ for some $\alpha \in \mathrm{Irr}(GU_2(q))$, then*

$$\frac{|D_\alpha^\circ(g)|}{\alpha(1)} \leq \begin{cases} g(q)/Q, & \alpha \neq 1_S, \\ 1+g(q)/Q, & \alpha = 1_S, \end{cases}$$

where $g(q) := (7q^4+q^3-q^2-5q-2)/2$.

Proof If $\chi = \zeta_{n,q}^i$ (see (16)), then $e(g,\xi^j) \leq 2$; in fact it can equal 2 for at most one ξ^j and it can be positive for at most two ξ^j's by Lemma 6.8. Hence $|\chi(g)| \leq (q^2+3q-2)/(q+1)$.

Now we may assume that $\chi = D_\alpha^\circ$ for some $\alpha \in \mathrm{Irr}(GU_2(q))$. We begin by estimating $\omega(xg)$ for $x \in S := GU_2(q)$, where ω is defined by (15). We distinguish the following cases.

1) $x = aI_2$ for some $a \in F_0$. Then $|\omega(xg)| = q^{2e(g,a^{-1})}$, and so by Lemma 6.8 it is $\leq q^4$ for one value of a, $\leq q^2$ for two others, and 1 for the remaining $q-2$ values of a.

2) x is conjugate to $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ for some $a \in F_0$. As in the proof of Proposition 6.9,

$$|\omega(xg)| = q^{\dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(g-a^{-1}) + \dim_{\mathbb{F}_{q^2}} (\mathrm{Im}(g-a^{-1}) \cap \mathrm{Ker}(g-a^{-1})}.$$

Hence, by Lemma 6.8, $|\omega(xg)| \le q^3$ for one value of a, $\le q^2$ for two others, and is 1 for the remaining $q-2$ values of a. Each value of a gives rise to q^2-1 elements x of S.

3) x is conjugate to $\mathrm{diag}(a,b)$ for some $a \ne b \in F_0$. Then $|\omega(xg)| = q^{e(g,a^{-1})+e(g,b^{-1})}$. Following the proof of Lemma 6.8, we can check that $|\omega(xg)| \le q^3$ for one (unordered) pair (a,b), $\le q^2$ for q others, and $\le q$ for the remaining $(q+1)(q-2)/2$ pairs (a,b). Each unordered pair (a,b) gives rise to $q(q-1)$ elements x of S.

4) x is conjugate to $\mathrm{diag}(a, a^{-q})$ for some $a \in \mathbb{F}_{q^2}^\times \setminus F_0$. Again $|\omega(xg)| = q^{e(g,a^{-1})+e(g,a^q)}$, and so by Lemma 6.8 it is 1.

Thus we have shown that $|\omega(xg)| \le q^4$ for one element x, $\le q^3$ for $2q^2-q-1$ elements x, $\le q^2$ for q^3+q^2 elements x, $\le q$ for $q(q^2-1)(q-2)/2$ elements x, and is 1 for $q(q^2-2)+q(q+1)^2(q-2)/2$ elements x, when x varies over S. Lemma 5.5 and the obvious estimate $|\alpha(x)| \le \alpha(1)$ imply that

$$|D_\alpha(g)/\alpha(1)| \le \frac{7q^4+q^3-q^2-5q-2}{2(q+1)(q^2-1)}.$$

In particular, we have finished if $\alpha \ne 1_S$ or St, since in these cases $D^\circ_\alpha = D_\alpha$. We have also finished if $\alpha = 1_S$, since $|D^\circ_\alpha(g)| \le |D_\alpha(g)| + 1$. Finally, we consider the case $\alpha = St$: now $|\alpha(x)| \le 1$ unless $x \in Z(S)$. Since in the above estimates we used the crude bound $|\alpha(g)| \le \alpha(1) = q$, we can easily improve the upper bound for $|D_\alpha(g)|$ by 1 to get the stated bound. ■

C. The (b,J)- and the (a,b,J)-properties

Assume now that $n \ge 7$. We use Propositions 6.9 and 6.10 and Lemmas 6.7 and 6.8 to estimate $\sum^2$, $\sum^3$, and $\sum^4$, defined after (17), where B, C are (a,b,J)-elements.

Clearly, the degree of any of the $(q+1)^2$ (irreducible) Weil characters of G is at least $(q^n-q)/(q+1)$. Hence, by Propositions 6.9 and 6.10,

$$\begin{aligned} |\textstyle\sum^2| &\le (2q(q^2+3q-2)^2)/(q^n-q) \\ &< \begin{cases} 0.503, & \text{if } q=2 \text{ and } n \ge 9, \\ 0.235, & \text{if } q=3 \text{ and } n \ge 8, \\ 0.083, & \text{if } q=4 \text{ and } n \ge 8, \\ 0.185, & \text{if } q=5 \text{ and } n \ge 7, \\ 0.079, & \text{if } q=7 \text{ and } n \ge 7. \end{cases} \end{aligned}$$

Recall that for any $\alpha \in \mathrm{Irr}(S)$ with $S = GU_2(q)$, $D^\circ_\alpha(1) > \kappa q^{2n-1}\alpha(1)/Q$ by Lemma 6.4, where $\kappa > 1 - 1/q^{n-3}$. Also, $|D^\circ_\alpha(X)|$ and $|D^\circ_\alpha(B,C)|$ are bounded in Propositions 6.9 and 6.10. Hence

$$\begin{aligned}
|\sum\nolimits^3|/(q+1) &\leq \sum_{\alpha \in \mathrm{Irr}(S)} \frac{|D^\circ_\alpha(B)| \cdot |D^\circ_\alpha(C)| \cdot |D^\circ_\alpha(X)|}{|D^\circ_\alpha(1)|} \\
&\leq \frac{f(q)g(q)^2 \sum_{\alpha \in \mathrm{Irr}(S),\ \alpha \neq 1_S} \alpha(1)^2 + (f(q)+Q)(g(Q)+q)^2}{\kappa Q^2 q^{2n-1}} \\
&= \frac{f(q)g(q)^2(qQ-1) + (f(q)+Q)(g(q)+Q)^2}{\kappa Q^2 q^{2n-1}},
\end{aligned}$$

as $\sum_{\alpha \in \mathrm{Irr}(S)} \alpha(1)^2 = |S| = qQ$. It follows that

$$|\sum\nolimits^3| < \begin{cases} 0.267, & \text{if } q = 2 \text{ and } n \geq 9, \\ 0.148, & \text{if } q = 3 \text{ and } n \geq 8, \\ 0.036, & \text{if } q = 4 \text{ and } n \geq 8, \\ 0.292, & \text{if } q = 5 \text{ and } n \geq 7, \\ 0.107, & \text{if } q = 7 \text{ and } n \geq 7. \end{cases}$$

Note that $D > q^{n+3}(q^{n-1}-1)(q^{n-5}-1)/(q+1)(q^2-1)(q^3+1)$. Applying (19) and Lemmas 6.7 and 6.8, we get

$$\begin{aligned}
|\sum\nolimits^4| &\leq (q^{n-1}(q+1))^{1/2} q^{n-1}(q+1)^3/D \\
&< \tfrac{(q+1)^{9/2} q^{(n-9)/2}(q^2-1)(q^3+1)}{(q^{n-1}-1)(q^{n-5}-1)} \\
&< \begin{cases} 0.991, & \text{if } q = 2 \text{ and } n \geq 9, \\ 1.166, & \text{if } q = 3 \text{ and } n \geq 8, \\ 0.661, & \text{if } q = 4 \text{ and } n \geq 8, \\ 5.121, & \text{if } q = 5 \text{ and } n \geq 7, \\ 4.840, & \text{if } q = 7 \text{ and } n \geq 7. \end{cases}
\end{aligned}$$

Altogether, these estimates yield

$$|\sum\nolimits^2| + |\sum\nolimits^3| + |\sum\nolimits^4| < \begin{cases} 1.761, & \text{if } q = 2 \text{ and } n \geq 9, \\ 1.549, & \text{if } q = 3 \text{ and } n \geq 8, \\ 0.780, & \text{if } q = 4 \text{ and } n \geq 8, \\ 5.598, & \text{if } q = 5 \text{ and } n \geq 7, \\ 5.026, & \text{if } q = 7 \text{ and } n \geq 7. \end{cases}$$

Thus (see (18)) we have proved:

Proposition 6.11 *Let $X \in GU_n(q)$ be indecomposable, and assume $q \leq 7$. Assume that $n \geq 9$ if $q = 2$, $n \geq 8$ if $q = 3, 4$, and $n \geq 7$ if $q = 5, 7$. Then X has the (b, J)-property for all $b \in F_0$, and X has the (a, b, J)-property for all $a, b \in F_0$ with $(a, b) \neq (1, 1)$, $(|X|^{-1}, 1)$.*

The condition $(a,b) \neq (1,1), (|X|^{-1},1)$ is imposed so that neither of the matrices B, C is of the form $(1,1,J_{n-2})$, as required for the above calculations.

6.3 Variations of the (a,b,J)-property for $GU_n(2)$

In this section, $q=2$, $G = GU_n(2)$ and $F_0 = \langle\omega\rangle$. Define an $(a,b,J)_2$-*element* of G to be a conjugate of one of the following matrices or its inverse:

$$\mathrm{diag}(\omega^2, \omega J_2, J_{n-3}),\ \mathrm{diag}(\omega^2 J_2, J_{n-2}),\ \mathrm{diag}(\omega,\omega,\omega^2,J_{n-3}),$$

$$\mathrm{diag}(\omega,\omega,J_{n-2}),\ \mathrm{diag}(\omega,\omega^2,J_{n-2}).$$

We prove an analogue of Proposition 6.11 for $(a,b,J)_2$-elements. The main result is Proposition 6.14.

Following the proof of Lemma 6.8, one obtains:

Lemma 6.12 *Let $n \geq 4$, $q=2$, and let $g \in G := GU_n(q)$ be an $(a,b,J)_2$-element. Then $|C_G(g)| \leq (q+1)^4 q^{n-3}$. If $\alpha \in \mathbb{F}_{q^2}^\times$, then one of the following holds.*

(i) *$e(g,\alpha) = 2$ for at most one value of α (which may depend on g).*

(ii) *$e(g,\alpha) \leq 1$.*

In either case, $\dim_{\mathbb{F}_{q^2}}(\mathrm{Ker}(g-\alpha)) + \dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-\alpha) \cap \mathrm{Ker}(g-\alpha)) \leq 2$.

Proposition 6.13 *Let $n \geq 5$, let $g \in G := GU_n(2)$ be an $(a,b,J)_2$-element, and let $\chi \in \mathrm{Irr}(G)$.*

(i) *If χ is a Weil character, then $|\chi(g)| \leq 8/3$.*

(ii) *If $\chi = D_\alpha^\circ$ for some $\alpha \in \mathrm{Irr}(GU_2(q))$, then*

$$|D_\alpha^\circ(g)/\alpha(1)| \leq \begin{cases} 50/9, & \alpha \neq 1_S, \\ 59/9, & \alpha = 1_S. \end{cases}$$

Proof For (i) we use the same arguments as in the proof of Proposition 6.10(i). We may assume that $\chi = D_\alpha^\circ$ for some $\alpha \in \mathrm{Irr}(GU_2(2))$. We begin by estimating $\omega(xg)$ for $x \in S := GU_2(2)$, where ω is defined by (15). We distinguish the following cases.

1) $x = aI_2$ for some $a \in F_0$. Then $|\omega(xg)| = q^{2e(g,a^{-1})}$, and so by Lemma 6.12 it is $\leq q^4$ for one value of a, and $\leq q^2$ for the two others.

2) x is conjugate to $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ for some $a \in F_0$. Here,

$$|\omega(xg)| = q^{\dim_{\mathbb{F}_{q^2}} \mathrm{Ker}(g-a^{-1}) + \dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-a^{-1}) \cap \mathrm{Ker}(g-a^{-1}))} \leq q^2$$

by Lemma 6.12. Each value of a gives rise to 3 elements x of S.

3) x is conjugate to $\mathrm{diag}(a,b)$ for some $a \neq b \in F_0$. Then $|\omega(xg)| = q^{e(g,a^{-1})+e(g,b^{-1})}$. By Lemma 6.12, $|\omega(xg)| \leq q^3$ for two (unordered) pairs (a,b), and $\leq q^2$ for the remaining one. Each unordered pair (a,b) gives rise to 2 elements x.

Thus we have shown that $|\omega(xg)| \leq 16$ for one element x, ≤ 8 for 4 elements x, and ≤ 4 for 13 elements x, when x varies over S. Lemma 5.5 and the obvious estimate $|\alpha(x)| \leq \alpha(1)$ imply that

$$|D_\alpha(g)/\alpha(1)| \leq \frac{16 + 8 \cdot 4 + 4 \cdot 13}{18} = 50/9.$$

In particular, we have finished if $\alpha \neq St$. If $\alpha = St$ then $|\alpha(x)| \leq 1$ unless $x \in Z(S)$. Since in the above estimates we used the crude bound $|\alpha(g)| \leq \alpha(1) = q$, we can easily improve the upper bound for $|D_\alpha(g)|$ by 1 to get the stated bound. ∎

Now take B and C to be $(a,b,J)_2$-elements of G. We use Propositions 6.9 and 6.13 and Lemmas 6.7 and 6.12 to estimate $\sum^2$, $\sum^3$, and $\sum^4$ (defined after (17)). We assume that $n \geq 9$.

Clearly, the degree of any of the 9 (irreducible) Weil characters of G is at least $(2^n-2)/3$. Propositions 6.9 and 6.13 imply that $|\sum^2| \leq 256/(2^n-2) < 0.503$.

For any $\alpha \in \mathrm{Irr}(S)$ with $S = GU_2(q)$, $D^\circ_\alpha(1) > 2^{2n-1}\kappa\alpha(1)/9$ by Lemma 6.4, where $\kappa > 1 - 1/2^{n-3}$. Next, $|D^\circ_\alpha(X)|$ and $|D^\circ_\alpha(B,C)|$ are bounded in Propositions 6.9 and 6.13. Hence

$$\begin{aligned} |\sum^3|/3 &\leq \sum_{\alpha \in \mathrm{Irr}(S)} \frac{|D^\circ_\alpha(B)| \cdot |D^\circ_\alpha(C)| \cdot |D^\circ_\alpha(X)|}{|D^\circ_\alpha(1)|} \\ &\leq \frac{2 \cdot (50/9)^2 \sum_{\alpha \in \mathrm{Irr}(S),\ \alpha \neq 1_S} \alpha(1)^2 + 3 \cdot (59/9)^2}{2^{2n-1}\kappa/9} \\ &< 10605/2^{2n-1}\kappa, \end{aligned}$$

and so $|\sum^3| < 0.247$.

By (19) and Lemmas 6.7 and 6.12,

$$|\sum^4| \leq (3 \cdot 2^{n-1})^{1/2} 2^{n-3} \cdot 3^4/D < \frac{3^{17/2} 2^{(n-13)/2}}{(2^{n-1}-1)(2^{n-5}-1)} < 0.743.$$

Altogether, these estimates yield

$$|\sum^2| + |\sum^3| + |\sum^4| < 0.503 + 0.247 + 0.743 = 1.493.$$

Thus (see (18)) we have proved:

Proposition 6.14 *Let $X \in G := GU_n(2)$ be indecomposable and $n \geq 9$. For any two $(a,b,J)_2$-elements B, C with $\det(X)\det(B) = \det(C)$, there exist $B_1 \in B^G$ and $C_1 \in C^G$ such that $XB_1 = C_1$.*

6.4 Variations of the (a,b,J)-property for $GU_n(3)$

In this section, $q=3$, $G=GU_n(3)$ and $\vartheta\in F_0$ is an element of order 4. An element of G is an $(a,b,J)_3$-*element* if it is conjugate to one of the following matrices:

$$\mathrm{diag}(\vartheta J_2, J_{n-2}),\ \text{or}\ \mathrm{diag}(\vartheta,\vartheta^j,J_{n-2})\ (j\in\{1,2,3\}).$$

Our critical result about these elements is Proposition 6.17.

Following the proof of Lemma 6.8, one obtains:

Lemma 6.15 *Let $n\geq 4$, $q=3$, and let $g\in G:=GU_n(q)$ be an $(a,b,J)_3$-element. Then $|C_G(g)|\leq 2(q+1)^3q^{n-2}$. Further, if $\alpha\in\mathbb{F}_{q^2}^\times$, then one of the following holds.*

(i) *$e(g,\alpha)$ equals 2 for one value of $\alpha\in F_0$, 1 for one more value of $\alpha\in F_0$, and 0 for all the other values of α.*

(ii) *$e(g,\alpha)=1$ for at most three values of $\alpha\in F_0$ and 0 for all the others.*

In either case, $\dim_{\mathbb{F}_{q^2}}(\mathrm{Ker}(g-\alpha))+\dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-\alpha)\cap\mathrm{Ker}(g-\alpha))\leq 2$.

Proposition 6.16 *Let $n\geq 5$, let $g\in G:=GU_n(3)$ be an $(a,b,J)_3$-element, and let $\chi\in\ \mathrm{Irr}(G)$.*

(i) *If χ is a Weil character, then $|\chi(g)|\leq 7/2$.*

(ii) *If $\chi=D_\alpha^\circ$ for some $\alpha\in\ \mathrm{Irr}(GU_2(q))$, then*

$$|D_\alpha^\circ(g)/\alpha(1)|\leq\begin{cases}9, & \alpha\neq 1_S,\\ 10, & \alpha=1_S.\end{cases}$$

Proof For (i) we use the same arguments as in the proof of Proposition 6.10(i). We may assume that $\chi=D_\alpha^\circ$ for some $\alpha\in\ \mathrm{Irr}(GU_2(3))$. To estimate $\omega(xg)$ for $x\in S:=GU_2(3)$, we distinguish the following cases.

1) $x=aI_2$ for some $a\in F_0$. Then $|\omega(xg)|=q^{2e(g,a^{-1})}$, and so by Lemma 6.15 it is $\leq q^4$ for one value of a, and $\leq q^2$ for the others.

2) x is conjugate to $\begin{pmatrix}a&1\\0&a\end{pmatrix}$ for some $a\in F_0$. Lemma 6.15 implies that

$$|\omega(xg)|=q^{\dim_{\mathbb{F}_{q^2}}\mathrm{Ker}(g-a^{-1})+\dim_{\mathbb{F}_{q^2}}(\mathrm{Im}(g-a^{-1})\cap\mathrm{Ker}(g-a^{-1}))}\leq q^2.$$

Each value of a gives rise to 8 elements x of S.

3) x is conjugate to $\mathrm{diag}(a,b)$ for some $a\neq b\in F_0$. Then $|\omega(xg)|=q^{e(g,a^{-1})+e(g,b^{-1})}$. By Lemma 6.15, $|\omega(xg)|\leq q^3$ for at most one unordered pair (a,b), and $\leq q^2$ for the remaining one. Each unordered pair (a,b) gives rise to 6 elements x.

4) x is conjugate to $\mathrm{diag}(a, a^{-q})$ for some $a \in \mathbb{F}_{q^2}^\times \setminus F_0$. Again $|\omega(xg)| = q^{e(g,a^{-1})+e(g,a^q)}$, and so by Lemma 6.8 it is 1. There are 24 elements x of this kind.

Thus we have shown that $|\omega(xg)| \le 81$ for one element x, ≤ 27 for 6 elements x, ≤ 9 for 65 elements x, and ≤ 1 for 24 elements x, when x varies over S. Lemma 5.5 and the obvious estimate $|\alpha(x)| \le \alpha(1)$ imply that

$$|D_\alpha(g)/\alpha(1)| \le \frac{81 + 27 \cdot 6 + 9 \cdot 65 + 1 \cdot 24}{96} < 9.$$

In particular, we have finished if $\alpha \ne St$. If $\alpha = St$, then $|\alpha(x)| \le 1$ unless $x \in Z(S)$. Since in the above estimates we used the crude bound $|\alpha(g)| \le \alpha(1) = q$, we can easily improve the upper bound for $|D_\alpha(g)|$ by 1 to get the stated bound. ■

Now take B and C to be $(a, b, J)_3$-elements of G. We use Propositions 6.9 and 6.16 and Lemmas 6.7 and 6.15 to estimate $\sum^2$, $\sum^3$, and $\sum^4$ (defined after (17)). We assume that $n \ge 8$.

Clearly, the degree of any of the 16 (irreducible) Weil characters of G is at least $(3^n - 3)/4$. Propositions 6.9 and 6.16 imply that $|\sum^2| \le 392/(3^{n-1} - 1) < 0.180$.

For any $\alpha \in \mathrm{Irr}(S)$ with $S = GU_2(q)$, $D^\circ_\alpha(1) > 3^{2n-1}\kappa\alpha(1)/32$ by Lemma 6.4. Next, $|D^\circ_\alpha(X)|$ and $|D^\circ_\alpha(B, C)|$ are bounded in Propositions 6.9 and 6.16. Hence

$$\begin{aligned} |\sum\nolimits^3|/4 &\le \sum_{\alpha \in \mathrm{Irr}(S)} \frac{|D^\circ_\alpha(B)| \cdot |D^\circ_\alpha(C)| \cdot |D^\circ_\alpha(X)|}{|D^\circ_\alpha(1)|} \\ &\le \frac{(69/32) \cdot 9^2 \sum_{\alpha \in \mathrm{Irr}(S),\ \alpha \ne 1_S} \alpha(1)^2 + (101/32) \cdot 10^2}{3^{2n-1}\kappa/32} \\ &< 541055/3^{2n-1}\kappa, \end{aligned}$$

and so $|\sum^3| < 0.152$.

By (19) and Lemmas 6.7 and 6.15,

$$|\sum\nolimits^4| \le (4 \cdot 3^{n-1})^{1/2} 2^7 \cdot 3^{n-2}/D < \tfrac{2^{15} 3^{(n-11)/2} \cdot 7}{(3^{n-1}-1)(3^{n-5}-1)} < 0.778.$$

Altogether, these estimates yield

$$|\sum\nolimits^2| + |\sum\nolimits^3| + |\sum\nolimits^4| < 0.180 + 0.152 + 0.778 = 1.11.$$

Thus (see (18)) we have proved:

Proposition 6.17 *Let $X \in G := GU_n(3)$ be indecomposable and $n \ge 8$. For any two $(a, b, J)_3$-elements B, C with $\det(X)\det(B) = \det(C)$, there exist $B_1 \in B^G$ and $C_1 \in C^G$ such that $XB_1 = C_1$.*

6.5 Proof of Theorem 6.1

In this section we prove Theorem 6.1. Throughout, let $G = SU_n(q)$ and, following Lemma 2.4, we may assume that $q \leq 7$. As a preliminary step, we obtain further results on the (b, J)- and (a, b, J)-properties, mainly for small dimensions.

A. More on the (a, b, J)-property

Our proof of Theorem 6.1 is based on the results of the previous sections, together with detailed information on the (b, J)- and (a, b, J)-properties of unitary matrices in low dimensions, which are mostly proved computationally.

First we extend the results from the previous sections. A pair (a, b) of elements of F_0 is *relevant* for $X \in GU_n(q)$ if $(a, b) \neq (1, 1)$ nor $(|X|^{-1}, 1)$.

Proposition 6.18 *Assume $n \geq 4$, and let $X \in GU_n(q)$ be indecomposable. If $n = 4$, assume that $|X| \neq 1$. Then*

(i) *X has the (b, J)-property for all $b \in F_0$;*

(ii) *X has the (a, b, J)-property for all relevant $(a, b) \in F_0^2$, with the following exception:*

$$q = 2,\ X = \omega J_4\,(\omega^3 = 1),\ (a, b) = (\omega, 1).$$

Proof For $n \geq 7$ ($n \geq 9$ if $q = 2$, $n \geq 8$ if $q = 3, 4$), this is Proposition 6.11. For the remaining values of n it was established computationally. ∎

For $q = 2$ and 3, we must extend the variations of the (a, b, J)-property developed in Sections 6.3 and 6.4 to smaller dimensions.

Proposition 6.19 *Let $n \geq 4$, $q = 2$, let $1 \neq \omega \in \mathbb{F}_4$, and let X be an indecomposable matrix in $GU_n(2)$. There exist $B, C \in GU_n(2)$ such that $XB = C$, with the following properties:*

$\lvert X\rvert$	*B conjugate to*	*C conjugate to*
1	$\mathrm{diag}(\omega^2, \omega J_2, J_{n-3})$	$\mathrm{diag}(\omega, \omega, \omega^2, J_{n-3})$
ω	$\mathrm{diag}(\omega^2, \omega J_2, J_{n-3})$	$\mathrm{diag}(\omega, \omega^2, \omega^2, J_{n-3})$
ω	$\mathrm{diag}(\omega^2 J_2, J_{n-2})$	$\mathrm{diag}(\omega, \omega, J_{n-2})$
ω	$\mathrm{diag}(\omega J_2, J_{n-2})$	$\mathrm{diag}(\omega, \omega^2, J_{n-2})$

Proof This follows from Proposition 6.14 for $n \geq 9$ and was proved computationally for $n \leq 8$. ∎

Proposition 6.20 *Let $n \geq 4$, $q = 3$, let $\omega \in \mathbb{F}_9$ have order 4, and let X be an indecomposable matrix in $GU_n(3)$. There exist $B, C \in GU_n(3)$ such that $XB = C$, with the following properties:*

$\lvert X\rvert$	*B conjugate to*	*C conjugate to*
1	$\mathrm{diag}(\omega J_2, J_{n-2})$	$\mathrm{diag}(\omega, \omega, J_{n-2})$
ω	$\mathrm{diag}(\omega J_2, J_{n-2})$	$\mathrm{diag}(-1, \omega, J_{n-2})$
-1	$\mathrm{diag}(\omega J_2, J_{n-2})$	$\mathrm{diag}(-\omega, \omega, , J_{n-2})$

Proof This is Proposition 6.17 for $n \geq 9$, and was proved computationally for $n \leq 8$. ∎

We also need the (b, J)- or (a, b, J)-properties for various types of non-indecomposable matrices in low dimensions. These are recorded in the next ten lemmas, all established computationally.

In the statements, A_i and A_i' denote indecomposable elements of $GU_i(q)$, and we use the notation $(M_1, \ldots, M_k)$ to denote the block diagonal matrix $\mathrm{diag}(M_1, \ldots, M_k)$ lying in a natural subgroup $GU_{m_1}(q) \perp \cdots \perp GU_{m_k}(q)$ of $GU_n(q)$, where each $M_i \in GU_{m_i}(q)$ and $n = \sum m_i$. Also $|\lambda|$ denotes the order of $\lambda \in \mathbb{F}_{q^2}$.

Lemma 6.21 *Let X be an element of $GU_5(q)$ or $GU_6(q)$ of the form (A_2, A_3) or (A_3, A_3'). If $q \geq 4$ (resp. $q = 3$), assume further that none of the indecomposable blocks of X has determinant 1 (resp. $|A_3|, |A_3'| \neq 1$). Then X has the (a, b, J)-property for all relevant $a, b \in F_0$.*

Lemma 6.22 (i) *Let X be an element of $GU_8(2)$ of the form $(A_2, A_2', \omega J_4)$, $(\omega J_4, \omega J_4)$ or $(\omega J_4, \omega^2 J_4)$, where $1 \neq \omega \in \mathbb{F}_4$. Then X has the (a, b, J)-property for all relevant $a, b \in F_0$.*

(ii) *Let $X \in GU_7(2)$ be of the form (A_2, A_2', A_3) or (A_3, A_4). Then X has the (a, b, J)-property for all relevant $a, b \in F_0$.*

(iii) *Let $X \in GU_6(2)$, and assume X is not diagonal of order 3, has no Jordan block J_1, and is not conjugate to (J_2, J_2, J_2) or $(\omega I_4, \omega J_2)$ ($1 \neq \omega \in F_0$). Then X has the (a, b, J)-property for all relevant $a, b \in F_0$.*

(iv) *Let $X \in GU_5(2)$, and assume X is not diagonal of order 3, has no Jordan block J_1, and is not conjugate to (J_2, J_3) or $(\omega I_3, \omega J_2)$ ($1 \neq \omega \in F_0$). Then X has the (b, J)-property for all $b \in F_0$.*

Lemma 6.23 *Let $X = (A_3, \lambda_1, \lambda_2)$ or $(A_2, A_2', \lambda_1) \in GU_5(3)$, where $1 \neq \lambda_i \in F_0$. Then X has the (a, b, J)-property for all relevant $a, b \in F_0$, with the exception of $X = \lambda(J_2, J_2, 1)$, where $|\lambda| = 4$.*

Lemma 6.24 *Let X be an element of $GU_4(q)$ of the form (A_2, A_2'). Assume $|X| \neq 1$, and if $q \geq 4$ assume further that $|A_2|, |A_2'| \neq 1$. Then*

(i) *X has the (b, J)-property for all $b \in F_0$, with the following exceptions:*

$$\begin{array}{ll} q = 5: & X = \lambda(J_2, J_2)\,(\lambda^3 = 1, \lambda \neq 1),\ b = \lambda^2 \\ q = 2: & X = \lambda(J_2, J_2)\,(\lambda^3 = 1, \lambda \neq 1),\ b = 1, \lambda^2 \end{array}$$

(ii) *if $A_2 \neq A_2'$, then X has the (a, b, J)-property for all relevant $a, b \in F_0$, with the following exceptions:*

$$\begin{array}{ll} q = 3: & X = (J_2,\ \lambda J_2)\,(|\lambda| = 4) \\ q = 2: & X = (J_2,\ \lambda J_2)\,(|\lambda| = 3) \end{array}$$

(iii) *if $q = 5$ and $A_2 = A_2'$, then X has the (a, b, J)-property for all relevant $a, b \in F_0$, with the following exceptions:*

$A_2 = \lambda J_2$: $(\lvert\lambda\rvert = 6)$	$(a,b) = (1,\alpha)\,(\alpha \neq -1, \lambda^5),\ (\lambda^2, \beta)\,(\beta \neq -1, \lambda)$, $(-1,1), (\lambda,1), (\lambda^4, \lambda^4), (\lambda^4, \lambda^2), (\lambda^5, 1)$
$A_2 = \lambda^2 J_2$: $(\lvert\lambda\rvert = 6)$	$(a,b) = (1,\alpha)\,(\alpha \neq \lambda^2),\ (\lambda^4, \beta)\,(\beta \neq \lambda^4)$, $(-1,1), (-1,-1), (-1, \lambda^5), (\lambda^5, 1), (\lambda^5, \lambda^5), (\lambda^5, \lambda)$, $(\lambda^2, \lambda^2), (\lambda^2, \lambda^4), (\lambda, 1), (\lambda, -1), (\lambda, \lambda)$
$A_2 = \mathrm{diag}(\omega, \omega^{-5})$: $(\lvert\omega\rvert = 24)$	$(a,b) = (\alpha,1)\,(\alpha \neq \omega^4),\ (1, \omega^{16}), (1, \omega^{20})$, $(\omega^4, \omega^4), (\omega^4, \omega^{20}), (\omega^8, \omega^4), (\omega^8, \omega^8)$
$A_2 = \mathrm{diag}(\omega^2, \omega^{-10})$: $(\lvert\omega\rvert = 24)$	$(a,b) = (\alpha,1)\,(\alpha \neq \omega^8),\ (1, \omega^8), (1, \omega^{16})$, $(\omega^8, \omega^8), (\omega^8, \omega^{16}), (\omega^{16}, \omega^8), (\omega^{16}, \omega^{16})$

Let X be a block diagonal matrix of the form $(X_1, X_2, X_3, \ldots)$; a *sub-block* matrix of X is a block diagonal matrix of the form $(X_{i_1}, X_{i_2}, \ldots)$, where $i_1 < i_2 < \cdots$; it is a *proper* sub-block matrix if it is not equal to X.

Lemma 6.25 *Let X be an element of $GU_6(q)$ of the form (A_2, A_2', A_2'').*

(i) *If $q \leq 3$ then X has the (a, b, J)-property for all relevant $a, b \in F_0$, except for $X = (J_2, J_2, J_2)$ and $q = 2$.*

(ii) *If $q \geq 4$, assume further that no proper sub-block matrix of X has determinant 1. Then either X, or one of the sub-block matrices (A_2, A_2'), (A_2, A_2''), (A_2', A_2''), has the (a, b, J)-property for all relevant $a, b \in F_0$.*

Lemma 6.26 *Let $X = (A_3, \lambda) \in GU_4(q)$, where $1 \neq \lambda \in F_0$. Assume that $|X| \neq 1$, and also, if $q \geq 3$, that $|A_3| \neq 1$. Then*

(i) *X has the (b, J)-property for all $b \in F_0$;*

(ii) *if $q \neq 2$, then X has the (a, b, J)-property for all relevant $a, b \in F_0$, except when $X = (\lambda J_3, \lambda)$ with $|\lambda| = q + 1$;*

(iii) *if $q = 5$ and $X = (\lambda J_3, \lambda)$ with $|\lambda| = q + 1$, then X has the (a, b, J)-property for $(a, b) = (\lambda, 1)$.*

Lemma 6.27 *Let $X = (A_2, \lambda_1, \lambda_2) \in GU_4(q)$, where $1 \neq \lambda_i \in F_0$. Assume that $|X| \neq 1$, and also, if $q \geq 4$, that no sub-block matrix of X has determinant 1. Then X has the (b, J)-property for all $b \in F_0$, with the following exceptions:*

$$\begin{array}{l} q = 7: \ X = (\lambda J_2, \lambda, \lambda) \, (|\lambda| = 8), \ b = \pm 1, \lambda^5, \lambda^7 \\ q = 5: \ X = (\lambda J_2, \lambda, \lambda) \, (|\lambda| = 6), \ b = \pm 1, \lambda^2, \lambda^5 \\ q = 4: \ X = (\lambda J_2, \lambda, \lambda) \, (|\lambda| = 5), \ b = 1, \lambda, \lambda^2, \lambda^4 \end{array}$$

Lemma 6.28 *Let $X \in GU_3(q)$ be indecomposable, and if $q \neq 2$ assume $|X| \neq 1$. Then X has the (b, J)-property for all $b \in F_0$, with the following exceptions:*

$$\begin{array}{l} q = 3, 5, 7: \ X = -J_3, \ b = \pm 1 \\ q = 2: \ X = \lambda J_3 \, (\lambda \in F_0), \ b = 1 \end{array}$$

Lemma 6.29 *Let $q = 2$ or 3, and let $X = (A_2, \lambda) \in GU_3(q)$, where $1 \neq \lambda \in F_0$.*

(i) *X has the (b, J)-property for all $b \in F_0$, with the following exceptions:*

$$\begin{array}{l} q = 2: \ X = (\mu J_2, \lambda) \, (\mu, \lambda \in F_0) \\ q = 3: \ X = (\pm \lambda J_2, \lambda) \, (|\lambda| = 4). \end{array}$$

Moreover, for $q = 2$: $(\lambda J_2, \lambda)$ is a commutator in $SU_3(2)$; (J_2, λ) has the (b, J)-property for $b = \lambda$; and $(\lambda^2 J_2, \lambda)$ has the (b, J)-property for $b = \lambda^2$.

(ii) *Suppose $q = 3$ and $X = (\pm \lambda J_2, \lambda)$ $(|\lambda| = 4)$. Then X has the (a, b, J)-property for the following (a, b):*

$$\begin{array}{l} (\lambda J_2, \lambda): \ (a, b) = (\pm 1, \lambda), (\pm \lambda, -\lambda) \\ (-\lambda J_2, \lambda): \ (a, b) = (\pm 1, -\lambda), (\pm \lambda, \lambda). \end{array}$$

Lemma 6.30 *Let $X \in GU_2(q)$, and assume that $q \neq 2$, that X is not a scalar matrix, and, if $q \geq 4$, that $|X| \neq 1$. If $b \in F_0$ and $b \notin \{1, |X|^{-1}\}$, then X has the (b, J)-property, with the following exceptions:*

$$\begin{array}{ll} q \geq 4: & X = \lambda J_2 \, (\lambda \in F_0), \ b = \lambda^{-1} \\ q = 3: & X = \lambda J_2 \, (|\lambda| = 4), \ b = \lambda^{-1} \\ & X = -J_2, \ b = -1 \\ & X = J_2, \ \text{all } b \end{array}$$

B. The proof of Theorem 6.1

Let $G = SU_n(q)$ with $q \leq 7$ and let $V = V_n(q^2)$ be the natural module for G. In view of Lemma 3.1, we assume that $n \geq 5$, and also that $n \geq 7$ if $q = 3$ and $n \geq 8$ if $q = 2$.

By Lemma 2.9 it suffices to prove that unbreakable elements are commutators. Thus we assume that

$$X \text{ is an unbreakable element of } G = SU_n(q) = SU(V)$$

and show that X is a commutator in G.

Recall that $(M_1, \ldots, M_k)$ denotes the block diagonal matrix $\mathrm{diag}(M_1, \ldots, M_k)$ lying in a natural subgroup $GU_{m_1}(q) \perp \cdots \perp GU_{m_k}(q)$ of $GU_n(q)$, where each $M_i \in GU_{m_i}(q)$ and $\sum m_i = n$.

Lemma 6.31 *If $X \in SU_n(q)$ is unbreakable, then*

$$X = (Z, Y_1, \ldots, Y_k, \lambda_1, \ldots, \lambda_l),$$

where $k \geq 0$, $l \geq 0$, and the following hold:

(1) *$Z = \emptyset$, A_2, A_3, (A_2, A_2') or ωJ_4 ($q = 2$, $1 \neq \omega \in F_0$), where A_i, A_i' denote indecomposable $i \times i$ matrices in $GU_i(q)$;*

(2) *each $Y_i \in GU_{n_i}(q)$ with $n_i \geq 4$, and Y_i has the (a, b, J)-property for all $a, b \in F_0$ which are relevant for Y_i;*

(3) *$1 \neq \lambda_i \in F_0$ for all i.*

Proof Write

$$X = (A_2^{(1)}, \ldots, A_2^{(a_2)}, A_3^{(1)}, \ldots, A_3^{(a_3)}, \ldots, A_k^{(1)}, \ldots, A_k^{(a_k)}, \lambda_1, \ldots, \lambda_l),$$

where each $A_i^{(j)} \in GU_i(q)$ is indecomposable, each $a_j \geq 0$, and $\lambda_i \in F_0$; note that $\lambda_i \neq 1$ as Z is unbreakable.

By 6.18 and 6.21, each sub-matrix $A_m^{(i)}$ with $m \geq 4$ (except for ωJ_4 with $q = 2$), and each sub-matrix $(A_2^{(i)}, A_3^{(j)})$ or $(A_3^{(i)}, A_3^{(j)})$ has the (a, b, J)-property for all relevant $a, b \in F_0$ (these sub-matrices satisfy the relevant determinant conditions by the unbreakability assumption on X).

By 6.25, for any i, j, k, either $(A_2^{(i)}, A_2^{(j)})$ or $(A_2^{(i)}, A_2^{(j)}, A_2^{(k)})$ has the (a, b, J)-property.

By 6.22, sub-matrices $(A_2, \omega J_4)$ in $GU_6(2)$, $(A_3, \omega J_4)$ in $GU_7(2)$, and $(\omega J_4, \omega J_4)$ or $(\omega J_4, \omega^2 J_4)$ in $GU_8(2)$, have the (a, b, J)-property for all relevant a, b.

Relabelling the sub-matrices of X as as Y_i, we obtain the statement. ■

Lemma 6.32 *Let $X = (Z, Y_1, \ldots, Y_k, \lambda_1, \ldots, \lambda_l)$ as in Lemma* 6.31. *Suppose that $k \geq 1$, and also that either $Z = \emptyset$, or $Z \neq \emptyset$ and Z has the (b, J)-property for some $b \in F_0$. Write $z = |Z|$ (if $Z \neq \emptyset$) and $y_i = |Y_i|$ for each i.*

For any $a_i \in F_0 \backslash \{1\}$ $(1 \leq i \leq k)$, there exist $B, C \in GU_n(q)$ with the following properties:

(i) *$XB = C$;*

(ii) *B and C are G-conjugate;*

(iii) *$|B| = |C| = a_1 \cdots a_k f$, where f is a polynomial in z, b, y_i, λ_i (just in y_i, λ_i if $Z = \emptyset$).*

Proof Let A^{con} denote a conjugate of $A \in GU_d(q)$. First assume $Z \neq \emptyset$. By assumption Z has the (b, J)-property; and as $a_i \neq 1$, each Y_i has the (λ, a_i, J)-property for all $\lambda \in F_0$. Hence we may write

$$\begin{aligned}
&Z\,(b, J)^{con} = (zb, J)^{con},\\
&Y_1\,(zb, a_1, J)^{con} = (y_1 zb, a_1, J)^{con},\\
&Y_2\,(y_1 zb, a_2, J)^{con} = (y_2 y_1 zb, a_2, J)^{con},\\
&\cdots\\
&Y_k\,(y_{k-1} \cdots y_1 zb, a_k, J)^{con} = (y_k \cdots y_1 zb, a_k, J)^{con},\\
&\lambda_1\,(y_k \cdots y_1 zb) = (\lambda_1 y_k \cdots y_1 zb),\\
&\lambda_2\,(\lambda_1 y_k \cdots y_1 zb) = (\lambda_2 \lambda_1 y_k \cdots y_1 zb),\\
&\cdots\\
&\lambda_l\,(\lambda_{l-1} \cdots \lambda_1 y_k \cdots y_1 zb) = (\lambda_l \cdots \lambda_1 y_k \cdots y_1 zb) = (b)
\end{aligned}$$

where each J denotes a Jordan block of the appropriate size. Hence $XB = C$, where $B, C \in GU_n(q)$ are both conjugates of the block diagonal matrix

$$(b,\ zb,\ y_1 zb,\ \ldots,\ y_k \cdots y_1 zb,\ \lambda_1 y_k \cdots y_1 zb,\ \ldots,\ \lambda_{l-1} \cdots \lambda_1 y_k \cdots y_1 zb,$$

$$a_1, \ldots, a_k,\ J, \ldots, J).$$

Since B is centralized by elements of arbitrary determinant, it is conjugate to C in $G = SU_n(q)$. This proves (i) and (ii), and (iii) is clear.

Finally, when $Z = \emptyset$ we argue as above, but omit the line $Z\,(b, J)^{con} = (zb, J)^{con}$ and take $z = 1$. ∎

Lemma 6.33 *Let $X = (Z, Y_1, \ldots, Y_k, \lambda_1, \ldots, \lambda_l)$ as in Lemma* 6.31. *Assume that $k \geq 2$ and that either $Z = \emptyset$, or $Z \neq \emptyset$ and Z has the (b, J)-property for some $b \in F_0$. Then X is a commutator in $G = SU_n(q)$.*

Proof Choose any $a_3, \ldots, a_k \in F_0 \backslash \{1\}$ and write $\lambda = a_3 \cdots a_k f$, where f is as in 6.32(iii). Then there exist $a_1, a_2 \in F_0 \backslash \{1\}$ such that $a_1 a_2 = \lambda^{-1}$.

Thus, if B, C are as in 6.32, then $|B| = |C| = 1$, and so $B, C \in G$. As B, C are G-conjugate, say $C = B^g$ with $g \in G$, it follows that

$$X = CB^{-1} = B^g B^{-1} = [g, B^{-1}],$$

a commutator in G. ■

Lemma 6.34 *Let $X = (Z, Y_1, \ldots, Y_k, \lambda_1, \ldots, \lambda_l)$ as in Lemma 6.31. Assume that $k \geq 2$, $Z \neq \emptyset$, and Z does not have the (b, J)-property for any $b \in F_0$. Then X is a commutator in $G = SU_n(q)$.*

Proof Now Z is as in 6.31(i). By assumption Z does not have the (b, J)-property for any $b \in F_0$, and so by 6.30, 6.28, 6.24(i) and 6.18(i), one of the following holds:

$$q = 2: \ Z = \lambda J_2 \, (\lambda \in F_0)$$
$$q = 3: \ Z = J_2$$

If $l \geq 1$ then by 6.29(i), either (Z, λ_1) has the (b, J)-property for some $b \in F_0$, or $q = 2$ and $(Z, \lambda_1) = (\lambda_1 J_2, \lambda_1)$. In the former case the conclusion follows from 6.33 if we replace Z by (Z, λ_1); and in the latter case $(Z, \lambda_1) = (\lambda_1 J_2, \lambda_1)$ is a commutator in $SU_3(2)$ by 6.29(i), and X is conjugate to $(Z, \lambda_1, Y_1, \ldots, Y_k, \lambda_2, \ldots, \lambda_l) \in SU_3(2) \times SU_{n-3}(2) < G$, so X is breakable, a contradiction. Hence we may assume that $l = 0$.

Consider now the case where $q = 2$, so that $Z = \lambda J_2$. Since X is unbreakable, one of the following must hold, where $\omega \in F_0$ and $\omega \neq 1$:

(a) $X = (J_2, Y_1, Y_2)$ $(|Y_1| = \omega, \, |Y_2| = \omega^2)$

(b) $X = (J_2, Y_1, Y_2, Y_3)$ $(|Y_1| = |Y_2| = |Y_3| = \omega)$

(c) $X = (\omega^2 J_2, Y_1, Y_2)$ $(|Y_1| = |Y_2| = \omega)$.

Assume first that every Y_i is indecomposable. We argue in similar fashion to the proof of 6.32, but using the special properties of Y_1 given by 6.19 instead of the (a, b, J)-property. Let A^{con} denote a conjugate of $A \in GU_d(q)$.

First consider case (a). Using 6.19 for Y_1 and the (a, b, J)-property for Y_2, write

$$J_2 \, (\omega, \omega) = \omega J_2,$$
$$Y_1 \, (\omega J_2, \omega^2, J)^{con} = (\omega^2, \omega^2, \omega, J)^{con},$$
$$Y_2 \, (\omega, \omega^2, J)^{con} = (\omega, \omega, J)^{con}.$$

Then $XB = C$ where $B, C \in GU_n(2)$ are both conjugate to

$$(\omega, \omega, \omega, \omega^2, \omega^2, \omega J_2, J, J).$$

This has determinant 1, so $B, C \in G = SU_n(2)$, and hence, writing $C = B^g$ with $g \in G$, we have $X = B^g B^{-1} = [g, B^{-1}]$, a commutator in G.

For case (b), we argue similarly: write

$$\begin{array}{l} J_2\,(\omega,\omega) = \omega J_2, \\ Y_1\,(\omega J_2, \omega^2, J)^{con} = (\omega^2, \omega^2, \omega, J)^{con}, \\ Y_2\,(\omega^2, \omega^2, J)^{con} = (1, \omega^2, J)^{con}, \\ Y_3\,(1, \omega^2, J)^{con} = (\omega, \omega^2, J)^{con}. \end{array}$$

Then $XB = C$ where $B, C \in GU_n(2)$ are both conjugate to

$$(\omega, \omega, \omega^2, \omega^2, \omega^2, \omega^2, 1, \omega J_2, J, J, J).$$

This has determinant 1, so again $B, C \in G$ and X is a commutator in G.

For case (c), write

$$\begin{array}{l} \omega^2 J_2\,(\omega^2, \omega^2) = \omega J_2, \\ Y_1\,(\omega J_2, J)^{con} = (\omega, \omega^2, J)^{con}, \\ Y_2\,(\omega, \omega^2, J)^{con} = (\omega^2, \omega^2, J)^{con}. \end{array}$$

Then $XB = C$ where $B, C \in GU_n(2)$ are both conjugate to

$$(\omega, \omega^2, \omega^2, \omega^2, \omega J_2, J, J).$$

Again this has determinant 1, so X is a commutator in G.

This completes the argument for $q = 2$, assuming that all the Y_i are indecomposable. Finally, suppose one of the Y_i, say Y_1, is not indecomposable. Then from the proof of 6.31, we see that Y_1 is of the form (A_2, A_2'), (A_2, A_3), (A_2, A_4), (A_3, A_3'), (A_3, A_4), (A_2, A_2', A_2'') or (A_4, A_4'), where $A_4 = \omega^i J_4$, $A_4' = \omega^j J_4$.

In the first three cases, we replace Y_1 by $(Z, Y_1) \in GU_6(2)$, $GU_7(2)$ or $GU_8(2)$; then $X = (Y_1, Y_2)$ or (Y_1, Y_2, Y_3), and Y_1 has the (a, b, J)-property for all relevant a, b by 6.22, so the conclusion follows from 6.33. In the fourth and fifth cases, we replace Z by A_3 and Y_1 by (Z, A_3') or (Z, A_4) (which has the (a, b, J)-property by 6.21, 6.22(iii)), and apply 6.33. In the sixth case, X is breakable. Finally, in the last case, we replace Z by $\omega^i J_4$ and Y_1 by $(Z, \omega^j J_4)$ and apply 6.33.

Now consider the case where $q = 3$, so that $Z = J_2$. Since X is unbreakable, one of the following must hold, where $\lambda \in F_0$ has order 4:

(a) $X = (J_2, Y_1, Y_2)$ ($|Y_1| = \mu$, $|Y_2| = \mu^{-1}$, $1 \neq \mu \in F_0$)

(b) $X = (J_2, Y_1, Y_2, Y_3)$ ($|Y_1| = |Y_2| = \lambda$, $|Y_3| = -1$)

(c) $X = (J_2, Y_1, Y_2, Y_3, Y_4)$ ($|Y_i| = \lambda$ for all i).

Assume first that every Y_i is indecomposable. First consider case (a). If $|\mu| = 4$, then using 6.20 for Y_1 and the (a, b, J)-property for Y_2, we write

$$\begin{array}{l} J_2\,(\mu, \mu) = \mu J_2, \\ Y_1\,(\mu J_2, J)^{con} = (-1, \mu, J)^{con}, \\ Y_2\,(-1, -1, J)^{con} = (-1, \mu, J)^{con}. \end{array}$$

Then $XB = C$ where $B, C \in GU_n(3)$ are both conjugate to

$$(\mu, \mu, -1, -1, \mu J_2, J, J).$$

This has determinant 1, so $B, C \in G = SU_n(3)$, and we see that X is a commutator in G as above. If $\mu = -1$, write instead

$$\begin{aligned} &J_2\,(\lambda, \lambda) = \lambda J_2, \\ &Y_1\,(\lambda J_2, J)^{con} = (-\lambda, \lambda, J)^{con}, \\ &Y_2\,(-\lambda, \lambda, J)^{con} = (\lambda, \lambda, J)^{con}. \end{aligned}$$

Then $XB = C$ where B, C are both conjugate to $(\lambda, \lambda, \lambda, -\lambda, \lambda J_2, J, J)$, of determinant 1, so again X is a commutator in G.

Now consider (b). Write

$$\begin{aligned} &J_2\,(\lambda, \lambda) = \lambda J_2, \\ &Y_1\,(\lambda J_2, J)^{con} = (-1, \lambda, J)^{con}, \\ &Y_2\,(-1, -1, J)^{con} = (-1, -\lambda, J)^{con} \\ &Y_3\,(-\lambda, \lambda, J)^{con} = (\lambda, \lambda, J)^{con}. \end{aligned}$$

Then $XB = C$ where B, C are both conjugate to

$$(\lambda, \lambda, \lambda, -\lambda, -1, -1, \lambda J_2, J, J, J),$$

of determinant 1, so again X is a commutator in G.

For case (c), write

$$\begin{aligned} &J_2\,(\lambda, \lambda) = \lambda J_2, \\ &Y_1\,(\lambda J_2, J)^{con} = (-1, \lambda, J)^{con}, \\ &Y_2\,(-1, \lambda, J)^{con} = (-\lambda, \lambda, J)^{con} \\ &Y_3\,(-\lambda, \lambda, J)^{con} = (1, \lambda, J)^{con} \\ &Y_4\,(1, \lambda, J)^{con} = (\lambda, \lambda, J)^{con}. \end{aligned}$$

Then $XB = C$ where B, C are both conjugate to

$$(\lambda, \lambda, \lambda, \lambda, \lambda, -\lambda, 1, -1, \lambda J_2, J, J, J, J).$$

This has determinant 1, so once again X is a commutator in G.

This completes the argument for $q = 3$, assuming that all the Y_i are indecomposable. Finally, suppose one of the Y_i, say Y_1, is not indecomposable. The proof of 6.31 implies that Y_1 is of the form (A_2, A_2'), (A_2, A_3), (A_3, A_3') or (A_2, A_2', A_2''). In the first case we replace Y_1 by $(Z, Y_1) \in GU_6(3)$, as this has the (a, b, J)-property by 6.25(i); then the conclusion follows from 6.33. In the second case, $(Z, Y_1) = (J_2, A_2, A_3)$. If (J_2, A_2) has the (a, b, J)-property for all relevant a, b then replace Z by A_3, Y_1 by (J_2, A_2) and apply 6.33; otherwise, by 6.24 $A_2 = \lambda J_2$ with $|\lambda| = 4$, and we replace Z by λJ_2,

Y_1 by (J_2, A_3) (which has the (a, b, J)-property by 6.21), and apply 6.33. Similarly in the third case we replace Z by A_3 and Y_1 by (J_2, A_3'). In the last case, $A_2 \neq J_2$ (otherwise X would be breakable), and we replace Z by A_2 and Y_1 by (J_2, A_2', A_2''), which has the (a, b, J)-property by 6.25.

This completes the proof of the lemma. ■

The last two lemmas give the following:

Corollary 6.35 *If $X = (Z, Y_1, \ldots, Y_k, \lambda_1, \ldots, \lambda_l)$ as in Lemma 6.31, and $k \geq 2$, then X is a commutator in $G = SU_n(q)$.*

Hence we may now assume that X is as in Lemma 6.31 with $k \leq 1$.

Lemma 6.36 *Let $X = (Z, Y_1, \lambda_1, \ldots, \lambda_l)$ as in Lemma 6.31 (so with $k = 1$). If either $Z = \emptyset$, or Z has the (b, J)-property for at least three values of $b \in F_0$, then X is a commutator in G.*

Proof We argue as in the proof of 6.32. Write $z = |Z|$ if $Z \neq \emptyset$, and $z = 1$ otherwise; and let $y_1 = |Y_1|$. By hypothesis, if $Z \neq \emptyset$ then we can find $b \in F_0$ such that Z has the (b, J)-property and also $bz, y_1bz \neq 1$. Then Y_1 has the (zb, a, J)-property for any $a \in F_0$. Hence we can write (omitting the first line and choosing any $b \neq 1, y_1^{-1}$ if $Z = \emptyset$):

$$\begin{aligned}
&Z\,(b, J)^{con} = (zb, J)^{con},\\
&Y_1\,(zb, a, J)^{con} = (y_1zb, a, J)^{con},\\
&\lambda_1\,(y_1zb) = (\lambda_1y_1zb),\\
&\cdots\\
&\lambda_l\,(\lambda_{l-1}\cdots\lambda_1y_1zb) = (b).
\end{aligned}$$

Hence $XB = C$, where $B, C \in GU_n(q)$ are both conjugates of

$$(a,\ b,\ zb,\ y_1zb,\ \lambda_1y_1zb,\ \ldots,\ \lambda_{l-1}\cdots\lambda_1y_1zb,\ J,\ J).$$

We can choose $a \in F_0$ such that $|B| = 1$. Then $B, C \in G$ and are G-conjugate, so X is a commutator in G.

■

Lemma 6.37 *Let $X = (Z, Y_1, \lambda_1, \ldots, \lambda_l)$ as in Lemma 6.31, and suppose that $q \geq 4$. Then X is a commutator in G.*

Proof If $Z = \emptyset$ then this statement follows from the previous lemma, so assume $Z \neq \emptyset$. Recall from 6.31 that $Z = A_2$, A_3 or (A_2, A_2'). If $q \geq 5$ then by 6.30, 6.28 and 6.24, Z has the (b, J)-property for at least three values of $b \in F_0$, and the conclusion again follows from 6.36.

Now assume that $q = 4$. We may also assume that Z has the (b, J)-property for fewer than three values of b, whence by 6.30, 6.28 and 6.24 we have $Z = \lambda J_2$ with $|\lambda| = 5$. By 6.30, Z has the (b, J)-property for $b = \lambda$ or λ^2. Since $|Z| = z = \lambda^2$, $bz \neq 1$ for both possible values of b, and hence we can choose $b \in \{\lambda, \lambda^2\}$ such that $bz, y_1 bz \neq 1$. Now the proof of 6.36 gives the conclusion. ∎

Lemma 6.38 *Let $X = (Z, Y_1, \lambda_1, \ldots, \lambda_l)$ as in Lemma 6.31, and suppose that $q = 3$. Then X is a commutator in G.*

Proof As in the previous proof, we can assume that Z has the (b, J)-property for fewer than three values of b, whence by 6.30, 6.28 and 6.24 we have $Z = A_2$ or $-J_3$.

If $l \geq 2$ then, by 6.27 and 6.26, either (Z, λ_1) or $(Z, \lambda_1, \lambda_2)$ has the (b, J)-property for all $b \in F_0$, so we replace Z by this matrix and apply 6.36.

Now suppose that $l = 1$. If (Z, λ_1) has the (b, J)-property for all b, then we have finished as before. Otherwise, 6.29 implies that $(Z, \lambda_1) = (\lambda J_2, \pm\lambda)$ for some $\lambda \in F_0$ with $|\lambda| = 4$. If $(Z, \lambda_1) = (\lambda J_2, \lambda)$ then this has the (a, b, J)-property for $(a, b) = (-1, \lambda)$ by 6.29, so for any $a \in F_0$ we write

$$\begin{aligned} (Z, \lambda_1)\,(-1, \lambda, 1)^{con} &= (\lambda, \lambda, 1)^{con} \\ Y_1\,(\lambda, a, J)^{con} &= (-1, a, J)^{con} \end{aligned}$$

and hence $XB = C$ where B, C are conjugate to $(-1, 1, \lambda, \lambda, a, J)$. Taking $a = 1$ we have $|B| = 1$, so X is a commutator in G. For $(Z, \lambda_1) = (\lambda J_2, -\lambda)$ we argue in the same way, this time using the (a, b)-property for $(a, b) = (1, \lambda)$.

Now assume that $l = 0$, so that $X = (Z, Y_1)$ with $Z = A_2$ or $-J_3$. If $Z \neq J_2$ then, by 6.30 and 6.28, Z has the (λ, J)-property for some λ of order 4 with $\lambda \neq z^{-1}$ (where $z = |Z|$). We write

$$\begin{aligned} Z\,(\lambda, 1)^{con} &= (z\lambda, 1)^{con} \\ Y_1\,(z\lambda, a, J)^{con} &= (\lambda, a, J)^{con} \end{aligned}$$

so that $XB = C$ with B, C conjugate to $(\lambda, z\lambda, a, 1, J)$, and taking $a = -z^{-1}$ we have $|B| = 1$, so X is a commutator in G.

Finally, assume that $Z = J_2$, so $X = (J_2, Y_1)$. Using 6.20, we choose $\lambda \in F_0$ of order 4 and write

$$\begin{aligned} J_2\,(\lambda, \lambda)^{con} &= \lambda J_2^{con} \\ Y_1\,(\lambda J_2, J)^{con} &= (\lambda, \lambda, J)^{con} \end{aligned}$$

so that $XB = C$ with B, C conjugate to $(\lambda, \lambda, \lambda J_2, J)$, of determinant 1, so X is a commutator in G. ∎

Lemma 6.39 *Let $X = (Z, Y_1, \lambda_1, \dots, \lambda_l)$ as in Lemma* 6.31*, and suppose that $q = 2$. Then X is a commutator in G.*

Proof If Z has the (b, J)-property for all $b \in F_0$, then the conclusion follows from 6.36, so assume this is not the case. Then 6.28 and 6.24 imply that $Z = \lambda J_2$, λJ_3 or $\lambda(J_2, J_2)$ for some $\lambda \in F_0$ (with $\lambda \neq 1$ in the last case).

Suppose $Z = \lambda J_3$ or $\lambda(J_2, J_2)$. If $l \geq 1$ then (Z, λ_1) has the (b, J)-property for all b by 6.22(iv) and 6.26, so we replace Z by this and apply 6.36. If $l = 0$ we argue in the usual way: $Z = \lambda J_3$ has the (b, J)-property for some $b \neq 1$ by 6.28, and we write

$$\begin{aligned} &Z\,(b, J)^{con} = (b, J)^{con} \\ &Y_1\,(b, b, J)^{con} = (b, b, J)^{con}; \end{aligned}$$

$Z = \lambda(J_2, J_2)$ has the (λ, J)-property by 6.24, and we write

$$\begin{aligned} &Z\,(\lambda, J)^{con} = (\lambda^2, J)^{con} \\ &Y_1\,(\lambda^2, 1, J)^{con} = (\lambda, 1, J)^{con}. \end{aligned}$$

It follows that X is a commutator in both cases in the usual way.

Now suppose $Z = \lambda J_2$. If $l \geq 2$ then $(Z, \lambda_1, \lambda_2)$ has the (b, J)-property for all b by 6.27, and the conclusion follows using 6.36. If $l = 1$ then, by 6.29, writing $Z' = (Z, \lambda_1)$, either $Z' = \lambda(J_2, 1)$ or $|Z'| = \mu$ and Z' has the (μ, J)-property for some $\mu \neq 1$. In the first case, Z' is a commutator in $SU_3(2)$ by 6.29(i), and $X \in SU_3(2) \times SU_{n-3}(2)$ is breakable, a contradiction. In the second case we write

$$\begin{aligned} &Z'\,(\mu, J)^{con} = (\mu^2, J)^{con} \\ &Y_1\,(\mu^2, 1, J)^{con} = (\mu, 1, J)^{con}, \end{aligned}$$

from which it follows that X is a commutator in the usual way.

Finally, assume $l = 0$, so that $X = (\lambda J_2, Y_1)$. If $\lambda = 1$, pick $1 \neq \omega \in F_0$ and use 6.19 to write

$$\begin{aligned} &J_2\,(\omega, \omega) = \omega J_2 \\ &Y_1\,(\omega J_2, \omega^2, J)^{con} = (\omega, \omega, \omega^2, J)^{con}; \end{aligned}$$

if $\lambda \neq 1$, use 6.19 to write

$$\begin{aligned} &\lambda J_2\,(\lambda, \lambda) = \lambda^2 J_2 \\ &Y_1\,(\lambda^2 J_2, J)^{con} = (\lambda, \lambda, J)^{con}. \end{aligned}$$

In either case it follows as usual that X is a commutator in G. ∎

The last three lemmas imply:

Corollary 6.40 *If $X = (Z, Y_1, \lambda_1, \ldots, \lambda_l)$ as in* 6.31 *(with $k = 1$), then X is a commutator in $G = SU_n(q)$.*

It remains to deal with the case where $k = 0$, so

$$X = (Z,\ \lambda_1, \ldots, \lambda_l) \tag{20}$$

where Z is one of $\emptyset$, A_2, A_3, (A_2, A_2') or ωJ_4 $(q = 2)$ and $1 \neq \lambda_i \in F_0$.

Proposition 6.41 *If $X = (Z,\ \lambda_1, \ldots, \lambda_l)$ as in* (20)*, and $q = 2$ or* 3*, then X is a commutator in G.*

Proof First suppose $q = 2$. If X has a sub-matrix (ω, ω, ω) $(1 \neq \omega \in F_0)$, then this is a commutator in $SU_3(2)$, and so $X \in SU_3(2) \times SU_{n-3}(2)$ is breakable, a contradiction. Thus no three of the λ_i are equal, and none is equal to 1. It follows that $l \leq 4$. Since $n \geq 8$, we deduce that $l = 4$ and $n = 8$, and moreover the λ_i must be $\omega, \omega, \omega^2, \omega^2$ in some order. But these have product 1, hence $|Z| = 1$ and $X \in SU_4(2) \times SU_4(2)$ is breakable, a contradiction.

Now assume $q = 3$ and let λ denote either of the elements in F_0 of order 4. As $n \geq 7$ by assumption, $l \geq 3$. If $Z = A_3$ or (A_2, A_2') then 6.23 shows that $(Z, \lambda_1, \lambda_2)$ or (Z, λ_1) (resp.) has the (a, b, J)-property for all relevant a, b, except when $(Z, \lambda_1) = (\lambda J_2, \lambda J_2, \lambda)$. Excluding this exception, we can write Y_1 for $(Z, \lambda_1, \lambda_2)$ or (Z, λ_1) and apply 6.36 to obtain the conclusion. In the exceptional case we may assume that $X = (\lambda J_2, \lambda J_2, \lambda, \lambda, \lambda)$ (there cannot be four λ's as X is unbreakable). But this implies $|X| = \lambda^3 \neq 1$, a contradiction.

Hence we may assume that $Z = \emptyset$ or A_2. In the first case $X = (\lambda_1, \ldots, \lambda_l)$ is diagonal, and we can assume it has no sub-matrix $(-1, -1)$ (as this is a commutator in $SU_2(3)$) or $(\lambda, \lambda, \lambda, \lambda)$ (as this has determinant 1). The only possibility with $n \geq 7$ and all $\lambda_i \neq 1$ is that $X = (-1, \lambda, \lambda, \lambda, -\lambda, -\lambda, -\lambda)$. But this has determinant -1, a contradiction.

Assume finally that $Z = A_2$. If $|Z| = 1$ then we may assume that X has no sub-matrix $(-1, -1)$ as before, and also no sub-matrix $(\lambda, -\lambda)$ (otherwise $(Z, \lambda, -\lambda)$ would have determinant 1). This is impossible if $n \geq 7$. If $|Z| = -1$ then we can assume that no λ_i is -1, and there is no sub-matrix (λ, λ) (since $(Z, -1)$ and (Z, λ, λ) have determinant 1), and again this cannot happen if $n \geq 7$. If $|Z| = \lambda$ then we may assume that no λ_i is $-\lambda$ and there is no sub-matrix $(-1, -1)$, and once more this is impossible for $n \geq 7$. This completes the proof. ∎

We may now assume that $q \geq 4$. Recall the assumption at the beginning of this section that $n \geq 5$. If $X = \lambda I$, a scalar matrix, then X is a

commutator by Lemma 2.3. Thus we assume also that X is not a scalar matrix.

Proposition 6.42 *If $X = (Z, \lambda_1, \ldots, \lambda_l)$ as in (20), then X is a commutator in $GU_n(q)$. If $(n, q+1) = 1$ then X is a commutator in $SU_n(q)$.*

Proof If $Z \neq \emptyset$, then by 6.30, 6.28 and 6.24, Z has the (b, J)-property for some $b \in F_0$. If $Z = \emptyset$, then, since X is non-scalar, by 6.30 there exist λ_j, λ_k with $\lambda_j \neq \lambda_k$ where the diagonal matrix (λ_j, λ_k) has the (b, J)-property for some b. Setting $Z = (\lambda_j, \lambda_k)$ and relabelling the λ_i in the latter case, we may therefore write in the usual way

$$\begin{aligned} &Z\,(b, J)^{con} = (zb, J)^{con}, \\ &\lambda_1\,(zb) = (\lambda_1 zb), \\ &\cdots \\ &\lambda_l\,(\lambda_{l-1} \cdots \lambda_1 zb) = (b) \end{aligned}$$

(where $z = |Z|$). Hence $XB = C$ where $B, C \in GU_n(q)$ are both conjugate to $(b, zb, \lambda_1 zb, \ldots, \lambda_{l-1} \cdots \lambda_1 zb, J)$. Therefore X is a commutator in $GU_n(q)$. If $(n, q+1) = 1$ then $GU_n(q) = SU_n(q) \times Z_{q+1}$, and it follows that X is a commutator in $SU_n(q)$. ∎

Proposition 6.43 *If $X = (Z, \lambda_1, \ldots, \lambda_l)$ as in (20), with $q \geq 4$, then X is a commutator in G.*

Proof By the previous proposition, we may assume that $(n, q+1) \neq 1$. Since X is unbreakable, it has no proper sub-matrix of determinant 1. Hence the total number of indecomposable blocks in X (namely l if $Z = \emptyset$, $l+1$ if $Z = A_2$ or A_3, and $l+2$ if $Z = (A_2, A_2')$) is at most $q+1$. In particular

$$n = \dim V \leq q + 3. \tag{21}$$

Observe that if X has exactly $q+1$ indecomposable blocks, then its unbreakability implies that each of these blocks must have the same determinant λ, an element of F_0 of order $q+1$.

Consider first $q = 4$. Here $n \leq 7$ and $(n, 5) \neq 1$, so $n = 5$ and $G = SU_5(4)$. For this group, the conclusion follows from 3.1.

Next consider $q = 5$. Here $n \leq 8$ and $(n, 6) \neq 1$, so $n = 6$ or 8. If $Z = \emptyset$ then $n = 6$, and the above observation implies that all λ_i are equal, so X is a scalar, contrary to the remark preceding 6.42. Suppose $Z = A_2$. Again $n = 6$ and $X = (A_2, \lambda_1, \lambda_2, \lambda_3, \lambda_4)$. Since X has no proper sub-matrix of determinant 1, there exists $\lambda \in F_0$ of order 6 such that one of the following holds:

(a) $X = (A_2, \lambda, \lambda, \lambda, \lambda)$, $|A_2| = \lambda^2$

(b) $X = (A_2, \lambda^2, \lambda, \lambda, \lambda)$, $|A_2| = \lambda$.

In case (a), 6.30 shows that A_2 has the (b, J)-property for $b = \lambda^2$, and we write

$$\begin{aligned} &A_2\,(\lambda^2, 1)^{con} = (\lambda^4, 1)^{con},\\ &\lambda\,(\lambda^4) = (\lambda^5),\\ &\lambda\,(\lambda^5) = (1),\\ &\lambda\,(1) = (\lambda),\\ &\lambda\,(\lambda) = (\lambda^2), \end{aligned}$$

so $XB = C$ with B, C conjugate to $(1, 1, \lambda, \lambda^2, \lambda^4, \lambda^5)$, of determinant 1. In case (b), A_2 has the (b, J)-property for $b = \lambda$ and we similarly see that $XB = C$ with B, C conjugate to the same matrix. Hence X is a commutator in G in either case.

Now suppose $Z = A_3$ (still with $q = 5$). If $n = 8$ then, since it has no proper sub-matrix of determinant 1, $X = (A_3, \lambda, \lambda, \lambda, \lambda, \lambda)$ with $|A_3| = \lambda$, where $\lambda \in F_0$ has order 6. Then $Z' = (A_3, \lambda)$ has the (b, J)-property for $b = \lambda^2$ by 6.26, so we argue as above to see that $XB = C$ with B, C conjugate to $(\lambda^2, \lambda^4, \lambda^5, 1, \lambda, J)$, of determinant 1. If $n = 6$ then $X = (A_3, \lambda_1, \lambda_2, \lambda_3)$. If, for some i, (A_3, λ_i) has the (a, b, J)-property for all relevant a, b, then we can use 6.40 to obtain the result; otherwise, 6.26 shows that $X = (\lambda J_3, \lambda, \lambda, \lambda)$ with $|\lambda| = 6$. In the latter case $X_4 = (\lambda J_3, \lambda)$ has the (a, b, J)-property for $(a, b) = (\lambda, 1)$ by 6.26(iii), so we write

$$\begin{aligned} &X_4\,(\lambda, 1, J)^{con} = (\lambda^5, 1, J)^{con},\\ &\lambda\,(\lambda^5) = (1),\\ &\lambda\,(1) = (\lambda), \end{aligned}$$

and so $XB = C$ with B, C conjugate to $(\lambda, \lambda^5, 1, 1, J)$, of determinant 1, giving the conclusion.

Now suppose $Z = (A_2, A_2')$ (still with $q = 5$). If $n = 8$, then its unbreakability implies that $X = (A_2, A_2', \lambda, \lambda, \lambda, \lambda)$ with $|A_2| = |A_2'| = \lambda$, where $\lambda \in F_0$ has order 6. By 6.24, Z has the (b, J)-property for all $b \in F_0$ (noting that $A_2 \neq \mu J_2$ as $|A_2| = \lambda$ has order 6), so taking $b = \lambda^2$ we get $XB = C$ with B, C conjugate to $(\lambda^2, \lambda^4, \lambda^5, 1, \lambda, J)$, of determinant 1. Suppose now that $n = 6$, $X = (A_2, A_2', \lambda_1, \lambda_2)$. Since X is unbreakable, there exists $\lambda \in F_0$ of order 6 such that the values of $|A_2|$, $|A_2'|$, λ_1, λ_2 are, in some order, one of the following:

(i) $\lambda, \lambda, \lambda, \lambda^3$

(ii) $\lambda, \lambda, \lambda^2, \lambda^2$

(iii) $\lambda^2, \lambda^2\lambda^3, \lambda^5$.

If Z satisfies the (a, b, J)-property for all relevant a, b, then the result follows from 6.40, so assume this is not the case. Now 6.24 shows that $A_2 = A_2'$, and hence $|A_2| = |A_2'| = \lambda$ or λ^2.

If $|A_2| = \lambda$ of order 6, then by 6.24(iii), $A_2 = (\omega, \omega^{-5})$ with $|\omega| = 24$, and $\lambda = \omega^{-4}$. Also $\lambda_1, \lambda_2 = \lambda, \lambda^3$ or λ^2, λ^2 from (i),(ii),(iii) above. In the first case note that by 6.24(iii), Z has the (a, b, J)-property for $(a, b) = (\lambda, \lambda^4)$ and write

$$\begin{aligned} &Z\,(\lambda, \lambda^4, J)^{con} = (\lambda^3, \lambda^4, J)^{con}, \\ &\lambda\,(\lambda^3) = (\lambda^4), \\ &\lambda^3\,(\lambda^4) = (\lambda), \end{aligned}$$

so $XB = C$ with B, C conjugate to $(\lambda, \lambda^4, \lambda^3, \lambda^4, J)$, of determinant 1; and in the second case similarly use the (a, b, J)-property for Z with $(a, b) = (\lambda, -1)$ to get $XB = C$ with B, C conjugate to $(\lambda, -1, \lambda^3, \lambda^5, J)$, of determinant 1. The result follows.

To conclude the proof of the proposition for $q = 5$, consider finally the case where $|A_2| = \lambda^2$. Here $\lambda_1, \lambda_2 = \lambda, \lambda$ or λ^3, λ^5 from (i),(ii),(iii) above. In the first case use the (a, b, J)-property of Z with $(a, b) = (\lambda^4, -1)$, and in the second use the (a, b, J)-property with $(a, b) = (\lambda, \lambda^4)$ (given by 6.24(iii)), to see that $XB = C$ with B, C conjugate to $(\lambda^2, \lambda^3, \lambda^4, -1, J)$ or $(\lambda, \lambda^4, \lambda^5, \lambda^2, J)$ in the respective cases. These have determinant 1, so X is a commutator in G. This completes the proof for $q = 5$.

Suppose finally that $q = 7$. Now $n \leq 10$ by (21), and $(n, 8) \neq 1$, so $n = 6, 8$ or 10. If $Z = \emptyset$ then $n = 6$ or 8. In the latter case $X = \lambda I$, which was excluded just before 6.42; and when $n = 6$, since X is unbreakable, there exists $\lambda \in F_0$ of order 8 such that $X = (\lambda^3, \lambda, \lambda, \lambda, \lambda, \lambda)$ or $(\lambda^2, \lambda, \lambda, \lambda, \lambda, \lambda^2)$. In the first case the sub-matrix $X_2 = (\lambda^3, \lambda)$ has the (b, J)-property for $b = \lambda^2$ by 6.30, so we can write

$$\begin{aligned} &X_2\,(\lambda^2, 1)^{con} = (\lambda^6, 1)^{con}, \\ &\lambda\,(\lambda^6) = (\lambda^7), \\ &\lambda\,(\lambda^7) = (1), \\ &\lambda\,(1) = (\lambda), \\ &\lambda\,(\lambda) = (\lambda^2), \end{aligned}$$

and so $XB = C$ with B, C conjugate to $(\lambda, \lambda^2, \lambda^6, \lambda^7, 1, 1)$, of determinant 1. In the second case the sub-matrix (λ^2, λ) has the (b, J)-property for $b = \lambda^6$ by 6.30, and we argue similarly that $XB = C$ with B, C conjugate to $(\lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^6, 1)$. Hence X is a commutator in G.

Next suppose $Z = A_2$. Then $n = 6$ or 8. If $X_4 = (A_2, \lambda_i, \lambda_j)$ has the (b, J)-property for all $b \in F_0$ for some i, j (say for $i, j = 1, 2$), then taking $x_4 = |X_4|$ and writing $X_4\,(b, J)^{con} = (x_4 b, J)^{con}$, $\lambda_3\,(x_4 b) = (\lambda_3 x_4 b)$ and so on, we see that $XB = C$ with B, C conjugate and $|B| = b^{n-3} f(x_4, \lambda_i)$. As $n - 3 = 3$ or 5, coprime to $|F_0| = 8$, we can choose $b \in F_0$ such that $|B| = 1$, giving the result. Otherwise, no such X_4 has the (b, J)-property for all b, and so by 6.27 $X = (\lambda J_2, \lambda, \lambda, \lambda, \lambda, \lambda, \lambda)$, where $|\lambda| = 8$. Here, the sub-matrix $X_4 = (\lambda J_2, \lambda, \lambda)$ has the (b, J)-property for $b = \lambda^2$ by 6.27, and we write $X_4\,(\lambda^2, J)^{con} = (\lambda^6, J)^{con}$, $\lambda\,(\lambda^6) = (\lambda^7)$, and so on, to see

that $XB = C$ with B, C conjugate to $(\lambda, \lambda^2, \lambda^6, \lambda^7, 1, J)$, of determinant 1, giving the conclusion.

Next consider $Z = A_3$. If for some i, (A_3, λ_i) has the (a, b, J)-property for all relevant $a, b \in F_0$, then 6.36 (with $Z = \emptyset, Y_1 = (A_3, \lambda_i)$) gives the result. Otherwise, 6.26 shows that $(A_3, \lambda_i) = (\lambda J_3, \lambda)$ ($|\lambda| = 8$) for all i, whence $n = 8$ and $X = (\lambda J_3, \lambda, \lambda, \lambda, \lambda, \lambda)$. Then by 6.26, $X_4 = (\lambda J_3, \lambda)$ has the (b, J)-property for all $b \in F_0$, in particular for $b = \lambda^2$. Hence, writing $X_4\,(\lambda^2, J)^{con} = (\lambda^6, J)^{con}$, $\lambda\,(\lambda^6) = (\lambda^7)$ and so on, we see that $XB = C$ with B, C conjugate to $(\lambda, \lambda^2, \lambda^6, \lambda^7, 1, J)$, of determinant 1.

Finally, consider $Z = (A_2, A_2')$. By 6.24, Z has the (b, J)-property for all $b \in F_0$, so taking $z = |Z|$ and writing $Z\,(b, J)^{con} = (zb, J)^{con}$, $\lambda_1\,(zb) = (\lambda_1 zb)$ and so on, we see that $XB = C$ with B, C conjugate and $|B| = b^{n-3} f(z, \lambda_i)$. As $n - 3 = 3, 5$ or 7, coprime to $|F_0| = 8$, we can choose $b \in F_0$ such that $|B| = 1$, giving the result. This completes the proof for $q = 7$, and hence the proposition is now proved. ■

Taken together, 6.31, 6.35, 6.40, 6.41 and 6.43 constitute a complete proof of Theorem 6.1.

7 Exceptional groups

We now prove Ore's conjecture for exceptional groups of Lie type. Lemma 2.2 implies that we need only consider the types $E_6^\epsilon\,(\epsilon = \pm)$, E_7 and E_8.

Theorem 7.1 *Let G be one of the simple groups $E_8(q)$, $E_7(q)$ and $E_6^\epsilon(q)$. Every element of G is a commutator.*

Write $K = \bar{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, let $\bar{G}$ be a simple adjoint algebraic group over K of type E_6, E_7 or E_8, and let σ be a Frobenius morphism of $\bar{G}$ with fixed point group $\bar{G}_\sigma$, so that $\bar{G}'_\sigma$ is one of the simple groups $E_6^\epsilon(q)$, $E_7(q)$ or $E_8(q)$.

Lemma 7.2 *Let G be one of the simple groups $E_8(q), E_7(q)$ or $E_6^\epsilon(q)$ (where $q > 2$).*

(i) *G has an irreducible character χ_0 of degree listed in the following table, and all other nontrivial irreducible characters χ of G have degree greater than the bound indicated in the table.*

G	$\chi_0(1)$	*lower bound for* $\chi(1)$, $\chi \neq 1, \chi_0$
$E_8(q)$	$\frac{q(q^2+1)^2(q^4+1)(q^6+1)(q^{12}+1)}{(q^2+1)^2(q^4+1)}$	q^{46}
$E_7(q)$	$\frac{q(q^{14}-1)(q^6+1)}{q^4-1}$	q^{26}
$E_6^\epsilon(q)$	$q(q^4+1)(q^6+\epsilon q^3+1)$	$q^{16}/2$

(ii) *If* $1 \neq u \in G$ *is unipotent,* $1 \neq x \in G$ *is arbitrary, and* $1 \neq \chi \in \mathrm{Irr}(G)$,

$$\frac{|\chi(u)|}{\chi(1)} \leq \frac{3}{4}, \quad \frac{|\chi(x)|}{\chi(1)} \leq \frac{19}{20}.$$

(iii) *The number of conjugacy classes* $k(G)$ *satisfies the upper bound in the following table.*

G	*upper bound for* $k(G)$
$E_8(q)$	$4.52\,q^8$
$E_7(q)$	531, $q = 2$
	$4.18\,q^7$, $q \geq 3$
$E_6^\epsilon(q)$	1389, $q = 3$
	$4.35q^6$, $q \geq 4$

Proof (i) This follows from [32].

(ii) This follows from [21].

(iii) The precise number of conjugacy classes in the adjoint groups is given by [14, 15]. The conclusion follows for $E_8(q)$. To get correct bounds for the simple groups of type E_7 and E_6, it suffices to multiply the numbers in [15] by $(2, q-1)$ and $(3, q-\epsilon)$ respectively. ■

Proof of Theorem 7.1 for $E_8(q)$

Let $G = E_8(q)$. We give a proof which works for all q, even though we only need to consider $q \leq 5$ by [12]. In the proof we freely use the information about conjugacy classes of unipotent elements in G given in [35], and about subsystem subgroups and their centralizers given in [27] and [28, Section 4].

Case 1: *Unipotent elements*

Let $x \in G$ be a non-identity unipotent element. We show that x is a commutator. By Lemma 7.2(i),

$$E(x) = \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(x)}{\chi(1)} \leq \frac{3}{4} + \sum_{\chi \neq 1, \chi_0} \frac{\chi(x)}{\chi(1)}.$$

By Lemma 7.2, the characters in the latter sum have degree greater than q^{46}, and there are less than $4.52\,q^8$ of them. Hence using Lemma 2.6,

$$E(x) \leq \frac{3}{4} + \frac{|C_G(x)|^{1/2}\sqrt{4.52}\,q^4}{q^{46}}.$$

Thus $|E(x)| < 1$ if the second term is less than $1/4$. This holds if $|C_G(x)|^{1/2} < q^{42}/(4 \cdot \sqrt{4.52})$, which holds if $|C_G(x)| < q^{84}/73$, hence also if $|C_G(x)| < q^{77}$.

Therefore by Lemma 2.5, in this case (x unipotent) we may assume that

$$|C_G(x)| > q^{77}.$$

Referring to [35, Table 10, p. 455], it follows that x lies in one of the $\bar{G}$-classes with the following labels:

$$D_4,\ D_4(a_1),\ 2A_2+2A_1,\ 2A_2+A_1,\ A_3,\ 2A_2,\ A_2+3A_1,$$
$$A_2+2A_1,\ A_2+A_1,\ 4A_1,\ A_2,\ 3A_1,\ 2A_1,\ A_1.$$

Hence x is a distinguished unipotent element in a Levi subgroup $\bar{L}$ of $\bar{G}$ corresponding to the label.

Write $C = C_{\bar{G}}(x)$. By Lang's Theorem (see [43, I, 3.4]), the number of G-classes in $x^{\bar{G}} \cap G$ is equal to the number of classes in C/C^0. When $C = C^0$, this number is 1, and so we may take $\bar{L}$ to be σ-stable, and $x \in \bar{L}'_\sigma = L(q)$. For each Levi subgroup in the above list, $L(q)$ is contained in a subsystem subgroup $D_4(q)$ or $A_4(q)A_4(q)$. By Lemmas 3.2 and 2.1, every element of each of these groups is a commutator, so the result follows when $C = C^0$.

Now assume that $C \neq C^0$. By [35, Table 10], the possible labels for the $\bar{G}$-class of x are $D_4\,(p=2)$, $D_4(a_1)$, $2A_2$, A_2+A_1 and A_2. In the first case $|C/C^0| = 2$, so there are 2 G-classes in $x^{\bar{G}} \cap G$. The unipotent element x lies in a subgroup G_2 of $\bar{L}'$, centralizing an F_4 in $\bar{G}$, and this F_4 is the reductive part of $C_{\bar{G}}(x)$. Thus there are representatives of both G-classes lying in $C_G(F_4(q))$. Hence they lie in $C_G(F_4(q)) = G_2(q)$, and so in a subgroup $D_4(q)$, and the result follows, again by 3.2.

A similar argument works for the class $D_4(a_1)$: here $C/C^0 \cong S_3$ acting as graph automorphisms on both the derived group of the Levi subgroup $\bar{L}' = D_4$, and the reductive part $D = D_4$ of $C_{\bar{G}}(x)$. Observe that $C_{\bar{G}}(\bar{L}') = D$ and vice versa. Hence the class representatives in $G = \bar{G}_\sigma$ lie in a subgroup $C_G(D_\sigma) = \bar{L}'_\sigma$, a possibly twisted subgroup $D_4^\epsilon(q)$, and again the result follows using 3.2.

The same argument works for the class A_2+A_1: here the reductive part $D = A_5$ of $C_{\bar{G}}(x)$ has centralizer $\bar{L}' = A_2A_1$, so the class representatives in G lie in $\bar{L}'_\sigma = A_2^\epsilon(q)A_1(q)$, which lies in a subgroup $D_4(q)D_4(q)$.

Finally consider the class $2A_2$. The corresponding class representatives in G are given in [35, Lemma 109], where they are called z_{181}, $z_{182}\,(p=2)$, $z_{183}\,(p\neq 2)$. The first of these lies in a Levi subgroup $\bar{L}'_\sigma = A_2(q)^2$, giving the conclusion in the usual way by 2.1. The expressions for z_{182}, z_{183} are products of root elements of G involving the roots α_i for $i = 53$, 54, 55, 57, 117, 122, 124. Using [35, Table 11], we have, in the more usual notation for roots (i.e. $c_1 \ldots c_8$ denotes the root $\sum c_i\alpha_i$, where $\alpha_i\,(1 \leq i \leq 8)$ are the fundamental roots):

$$\alpha_{53} = 12232100, \quad \alpha_{54} = 11232110, \quad \alpha_{55} = 11222210, \quad \alpha_{57} = 11232210,$$
$$\alpha_{117} = 11222111, \quad \alpha_{122} = 11122221, \quad \alpha_{124} = 11232211$$

These roots span a subsystem A_2D_4. Hence the representatives z_{182}, z_{183} lie in a subgroup $A_2(q)D_4(q)$, and the result follows as usual. This completes the unipotent case.

Case 2: *Non-unipotent elements* Now let $x = su \in G$, where $s \neq 1$ is the semisimple part of x and u is the unipotent part. Using Lemma 7.2 as above,

$$E(x) = \sum_{1 \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(x)}{\chi(1)} \leq \frac{19}{20} + \sum_{\chi \neq 1, \chi_0} \frac{\chi(x)}{\chi(1)} \leq \frac{19}{20} + \frac{|C_G(x)|^{1/2}\sqrt{4.52}\, q^4}{q^{46}}. \tag{22}$$

Hence $|E(x)| < 1$ if the second term is less than $1/20$, which holds if $|C_G(x)| < q^{84}/1808$, hence also if $|C_G(x)| < q^{73}$.

Assume that $|C_G(x)| > q^{84}/1808$. Then $C_G(s)$ is a subsystem subgroup of at least this order, and inspection of such subgroups shows that $C_G(s)$ has a quasisimple normal subgroup C equal to one of the subsystem groups $E_7(q)$, $D_8(q)$, $A_8^\epsilon(q)$, $E_6^\epsilon(q)$, $D_7^\epsilon(q)$. Moreover s lies in $C_G(C)$, which is $A_1(q)$, $Z_{(2,p-1)}$, $Z_{(3,q-\epsilon)}$, $A_2^\epsilon(q)$, $Z_{q-\epsilon}$ in the respective cases.

Suppose $C = D_8(q)$. Here p is odd and s is an involution in $Z(C)$. Thus $|C_C(u)| > q^{73}$, and inspection of the centralizers of unipotent elements of orthogonal groups given in [50, p. 34] shows that u has no Jordan blocks of size greater than 4 on the natural 16-dimensional D_8-module, hence it lies in a subgroup $D_4(q)D_4(q)$ of C. This subgroup contains $Z(C)$, so it contains x, and the result follows using 3.2 as usual. A similar argument handles the case where $C = D_7^\epsilon(q)$: here $s \in Z_{q-\epsilon} < Z_{q-\epsilon}D_7^\epsilon(q) < D_8(q)$, $|C_C(u)| > q^{73}/q - \epsilon$, and we need to consider also the case where q is even, using [50, p. 60]. We again find that x lies in a subgroup $D_4(q)D_4(q)$.

Now consider $C = A_8^\epsilon(q)$. Here s is a element of order 3 in $Z(C)$. By [50], C has no non-identity unipotent element with centralizer order greater than q^{73}. Hence $u = 1$ and $x = s$, which is a commutator in C by Lemma 2.3.

Next suppose $C = E_6^\epsilon(q)$, so $s \in C_G(C) = A_2^\epsilon(q) \cong SL_3^\epsilon(q)$. Then $|C_C(u)| > q^{73}/|A_2^\epsilon(q)|$, which by [34, Section 4] forces the projection of u to C to be 1. Hence $x = su \in A_2^\epsilon(q)$, which lies in a subgroup $A_3^\epsilon(q)$, giving the conclusion by Corollary 3.2.

Finally, suppose $C = E_7(q)$, so $s \in C_G(C) = A_1(q)$, a fundamental $SL_2(q)$ in G. Then $|C_C(u)| > q^{73}/|A_1(q)|$, so from [35, Table 9] we see that $u^{\bar{C}}$ is one of the classes $1, A_1, 2A_1, 3A_1''$. In the first three cases $C_{\bar{C}}(u)$ is connected, so $x = su$ lies in a product $(A_1(q))^3$ of 3 fundamental $SL_2(q)$'s, hence in a subgroup $D_4(q)D_4(q)$. In the $3A_1''$ case, $C_C(u)$ contains a subgroup $F_4(q)$, which has G-centralizer $G_2(q)$, so $x \in G_2(q) < D_4(q)$. The result follows from 3.2 in the usual way.

This completes the proof of Theorem 7.1 for $G = E_8(q)$.

Proof of Theorem 7.1 for $E_7(q)$

Let $G = E_7(q)$. By 2.4, Ore's conjecture holds for G when $q \geq 5$, so we may assume that $q \leq 4$. Let $G = \bar{G}'_\sigma$ with $\bar{G} = E_7(K)$ as before. The proof follows the same lines as for $E_8(q)$.

Let $x \in G$, and suppose first that x is a non-identity unipotent element of G. Using Lemmas 2.6 and 7.2,

$$E(x) = \sum_{1 \neq \chi \in \ \mathrm{Irr}(G)} \frac{\chi(x)}{\chi(1)} \leq \frac{3}{4} + \frac{|C_G(x)|^{1/2} k(G)^{1/2}}{q^{26}}, \tag{23}$$

and hence $|E(x)| < 1$ if $|C_G(x)|$ is less than $q^{52}/8496$ $(q = 2)$ or $q^{45}/67$ $(q \geq 3)$. Assume now that $|C_G(x)|$ is larger than these bounds. From [35, Table 9] we see that $x^{\bar{G}}$ lies in one of the classes $D_4(a_1)$, $(A_3 + A_1)'$, $(A_3 + A_1)''$, 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. Write $C = C_{\bar{G}}(x)$. As in the E_8 argument, if $C = C^0$, then x lies in a Levi subgroup $\bar{L}'_\sigma = L(q)$, where $\bar{L}'$ is in the above list, and all such subgroups $L(q)$ can be seen to lie in a subsystem subgroup $A_2(q)A_5(q)$, giving the result by Lemma 2.1.

This leaves the classes in the list for which $C \neq C^0$, which are $D_4(a_1)$, $A_2 + A_1$ and A_2. In the first case we argue as for the $D_4(a_1)$ class in E_8 that x lies in a subgroup $L'_\sigma = D_4^\epsilon(q)$, giving the result by 3.2. For the A_2 class, the reductive part of C is $D = A_5$, and $D_\sigma = A_5^\epsilon(q)$ has $\bar{G}$-centralizer $\bar{L}' = A_2$, so again $x \in \bar{L}'_\sigma = A_2^\epsilon(q) < A_3^\epsilon(q)$, giving the result by 3.2. Finally, for the $A_2 + A_1$ class, the reductive part of C is $D = T_1 A_3$. Hence x lies in the centralizer of a subgroup $A_2^\epsilon(q)$ of D_σ, which is $A_5^\epsilon(q)$, giving the conclusion by 3.1.

Now suppose x is not unipotent, and write $x = su$ with s the semisimple part and u the unipotent part. Arguing as above for (22), replacing $3/4$ in (23) by $19/20$, we see that $|E(x)| < 1$ if $|C_G(x)|$ is less than 2^{34} if $q = 2$, less than 3^{38} if $q = 3$, and less than q^{39} if $q = 4$. Assume $|C_G(x)|$ is greater than these bounds. Inspection of semisimple element centralizers of such orders in [9] shows that $C_G(s)$ has a quasisimple normal subgroup $C = A_r^\epsilon(q)$ $(r = 4, 5, 6 \text{ or } 7)$, $D_5^\epsilon(q)$, $D_6(q)$ or $E_6^\epsilon(q)$.

If $C = A_4^\epsilon(q)$, then the bound on $|C_G(x)|$ forces $q = 2$ and the projection of u in C to be 1, so that x lies in $C_G(A_4^\epsilon(2)) \leq C_G(A_1(2)) = D_6(2)$, giving the result by 3.1(vi).

If $C = A_5^\epsilon(q)$ then $s \in C_G(C) = A_2^\epsilon(q)Z$. The lower bound on $|C_G(x)|$ forces the projection of u in C to have Jordan form 1 or (J_2, J_1^4). Hence x centralizes a subgroup $A_2^\epsilon(q)$ of C, and so $x \in C_G(A_2^\epsilon(q)) = A_5^\epsilon(q)$, giving the result by 3.1(iii).

Now assume $C = A_6^\epsilon(q)$. Then s has order dividing $(q - \epsilon)/(2, q - \epsilon)$. If $q = 2$ then $\epsilon = -$ and $\langle s \rangle \times C = 3 \times SU_7(2) < SU_8(2) < G$; however

an element of order 3 in $SU_8(2)$ centralizing $SU_7(2)$ is central, contradicting the fact that $C \lhd C_G(s)$. If $q = 3$ then s has order 2, and again $C_G(x)$ must be $A_7^\epsilon(q)$. Finally, suppose $q = 4$. Then $C_G(s) = (q-\epsilon) \times SL_7^\epsilon(4) < SL_8^\epsilon(4)$. If $\epsilon = +$, then the conclusion follows by 2.1; if $\epsilon = -$, the bound on $|C_G(x)|$ implies that $u = 1$, so $x = \mathrm{diag}(\omega^3, \omega, \ldots, \omega) \in SU_8(4)$, where $\omega^5 = 1$. Hence x lies in a subgroup $SU_3(4) \times SU_5(4)$, giving the result by 3.1.

Next suppose $C = A_7^\epsilon(q)$. Then $|s| = 2$, $\epsilon = -$ and $q = 3$. The bound forces the Jordan form of u in $A_7^\epsilon(q)$ to have no blocks of size greater than 3, and at least 2 trivial blocks. Hence $x = su \in A_3^\epsilon(q)A_3^\epsilon(q) < A_7^\epsilon(q)$, giving the conclusion by 3.1.

Next consider $C = D_6(q)$. Here $s \in C_G(C) = A_1(q)$. If $q = 2$ then $|s| = 3$, and $x = su \in A_1(2)D_6(2)$ with $s \in A_1(2)$ and $u \in D_6(2)$. Since s is a commutator in $A_1(2)$, the conclusion now follows by 3.1(vi). Now suppose $q = 3$ or 4. Using [50, p. 34], the bound on $|C_G(x)|$ forces the Jordan form of the projection u_0 of u in the natural 12-dimensional D_6-module to be one of 1, (J_2^2, J_1^8), (J_3, J_1^9), (J_2^4, J_1^4), (J_2^6), (J_3, J_2^2, J_1^5). If $q = 4$ the projection of u in C lies in a subgroup $\Omega_8(q) \times \Omega_4(q)$, and so $x \in A_1(q) \times \Omega_8(q) \times \Omega_4(q)$, giving the result by 3.1. Finally let $q = 3$. If u_0 has no J_3 blocks, then $u_0 \in A_5^\epsilon(q) < C$, so $x \in A_1(q)A_5^\epsilon(q) < A_2^\epsilon(q)A_5^\epsilon(q)$, and the result follows using 3.1. If $u_0 = (J_3, J_2^2, J_1^5)$, then the bound on $|C_G(x)|$ forces the projection of u in $C_G(C) = A_1(q)$ to be 1, and so $x = su \in D_4^\epsilon(q) < C$, giving the result by 3.1. If $u_0 = (J_3, J_1^9)$, then x centralizes a subgroup $A_2(q)$ of C generated by root groups, and so $x \in C_G(A_2(q)) = A_5(q)$, giving the result by 2.1.

The case where $C = D_5^\epsilon(q)$ is similar and easier: here, the bound on $|C_G(x)|$ forces the projection u_0 of u in C to be 1 if $q \geq 34$, and to centralize a root $A_2(q)$ in C if $q = 2$. Hence in any case x centralizes a root $A_2(q)$, so $x \in C_G(A_2(q)) = A_5(q)$, giving the result by 2.1.

Finally, suppose $C = E_6^\epsilon(q)$. If $q = 2$ then $|s| = 3$ and $\langle s \rangle = Z(C)$, so $x \in C = {}^2E_6(2)$ and the result follows by 3.1. Assume $q \geq 3$. By [34], the bound on $|C_G(x)|$ forces u to be in one of the C-classes labelled $1, A_1, 2A_1, 3A_1, A_2$, the latter two only if $q \leq 3$. Moreover, the centralizer of u in $\bar{E}_6$ is connected, except for the last class A_2, in which case $C_{\bar{E}_6}(u)/C_{\bar{E}_6}(u)^0 \cong Z_2$.

If u is in the class 1 or A_1, then $C_C(u)$ contains a subsystem subgroup $A_5^\epsilon(q)$, so $x \in C_G(A_5^\epsilon(q)) = A_2^\epsilon(q) < A_3^\epsilon(q)$, giving the result in the usual way. If u is in class $2A_1$ then $u \in B_1(q) < D_5^\epsilon(q) < C$, so $C_C(u)$ contains a subgroup $B_3(q)$, which in turn contains an $A_2(q)$ generated by root groups, so $x \in C_G(A_2(q)) = A_5(q)$, giving the result by 2.1.

Now suppose that u is in class $3A_1$ or A_2, in which case $q \leq 3$. In the first case u lies in a subgroup $A_5^\epsilon(q)$ of C, and hence $x = su$ lies in a subgroup $A_5^\epsilon(q)A_2^\epsilon(q)$ of G. For $q = 3$ this gives the result by 3.2; for $q = 2$, observe that u centralizes a fundamental SL_2 of C, hence x lies in $C_G(SL_2(2)) = D_6(2)$, again giving the conclusion by 3.2.

Finally, suppose u is in class A_2, so $C_{\bar{E}_6}(u)/C_{\bar{E}_6}(u)^0 \cong Z_2$, and $u^{\bar{E}_6} \cap C$ splits into two C-classes. One of these has representative lying in a subsystem subgroup $A_2^\epsilon(q)$; if u is in this class, then $x = su$ lies in subsystem subgroups $A_2^\epsilon(q)A_5^\epsilon(q)$ and $D_6(q)$ of G, giving the result as before. Suppose u is in the other class. Since $C_{\bar{E}_6}(u)$ contains a subsystem A_2^2, which has fixed point group $A_2(q^2)$, u lies in $C_C(A_2(q^2)) = A_2^{-\epsilon}(q)$ (see [27, Table 5.1]), and hence $x = su$ lies in $N_G(A_2^{-\epsilon}(q)) = A_2^{-\epsilon}(q)A_5^{-\epsilon}(q)$. This yields the conclusion for $q = 3$ and also for $q = 2, \epsilon = -$, by 3.2. However, in the remaining case $\epsilon = +, q = 2$, $C = E_6(2)$ does not centralize any non-identity element of $G = E_7(2)$, so this does not occur.

This completes the proof of Theorem 7.1 for $G = E_7(q)$.

Proof of Theorem 7.1 for $E_6^\epsilon(q)$

Let $G = E_6^\epsilon(q)$. We may assume that $q \geq 3$ by 3.1(vi). By 2.4, we may assume that $q \leq 5$ if $\epsilon = +$ and $q \leq 7$ if $\epsilon = -$.

Let x be a non-identity unipotent element of G. Using 2.6 and 7.2 as before,

$$E(x) = \sum_{1 \neq \chi \in \ \mathrm{Irr}(G)} \frac{\chi(x)}{\chi(1)} \leq \frac{3}{4} + \frac{|C_G(x)|^{1/2} k(G)^{1/2}}{q^{16}/2},$$

and hence $|E(x)| < 1$ if $|C_G(x)| \leq q^{21}$. Thus assume $|C_G(x)| > q^{21}$. By [34], $x^{\bar{G}}$ is in one of the classes $D_4(a_1)$, $A_3 + A_1$, $2A_2 + A_1$, A_3, $A_2 + 2A_1$, $2A_2$, $A_2 + A_1$, A_2, $3A_1$, $2A_1$, A_1. In the first case x lies in a subgroup $D_4^\delta(q)$; in the second x lies in a subgroup $A_3^\epsilon(q)A_1(q)$ if $q > 3$ and in a subgroup $A_5^\epsilon(q)$ if $q = 3$; and in all other cases x lies in a subgroup $A_2^\epsilon(q)^3$ or $A_2^\pm(q)A_2^\pm(q^2)$. The result follows from 3.1.

Now suppose $x \in G$ is non-unipotent, say $x = su$ with s the semisimple part. The above inequality for $E(x)$ holds with $3/4$ replaced by $19/20$, giving $|E(x)| < 1$ if $|C_G(x)| < q^{19}/2$. Thus assume that $|C_G(x)| > q^{19}/2$. Then $C_G(s)$ has a quasisimple normal subgroup $C = D_5^\epsilon(q)$, $D_4^\delta(q)$, $A_5^\epsilon(q)$, $A_4^\epsilon(q)$, $A_3^\epsilon(q)$, $(A_2^3)_\sigma$ or $(A_2^2)_\sigma$ (the latter two possibilities denoting the fixed points under σ of subsystem subgroups $A_2(K)^3$ or $A_2(K)^2$ of $\bar{G}$).

Suppose first that $C = D_5^\epsilon(q)$. Inspection of unipotent centralizer orders in [50] shows that $u \in C$ has one of the following Jordan block structures on the natural 10-dimensional C-module:

q odd: $u = (J_3^2, J_1^4)$, (J_3, J_2^2, J_1^3), (J_2^4, J_1^2), (J_3, J_1^7), (J_2^2, J_1^6) or (J_1^{10})

q even: $u = (J_3^2, J_1^4)$, (J_2^4, J_1^2) (2 classes), (J_2^2, J_1^6) (2 classes), or (J_1^{10}).

If $u = (J_3^2, J_1^4)$, then u lies in a subgroup $A = A_2^{\pm\epsilon}(q)$ of C generated by root subgroups, so $x = su \in AC_G(A) = (A_2^\epsilon(q))^3$ or $A_2^{-\epsilon}(q)A_2(q^2)$ (see [27, Table 5.1]), and the conclusion follows by 3.2.

We claim that for all the other classes, u is centralized by a fundamental subgroup $A_1(q)$ of C. For q odd this follows from the fact that in dimension 4, an element (J_2^2) lies in one of the $SL_2(q)$ factors of $SL_2(q) \otimes SL_2(q) = \Omega_4^+(q)$. For q even, it is clear except for the 2 classes (J_2^4, J_1^2); these are the classes called a_4 and c_4 in [1], from which we see that $a_4 = \mathrm{diag}(a_2, a_2)$, $c_4 = \mathrm{diag}(a_2, c_2)$, and $a_2 = (J_2^2)$ lies in a factor $SL_2(q)$ of $\Omega_4^+(q)$ as above.

Hence $x = su \in C_G(A_1(q)) = A_5^\epsilon(q)$ which yields the conclusion for $\epsilon = +$ by 2.1, and for $\epsilon = -$, $q \leq 4$ by 3.1. Thus assume now that $\epsilon = -$ and $q > 4$, so that $q = 5$ or 7.

If $u = (J_3, J_1^7)$, (J_2^2, J_1^6) or (J_1^{10}), then u centralizes a subgroup $A_2^\epsilon(q)$ of C, so x lies in the centralizer of this subgroup, which is $(A_2^\epsilon(q))^2$, giving the conclusion by 3.2.

The remaining cases are $u = (J_3, J_2^2, J_1^3)$ or (J_2^4, J_1^2). These have D_5-centralizers of dimensions 21 and 25 respectively. In these cases we place x in a subgroup $A_2^-(q)^3$ of G. First observe that by [29, 2.1], for the subsystem subgroup A_2^3 of the algebraic group E_6,

$$L(E_6)|A_2^3 = L(A_2^3) + (V_3 \otimes V_3 \otimes V_3) + (V_3^* \otimes V_3^* \otimes V_3^*),$$

where V_3 is the natural module for $A_2 = SL_3$. For $c \in \mathbb{F}_{q^2}$, let $t(c)$ be the image in A_2^3 of the element $((c, c, c^{-2}), (c^{-1}, c^{-1}, c^2), (1, 1, 1))$; we check that $t(c)$ has centralizer of dimension 46 in $L(E_6)$, and so this centralizer is D_5T_1. Hence we may take the semisimple element s to be $t(c)$ for some $c \in \mathbb{F}_{q^2}$ of order dividing $q+1$. Moreover, let $u_1 = ((J_2, J_1), (J_2, J_1), (J_2, J_1))$, and $u_2 = ((J_1^3), (J_2, J_1), (J_2, J_1)) \in A_2^3$; we check that su_1 and su_2 have centralizers in $L(E_6)$ of dimensions 22 and 26 respectively, and hence $x = su$ is conjugate to one of these elements. It follows that x lies in a subgroup $A_2^-(q)^3$ of G, as desired, and the conclusion now follows by 3.2.

This completes the argument when $C = D_5^\epsilon(q)$.

The other possibilities for C are much easier to handle, and we do so rather briefly. First consider the case where $C = D_4^\delta(q)$. Here the bound $|C_G(x)| > q^{19}/2$ forces u to be either 1 or a long root element in C. Hence u lies in a subgroup $A = A_2^\epsilon(q)$ of C, whence $x = su \in AC_G(A) = A_2^\epsilon(q)^3$, giving the conclusion by 3.2.

If $C = A_5^\epsilon(q)$ then $s \in C_G(C) = A_1(q)$, and the projection u_0 of U in C must be 1, (J_2, J_1^4), (J_2^2, J_1^2) or (J_3, J_1^3). For $q = 3$, observe that u_0 centralizes a fundamental $A_1(q)$, so $x \in C_G(A_1(q)) = A_5^\epsilon(q)$, giving the conclusion by 3.1. For $q > 3$, observe that u_0 lies in a subgroup $A_3^\epsilon(q)$ of C, and so $x = su \in A_1(q)A_3^\epsilon(q)$, giving the conclusion by 3.2.

If C is $A_4^\epsilon(q)$ or $A_3^\epsilon(q)$, then the projection u_0 of u in C must be 1 or a transvection, which lies in a subgroup $A_2^\epsilon(q)$, giving the result as before.

Finally, if C is $(A_2^3)_\sigma$ or $(A_2^2)_\sigma$, the bound forces $u = 1$ and s lies in a subgroup $(A_2^3)_\sigma$, giving the conclusion by 3.2.

This completes the proof of Theorem 7.1.

The proof of Ore's conjecture is now complete.

References

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

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

[3] O. Bonten, Über Kommutatoren in endlichen einfachen Gruppen, Aachener Beitrge zur Mathematik, Bd. 7, Verlag der Augustinus-Buchhandlung, Aachen, 1993

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

[5] J.J. Cannon and D.F. Holt, Computing conjugacy class representatives in permutation groups. *J. Algebra* **300** (2006), 213–222.

[6] R.W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley Interscience, 1985.

[7] F. Celler, C.R. Leedham-Green, S.H. Murray, A.C. Niemeyer and E.A. O'Brien. Generating random elements of a finite group. *Comm. Algebra*, **23** (1995), 4931–4948.

[8] J.H.Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[9] D.I. Deriziotis, The centralizers of semisimple elements of the Chevalley groups E_7 and E_8, *Tokyo J. Math.* **6** (1983), 191–216.

[10] F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Math. Soc. Student Texts **21**, Cambridge Univ. Press 1991.

[11] L. Dornhoff, *Group Representation Theory*, Marcel Dekker, New York, 1972.

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

[13] V. Ennola, On the characters of the finite unitary groups, *Ann. Acad. Scient. Fenn.* A I, no. 323 (1963).

[14] P. Fleischmann and I. Janiszczak, The semisimple conjugacy classes and the generic class number of the finite simple groups of Lie type E_8, *Comm. Algebra* **22** (1994), 2221–2303.

[15] P. Fleischmann and I. Janiszczak, The semisimple conjugacy classes of finite groups of Lie type E_6 and E_7, *Comm. Algebra* **21** (1993), 93–161.

[16] F. G. Frobenius, Über Gruppencharaktere, Sitzber. Preuss. Akad. Wiss. (1896) 985–1021; reprinted in Gesammelte Abhandlungen, Vol. 3 (Springer, Heidelberg, 1968) 1–37.

[17] J. Fulman and R. M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, preprint, arXiv:0902.2238.

[18] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.9*, 2006, `http://www.gap-system.org`

[19] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems, to appear in *Trans. Amer. Math. Soc.*

[20] P. Gérardin, Weil representations associated to finite fields, *J. Algebra* **46** (1977), 54 - 101.

[21] D. Gluck, Sharper character value estimates for groups of Lie type, *J. Algebra* **174** (1995), 229–266.

[22] R. Gow, Commutators in the symplectic group, *Arch. Math.* **50** (1988), 204–209.

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

[24] R. Guralnick and P.H. Tiep, Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969–5023.

[25] W.H. Hesselink, Nilpotency in classical groups over a field of characteristic 2, *Math. Z.* **166** (1979), 165–181.

[26] 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.

[27] 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.

[28] M.W. Liebeck and G.M. Seitz, Subgroups generated by root subgroups in groups of Lie type, *Annals of Math.*, **139** (1994), 293-361.

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

[30] M.W. Liebeck and G.M. Seitz, Unipotent and nilpotent classes in simple algebraic groups and Lie algebras, preprint.

[31] M.W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61–86.

[32] F. Lübeck, Smallest degrees of representations of exceptional groups of Lie type, *Comm. Algebra* **29** (2001), 2147 – 2169.

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

[34] K. Mizuno, The conjugate classes of Chevalley groups of type E_6, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **24** (1977), 525–563.

[35] K. Mizuno, The conjugate classes of unipotent elements of the Chevalley groups E_7 and E_8, *Tokyo J. Math.* **3** (1980), 391–461.

[36] G. Navarro and Pham Huu Tiep, Degrees of rational characters of finite groups, (submitted).

[37] J. Neubüser, H. Pahlings and E. Cleuvers, Each sporadic finasig G has a class C such that $CC = G$, *Abstracts AMS* **34** (1984), 6.

[38] Hung Ngoc Nguyen, Low-dimensional characters of finite classical groups, preprint, University of Florida, www.math.ufl.edu/~hnguyen

[39] S. Nozawa, On the characters of the finite general unitary group $U(4, q^2)$, *J. Fac. Sci. Univ. Tokyo Sect. IA* **19** (1972), 257 - 295.

[40] O. Ore, Some remarks on commutators, *Proc. Amer. Math. Soc.* **2** (1951), 307–314.

[41] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, to appear in *Annals of Math.*

[42] P. Sin and Pham Huu Tiep, Rank 3 permutation modules for finite classical groups, *J. Algebra* **291** (2005), 551 - 606.

[43] T.A. Springer and R. Steinberg, Conjugacy classes, in: *Seminar on algebraic groups and related topics* (ed. A. Borel et al.), Lecture Notes in Math. 131, Springer, Berlin, 1970, pp. 168-266.

[44] R.C. Thompson, Commutators in the special and general linear groups, *Trans. Amer. Math. Soc.* **101** (1961), 16–33.

[45] R.C. Thompson, On matrix commutators, *Portugal. Math.* **21** (1962), 143–153.

[46] R.C. Thompson, Commutators of matrices with coefficients from the field of two elements, *Duke Math. J.* **29** (1962), 367–373.

[47] P.H. Tiep and A. Zalesskii, Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.

[48] Pham Huu Tiep and A. E. Zalesskii, Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* **192** (1997), 130 - 165.

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

[50] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* 3 (1965), 1-62.