



Involutions in finite simple groups as products of conjugates

Daniele Dona, Martin W. Liebeck & Kamilla Rekvényi

To cite this article: Daniele Dona, Martin W. Liebeck & Kamilla Rekvényi (2024) Involutions in finite simple groups as products of conjugates, Communications in Algebra, 52:9, 3750-3761, DOI: [10.1080/00927872.2024.2328803](https://doi.org/10.1080/00927872.2024.2328803)

To link to this article: <https://doi.org/10.1080/00927872.2024.2328803>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC



Published online: 20 Mar 2024.



Submit your article to this journal [↗](#)



Article views: 235



View related articles [↗](#)



View Crossmark data [↗](#)

Involutions in finite simple groups as products of conjugates

Daniele Dona^a, Martin W. Liebeck^b, and Kamilla Rekvényi^b

^aAlfréd Rényi Institute of Mathematics, Budapest, Hungary; ^bImperial College London, London, UK

ABSTRACT

Let G be a finite non-abelian simple group, C a non-identity conjugacy class of G , and Γ_C the Cayley graph of G based on $C \cup C^{-1}$. Our main result shows that in any such graph, there is an involution at bounded distance from the identity.

ARTICLE HISTORY

Received 13 February 2024
Communicated by Mandi Schaeffer Fry

KEYWORDS

Cayley graphs; conjugacy classes; finite simple groups; involutions

2020 MATHEMATICS

SUBJECT CLASSIFICATION

20D06; 05C25; 20C15; 20E34

1. Introduction

For a finite group G with a generating set S that is closed under inversion, the Cayley graph $\Gamma(G, S)$ is defined to be the graph with vertex set G and edge set consisting of all $\{g, gs\}$ for $g \in G, s \in S$. This paper is a contribution to the study of the Cayley graphs of finite (non-abelian) simple groups G in the case where the generating set is of the form $C \cup C^{-1}$, where C is a non-identity conjugacy class of G . By [12], the diameter of such a Cayley graph is bounded above by $c \log |G| / \log |C|$, where c is an absolute constant. Also, for G a simple group of Lie type of rank l , an explicit upper bound, linear in l , for the diameters of all such Cayley graphs, is obtained in [8].

Here we study a more refined question concerning distances in these Cayley graphs $\Gamma_C := \Gamma(G, C \cup C^{-1})$ for simple groups G . For a subset $H \subseteq G$ not containing the identity, define a number $d(H)$ as follows. Let d_C denote the distance function on Γ_C , and set

$$d_C(H) = \min \{d_C(1, h) : h \in H\},$$

so that $d_C(H) = \min \{k : (C \cup C^{-1})^k \cap H \neq \emptyset\}$. Now define

$$d(H) = \max_{C \neq 1} d_C(H).$$

In other words, for every non-identity conjugacy class C of G , we have $(C \cup C^{-1})^k \cap H \neq \emptyset$ for some $k \leq d(H)$.

Clearly, there are some subsets H for which $d(H)$ is equal to $d_G := \max_{C \neq 1} \text{diam}(\Gamma_C)$, hence grows with the rank of G . Our main results show that this is not the case when $H = \text{Inv}(G)$, the set of involutions in the simple group G . Indeed, we show that $d(\text{Inv}(G))$ is bounded above by an absolute constant: explicitly, by 2 for alternating groups $G = A_n$ ($n \geq 6$), by 3 for $G = A_5$, and by 12 for classical

CONTACT Martin W. Liebeck  m.liebeck@imperial.ac.uk  Imperial College London, 180 Queen's Gate, South Kensington, London, SW7 2AZ, UK.

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

groups. Constants for G an exceptional group of Lie type and G sporadic already follow from existing results: see [Proposition 1.6](#). Thus for any non-identity conjugacy class C of a finite simple group G , there is a bounded product of elements of $C \cup C^{-1}$ that is an involution.

We now state our results. For classical groups, our proofs are inductive, which necessitates consideration of the general linear, unitary and orthogonal groups rather than just the simple groups. For $\epsilon = \pm$, $GL_n^\epsilon(q)$ denotes $GL_n(q)$ if $\epsilon = +1$, and $GU_n(q)$ if $\epsilon = -1$, with similar notation for $SL_n^\epsilon(q)$. Also when n is even, $O_n^\epsilon(q)$ denotes the orthogonal group $O_n^\pm(q)$ as usual, and when n is odd it denotes the orthogonal group $O_n(q)$. For a subgroup $S \leq G$ and $g \in G$, we write $g^S = \{x^{-1}gx : x \in S\}$.

Theorem 1.1. *Let $G = GL_n^\epsilon(q)$ and $S = SL_n^\epsilon(q)$, with $n \geq 2$ and $(n, q, \epsilon) \neq (2, 2, \epsilon)$ or $(3, 2, -)$. Let $g \in G \setminus Z(G)$, and $C = g^S$. Then there exists an involution $t \in S$, with $t \notin Z(S)$ when $n \neq 2$, and elements $x_i \in C$, $y_i \in C^{-1}$ for $1 \leq i \leq 6$, such that $\prod_{i=1}^6 x_i y_i = t$.*

Theorem 1.2. *Let $G = Sp_{2m}(q)$, with $m \geq 2$. Let $g \in G \setminus Z(G)$, and $C = g^G$. Then there exists an involution $t \in G \setminus Z(G)$, and elements $x_i \in C$, $y_i \in C^{-1}$ for $1 \leq i \leq 6$, such that $\prod_{i=1}^6 x_i y_i = t$.*

Theorem 1.3. *Let $G = O_n^\epsilon(q)$ and $S = \Omega_n^\epsilon(q)$, with $n \geq 7$, and q odd if n is odd. Let $g \in G \setminus Z(G)$, and $C = g^S$. Then there exists an involution $t \in S \setminus Z(S)$, and elements $x_i \in C$, $y_i \in C^{-1}$ for $1 \leq i \leq 6$, such that $\prod_{i=1}^6 x_i y_i = t$.*

The following corollary follows directly from these theorems, except in the case where $G = PSL_2(q)$ with q odd, in which case $C^3 = G$ for all non-identity conjugacy classes C , by [[1](#), Theorem 4.2 (a)].

Corollary 1.4. *Let G be a classical simple group, and let $1 \neq g \in G$. Then there are 12 conjugates of $g^{\pm 1}$ with product equal to an involution. Thus $d(\text{Inv}(G)) \leq 12$.*

In [Section 5](#) we provide a different proof that for $G = PSL(n, q)$ and $1 \neq g \in G$, there is a product of at most 48 conjugates of $g^{\pm 1}$ that is equal to an involution (see [Theorem 5.1](#)). Although this bound 48 is worse than the bound in [Corollary 1.4](#), the proof is constructive, in the sense that it provides an algorithm that, given g , provides an explicit product of conjugates of g that is an involution.

For alternating groups we prove the following.

Theorem 1.5. *For all $g \in S_n \setminus 1$, there exists $h \in A_n$ such that $[g, h]$ has order 2, unless $n = 5$ and g is a 5-cycle. Thus $d(\text{Inv}(A_n)) = 2$ for $n \geq 6$, and $d(\text{Inv}(A_5)) = 3$.*

For the remaining simple groups, we note the following result, which follows directly from [[8](#), Theorem 2] (for exceptional groups of Lie type, including the Tits group ${}^2F_4(2)'$) and [[19](#)] (for sporadic groups).

Proposition 1.6. *If G is a simple group of exceptional Lie type, then $d(\text{Inv}(G)) \leq 376$; and if G is a sporadic simple group, then $d(\text{Inv}(G)) \leq 6$.*

Finally, we mention a consequence of our bounds on $d(\text{Inv}(G))$ for simple groups G . Namely, we obtain a new bound on the orbital diameters of primitive permutation groups of simple diagonal type, improving a result in [[15](#)]. See [Section 7](#) for details.

The layout of the paper is as follows. In [Sections 2–4](#) we prove [Theorems 1.1–1.3](#), and [Section 5](#) contains our constructive proof for $PSL_n(q)$. The proof of [Theorem 1.5](#) can be found in [Section 6](#), and the final section contains our result on orbital diameters.

2. Proof of Theorem 1.1

The proof will be inductive, and the following lemma is the $n = 2$ case, which forms the base for the induction.

Lemma 2.1. *Let $G = GL_2^{\mathbb{C}}(q)$ and $S = SL_2(q)$, with $q > 2$. If $g \in G \setminus Z(G)$, and $C = g^S$, then there exist elements $x_i \in C$, $y_i \in C^{-1}$ for $1 \leq i \leq 6$, such that*

$$\prod_{i=1}^6 x_i y_i = \begin{cases} -I, & \text{if } q \text{ is odd} \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & \text{if } q \text{ is even.} \end{cases}$$

Proof. First choose $h \in S$ such that $[g, h] \neq I$, and note that $[g, h] \in CC^{-1} \subseteq S$. If q is even, then $(CC^{-1})^3 = S$ by [1, Theorem 4.2 (a)], and the conclusion follows.

Now assume that q is odd, and let $x = [g, h]$. If $x = -I$, there is nothing to prove, so suppose $x \neq -I$. By [1, p. 43], the number of solutions to the equation $x_1 \cdots x_6 = -I$ with each $x_i \in x^S$ is equal to

$$\frac{|x^S|^6}{|S|} \sum_{\chi \in \text{Irr}(S)} \frac{\chi(x)^6 \chi(-I)}{\chi(1)^5}.$$

Using the character table of S (see for example [3, p. 229]), we check that this sum is positive, and the result follows. $\square$

Proof of Theorem 1.1

We prove the theorem first for $G = GL_n(q)$, and then indicate the changes needed to handle $GU_n(q)$. Let $G = GL_n(q) = GL(V)$ and $S = SL_n(q)$, with $(n, q) \neq (2, 2)$, let $g \in G \setminus Z(G)$, and $C = g^S$. The proof goes by induction on n . The base case $n = 2$ is given by Lemma 2.1, so assume $n \geq 3$. Assume also that (n, q) is not $(3, 2)$, $(3, 3)$, $(3, 4)$, $(3, 5)$, $(4, 2)$, or $(4, 3)$. In these cases the result follows by calculations in GAP [6].

(1) Consider first the case where g is *decomposable*, i.e. g lies in a proper subgroup $GL_{n_1}(q) \times GL_{n_2}(q)$ of G preserving a decomposition $V = V_1 \oplus V_2$, where $\dim V_i = n_i$. Say $g = g_1 \oplus g_2$, where $g_i \in GL(V_i)$.

Assume that there exists i such that $g_i \notin Z(GL(V_i))$, say $i = 1$. Then by induction, one of the following holds:

(i) there is an involution $t_1 \in SL(V_1)$, and $SL(V_1)$ -conjugates x'_j and y'_j ($1 \leq j \leq 6$) of g_1 and g_1^{-1} respectively, such that $\prod_1^6 x'_j y'_j = t_1$;

(ii) $(n_1, q) = (2, 2)$.

In case (i), if we let $x_j = x'_j \oplus g_2$ and $y_j = y'_j \oplus g_2^{-1}$, then these are S -conjugates of g and g^{-1} , with product $t_1 \oplus 1$, a non-central involution in S . In case (ii) we have $n \geq 5$ by assumption, so $n_2 \geq 3$. If $g_2 \neq 1$, work as above with g_2 instead of g_1 ; and if $g_2 = 1$, we can replace g_1 by $(g_1, 1) \in GL_3(2)$ and proceed as above.

Now assume that $g_i \in Z(GL(V_i))$ for $i = 1, 2$, so $g = \lambda I_{n_1} \oplus \mu I_{n_2}$ for some $\lambda, \mu \in \mathbb{F}_q^*$. Then we can replace g by the S -conjugate $h_1 \oplus h_2$, where $h_1 = (\lambda I_{n_1-1}, \mu)$, $h_2 = (\lambda, \mu I_{n_2-1})$, and proceed as in the previous paragraph.

(2) Now consider the case where g is *indecomposable*, i.e. does not preserve any proper decomposition $V = V_1 \oplus V_2$. Let $g = su$ be the Jordan decomposition of g , where s is semisimple, u is unipotent, and $us = su$. The structure of the centralizer $C_G(s)$ is well known, and we have

$$u \in C_G(s) = \prod_{i=1}^k GL_{m_i}(q^{d_i}) \leq \prod_{i=1}^k GL_{m_i d_i}(q) \leq G,$$

where $\sum m_i d_i = n$. Since g is indecomposable, we have $k = 1$, so $C_G(s) = GL_m(q^d)$ with $md = n$, and also u is a single Jordan block $J_m \in GL_m(q^d)$. Moreover, if $2 < m < n$, or if $m = 2$ with q even, then

we can apply induction in the group $GL_m(q^d)$ to obtain the conclusion of the theorem, so assume that $m = 1, 2$ or n (with q odd if $m = 2$).

If $m = 1$ then $g = s$ and $C_G(g) = GL_1(q^n)$; if $m = n$ then $g = \lambda J$ with J a unipotent Jordan block, and $C_G(g)$ has order $(q - 1)q^{n-1}$; and if $m = 2$ then $C_G(g) = C_{GL_2(q^d)}(J_2)$ has order $(q^d - 1)q^d$. In all cases,

$$|C_G(g)| < q^n. \quad (1)$$

Suppose first that $m = n$, so $g = \lambda J$. Let $C = J^S$, the conjugacy class of J in $S = SL_n(q)$, and let t be a non-central involution in S . By [1, p. 43], the number of solutions to the equation $\prod_1^6 x_i y_i = t$ with $x_i \in C, y_i \in C^{-1}$ is

$$N := \frac{|C|^{12}}{|S|} \sum_{\chi \in \text{Irr}(S)} \frac{\chi(J)^6 \chi(J^{-1})^6 \chi(t)}{\chi(1)^{11}}. \quad (2)$$

To show that this sum is nonzero, we use the following facts; in (c), $k(S)$ denotes the number of conjugacy classes in S :

- (a) $|\chi(J)| = |\chi(J^{-1})| \leq q^{n/2}$ for all $\chi \in \text{Irr}(S) \setminus 1$, by (1);
- (b) $\chi(1) \geq \frac{q^n - 1}{q - 1} - 1 > q^{n-1}$ for all $\chi \in \text{Irr}(S) \setminus 1$, by [18, Theorem 3.1];
- (c) $k(S) \leq 2.5q^{n-1}$, by [5, Proposition 3.6].

It follows from (a)-(c) that

$$\sum_{\chi \in \text{Irr}(S) \setminus 1} \frac{|\chi(J)^6 \chi(J^{-1})^6|}{\chi(1)^{10}} \leq \frac{2.5q^{n-1}(q^{n/2})^{12}}{q^{10(n-1)}} = 2.5q^{-3n+9}.$$

This is less than 1 when $n \geq 4$, so the sum in (2) is nonzero, and the conclusion follows in this case. For $n = 3$, the character table of $SL_3(q)$ is available in [14]. We can replace the bound for $|\chi(J)| = |\chi(J^{-1})|$ by $2q + 1$ for all $\chi \in \text{Irr}(S) \setminus 1$, so the sum in (2) is nonzero for $q \geq 7$ and the conclusion follows.

Now suppose that $m = 1$, so $g = s$ and $C_G(g) = GL_1(q^n)$. The determinant map $C_G(g) \mapsto \mathbb{F}_q^*$ is surjective, so we have $g^G = g^S$. Hence, as above, it is sufficient to prove that $N' > 0$, where

$$N' := \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)^6 \chi(g^{-1})^6}{\chi(1)^{10}}. \quad (3)$$

The contribution of the $q - 1$ linear characters of G to N' is $q - 1$. For the nonlinear characters $\chi \in \text{Irr}(G)$, again using [5, 18], we have

- (a) $|\chi(g)| = |\chi(g^{-1})| \leq q^{n/2}$;
- (b) $\chi(1) \geq \frac{q^n - 1}{q - 1} - 1 > q^{n-1}$;
- (c) $k(G) \leq q^n$.

Hence the contribution of the nonlinear characters to N' is of absolute value less than

$$\frac{q^n (q^{n/2})^{12}}{q^{10(n-1)}} = q^{-3n+10},$$

which is less than 1 for $n \geq 4$. For $n = 3$, the result follows as again by [17] we can replace the bound for $|\chi(g)| = |\chi(g^{-1})|$ by 6 for all nonlinear $\chi \in \text{Irr}(G)$.

Finally, suppose $m = 2$ with q odd. Here $C_G(g) = C_{GL_2(q^d)}(J_2)$ and the image of the determinant map $C_G(g) \mapsto \mathbb{F}_q^*$ has index 2 in $\mathbb{F}_q^*$. It follows that $g^S = g^{G^*}$, where G^* is of index 2 in G . The argument of the previous paragraph goes through with G^* replacing G , and replacing the inequality in (c) by $k(G^*) \leq \frac{1}{2}(q^n + 3q^{n-1})$ (see [5, Corollary 3.7]).

This completes the proof of the theorem for $G = GL_n(q)$.

We now indicate the changes in the proof needed for $G = GU_n(q)$. First, we need to deal computationally with some small cases, namely

$$n = 3 (q \leq 7), n = 4 (q \leq 3), \text{ and } (n, q) = (5, 2), (6, 2). \quad (4)$$

We now assume none of these cases holds. If g is decomposable, i.e. g lies in a proper subgroup $GU_{n_1}(q) \times GU_{n_2}(q)$ of G preserving an orthogonal decomposition $V = V_1 \oplus V_2$, then we argue by induction in similar fashion to the $GL_n(q)$ case, as follows. Write $g = g_1 \oplus g_2$ with $g_i \in GU(V_i)$, and assume first that there exists i such that $g_i \notin Z(GU(V_i))$, say $i = 1$. Then by induction, one of the following holds:

(i) there is an involution $t_1 \in SU(V_1)$, and $SU(V_1)$ -conjugates x'_j and y'_j ($1 \leq j \leq 6$) of g_1 and g_1^{-1} respectively, such that $\prod_1^6 x'_j y'_j = t_1$;

(ii) $(n_1, q) = (3, 2)$.

In case (i), if we let $x_j = x'_j \oplus g_2$ and $y_j = y'_j \oplus g_2^{-1}$, then these are S -conjugates of g and g^{-1} , with product $t_1 \oplus 1$, a non-central involution in S . In case (ii) we have $n \geq 7$ by assumption, so $n_2 \geq 4$. If $g_2 \notin Z(GU(V_2))$, work as above with g_2 instead of g_1 ; otherwise, $g_2 = \omega I_{n_2}$, we can replace g_1 by $(g_1, \omega) \in GU_4(2)$ and proceed as above.

Now assume that $g_i \in Z(GU(V_i))$ for $i = 1, 2$, so $g = \lambda I_{n_1} \oplus \mu I_{n_2}$ for some $\lambda, \mu \in \mathbb{F}_{q^2}$. Then we can replace g by the S -conjugate $h_1 \oplus h_2$, where $h_1 = (\lambda I_{n_1-1}, \mu)$, $h_2 = (\lambda, \mu I_{n_2-1})$, and proceed as in the previous paragraph.

So assume g is indecomposable, and let $g = su$ be the Jordan decomposition of g . Then

$$u \in C_G(s) = \prod_{i=1}^k GL_{m_i}(q^{2d_i}) \times \prod_{i=1}^l GU_{r_i}(q^{e_i}) \leq \prod_{i=1}^k GL_{2m_i d_i}(q) \times \prod_{i=1}^l GU_{r_i e_i}(q) \leq G,$$

where $\sum 2m_i d_i + \sum r_i e_i = n$ and all e_i are odd. Since g is indecomposable, $k + l = 1$. As in the GL case, we can apply induction to see that one of the following holds:

(i) $C_G(s) = GU_n(q)$, and $g = \lambda J$ where J is a single Jordan block in G and $\lambda \in \mathbb{F}_{q^2}$;

(ii) $C_G(s) = GL_1(q^n)$ with n even, or $GU_1(q^n)$ with n odd;

(iii) $C_G(s) = GL_2(q^{2d})$ ($n = 4d$) or $GU_2(q^e)$ ($n = 2e$, e odd), where q is odd, and u is a single Jordan block $J_2 \in C_G(s)$.

The maximal possible value of $|C_G(g)|$ is its value in (i), namely $(q+1)q^{n-1}$.

Consider first case (i). We need to argue as in the GL case that the sum in (2) is nonzero. To do this we use the facts:

- $\chi(1) \geq \frac{q^n - q}{q+1}$ for all $\chi \in \text{Irr}(S) \setminus 1$, by [18, Theorem 4.1];
- $k(S) \leq 8.26q^{n-1}$, by [5, Proposition 3.10].

Hence

$$\sum_{\chi \in \text{Irr}(S) \setminus 1} \frac{|\chi(J)^6 \chi(J^{-1})^6|}{\chi(1)^{10}} \leq \frac{8.26q^{n-1}((q+1)q^{n-1})^6}{((q^n - q)/(q+1))^{10}}.$$

One checks that the right hand side is less than 1 unless $n = 3$ or $(n, q) = (7, 2), (5, 3), (4, 5), (4, 4)$ or as in the exclusions in (4). For $n = 3$, the character table of $SU_3(q)$ is available in [14]. We can replace the bound for $|\chi(g)| = |\chi(g^{-1})|$ by $\frac{4q+1}{3}$ for all $\chi \in \text{Irr}(S) \setminus 1$, so the sum in (2) is nonzero for $q \geq 7$ and the conclusion follows. For $(n, q) = (7, 2), (5, 3), (4, 5), (4, 4)$ we can calculate $k(S)$ using GAP, and by replacing $8.26q^{n-1}$ with these exact values we find that the sum in (2) is nonzero. This completes the proof in case (i).

In case (ii) we have $g^S = g^G$ and as before we need to show that the sum in (3) is positive. For this we argue as in the previous paragraph, using the bound $k(G) \leq 8.26q^n$ from [5, Proposition 3.9], for $n = 3$ also the bound $|\chi(g)| = |\chi(g^{-1})| \leq 6$ from [4], and for $(n, q) = (4, 4)$ using the fact that $k(G) = 470$ from a computation in GAP.

Finally, in case (iii) as in the GL case we have $g^S = g^{G^*}$, where G^* is of index 2 in G , and we argue in the usual way, using the bound $k(G^*) \leq 4.13q^{n-1}(q+1)$ from [5, Corollary 3.11] (and also for $(n, q) = (5, 2)$ and $(4, 4)$, the exact values of $k(G^*)$, computed in GAP).

This completes the proof of Theorem 1.1.

3. Proof of Theorem 1.2

We prove by induction on m the statement of [Theorem 1.2](#), but including also the case where $m = 1$ (which is already proved in [Lemma 2.1](#)). So let $G = Sp_{2m}(q) = Sp(V)$ with $m \geq 2$, let $g \in G \setminus Z(G)$ and $C = g^G$. Our approach is similar to that in the previous section.

(1) Consider first the case where g is decomposable, i.e. g lies in a proper subgroup $Sp_{2m_1}(q) \times Sp_{2m_2}(q)$ of G preserving an orthogonal decomposition $V = V_1 \oplus V_2$, where $\dim V_i = 2m_i$. Say $g = g_1 \oplus g_2$, where $g_i \in Sp(V_i)$. Then induction gives the conclusion in exactly the same way as in (1) of the previous section.

(2) Now suppose g is indecomposable, and let $g = su$ be the Jordan decomposition. The structure of $C_G(s)$ is as follows: if for $\epsilon \in \{\pm 1\}$, V_ϵ denotes the ϵ -eigenspace of s , then V_ϵ is non-degenerate and

$$\begin{aligned} C_G(s) &= Sp(V_1) \times Sp(V_{-1}) \times \prod_{i=1}^k GL_{r_i}(q^{d_i}) \times \prod_{i=1}^l GU_{s_i}(q^{e_i}) \\ &\leq Sp(V_1) \times Sp(V_{-1}) \times \prod_{i=1}^k Sp_{2r_i d_i}(q) \times \prod_{i=1}^l Sp_{2s_i e_i}(q) \leq G. \end{aligned}$$

Since g is indecomposable, there is only one factor in $C_G(s)$, and so one of the following holds:

- (i) $s = \pm I$, $C_G(s) = G$, and u is an indecomposable unipotent element of G ;
- (ii) $C_G(s) = GL_r(q^d)$ or $GU_r(q^d)$ with $rd = m$, and u is a single Jordan block $J_r \in C_G(s)$.

In case (i), we use [7, Proposition 2.3, Theorem 3.1] for the classification of unipotent classes in G . If q is odd, the indecomposable such classes are those labelled $V_\beta(2m)$ (a single Jordan block) and $W(m)$ for m odd (two blocks of size m); for the latter class, $g = \pm W(m)$ lies in a subgroup $GL_m(q)$ of G , and the conclusion follows from [Theorem 1.1](#). If q is even, the indecomposable unipotent classes are those labelled $V_\beta(2m)$, $W(m)$ and $W_\alpha(m)$ (m odd); elements in the classes $W(m)$ and $W_\alpha(m)$ lie in subgroups $GL_m(q)$ and $GU_m(q)$ respectively, so again the result follows from [Theorem 1.1](#) in these cases.

In summary, in case (i) we may take it that $g = \pm V_\beta(2m)$, a single Jordan block. The centralizer order is $|C_G(g)| = 2q^m$ (see [11, Chapter 7]).

In case (ii), u is a single Jordan block $J_r \in C_G(s) = GL_r^\pm(q^d)$ with $rd = m$. The maximal centralizer order occurs when $C_G(s) = GU_m(q)$, and is $(q+1)q^{m-1}$. We conclude that in both cases (i) and (ii),

$$|C_G(g)| \leq 2q^m \text{ and } \dim C_V(g) \leq 1. \quad (5)$$

At this point we use character theory, as in the previous section. Again, we need to show that the sum in (3) is positive.

First assume that q is odd. Here we use the following “gap” result taken from [18, 5.2]: $G = Sp_{2m}(q)$ has a collection $\mathcal{W}$ of four irreducible characters of degree $\frac{1}{2}(q^m \pm 1)$ (called Weil characters), such that for all $1 \neq \chi \in \text{Irr}(G) \setminus \mathcal{W}$, we have $\chi(1) \geq \frac{(q^m-1)(q^m-q)}{2(q+1)}$. We break the sum in (3) into separate parts:

$$N' = 1 + \sum_{\chi \in \mathcal{W}} \frac{\chi(g)^6 \chi(g^{-1})^6}{\chi(1)^{10}} + \sum_{1 \neq \chi \in \text{Irr}(G) \setminus \mathcal{W}} \frac{\chi(g)^6 \chi(g^{-1})^6}{\chi(1)^{10}} = 1 + \Sigma_1 + \Sigma_2. \quad (6)$$

To bound Σ_1 , we use the following fact (see for example [13, p. 79]): for $\chi \in \mathcal{W}$, there are complex numbers a, b of modulus 1 such that for all $x \in G$,

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

and hence $|\chi(g)| \leq \frac{1}{2}q^{1/2}$. It follows that

$$|\Sigma_1| \leq \frac{4(q^{1/2}/2)^{12}}{((q^m-1)(q^m-q)/2(q+1))^{10}}.$$

Now we bound Σ_2 . Here we use the bound $k(G) \leq 10.8q^m$ from [5, Proposition 3.12]. Noting that $|\chi(g)| \leq |C_G(g)|^{1/2} \leq (2q^m)^{1/2}$, we see that

$$|\Sigma_2| \leq \frac{10.8q^m \cdot (2q^m)^6}{((q^m-1)(q^m-q)/2(q+1))^{10}}.$$

We now check that for $m \geq 2$ and q odd, with $(m, q) \neq (2, 3)$, we have $|\Sigma_1| + |\Sigma_2| < 1$ (the case $(m, q) = (2, 3)$ was handled using GAP). Hence the sum N' in (6) is positive, completing the proof of [Theorem 1.2](#) when q is odd.

Now assume q is even. Here we use [18, Theorem 5.5], which states that provided $(m, q) \neq (2, 2)$, we have $\chi(1) \geq \frac{(q^m-1)(q^m-q)}{2(q+1)}$ for all $\chi \in \text{Irr}(G) \setminus 1$. Also $k(G) \leq 15.2q^m$ by [5, Theorem 3.13], and hence

$$\sum_{\chi \in \text{Irr}(G) \setminus 1} \frac{|\chi(g)^6 \chi(g^{-1})^6|}{\chi(1)^{10}} \leq \frac{15.2q^m \cdot (2q^m)^6}{((q^m-1)(q^m-q)/2(q+1))^{10}}.$$

Once again we check that this is less than 1 for $m \geq 2$ and q even, with $(m, q) \neq (2, 2)$ or $(3, 2)$ for which cases the result follows by calculations in GAP.

This completes the proof of [Theorem 1.2](#).

4. Proof of Theorem 1.3

This is similar to the previous section, but requires a bit more care in some places. For the induction argument we shall need the following lemma.

Lemma 4.1. *Let $G = O_4^\epsilon(q)$ and $S = \Omega_4^\epsilon(q)$, with $q > 3$. Let $g \in G \setminus Z(G)$, and $C = g^S$. Then there exists a non-central involution $t \in S$, and elements $x_i \in C$, $y_i \in C^{-1}$ for $1 \leq i \leq 6$, such that $\prod_{i=1}^6 x_i y_i = t$.*

Proof. We have $O_4^\epsilon(q) \cong \Omega_4^\epsilon(q).2^a$, where $a = (2, q-1)$, and $\Omega_4^-(q) \cong \text{PSL}_2(q^2)$, $\Omega_4^+(q) \cong \text{SL}_2(q) \circ \text{SL}_2(q)$. Choose $x \in S$ such that $h := [g, x] \in S \setminus Z(S)$. It is sufficient to find 6 conjugates of h with product equal to a non-central involution in S . This can be done, as was shown in the proof of [Lemma 2.1](#). $\square$

We now prove [Theorem 1.3](#). Let $G = O_n^\epsilon(q)$ and $S = \Omega_n^\epsilon(q)$, with $n \geq 5$, and q odd if n is odd. Let $g \in G \setminus Z(G)$, and $C = g^S$. We assume that

$$(n, q) \neq (7, 3), (8, 2), (8, 3). \quad (7)$$

These cases are handled by computation using GAP.

As usual we proceed by induction on n . The cases $n = 5$ and $n = 6$ are covered by [Theorems 1.1](#) and [1.2](#) in view of the isomorphisms $\Omega_5(q) \cong \text{PSp}_4(q)$ and $\text{P}\Omega_6^\epsilon(q) \cong \text{PSL}_4^\epsilon(q)$. So assume $n \geq 7$.

(1) Consider first the case where g is decomposable, i.e. g lies in a proper subgroup $O_{n_1}(q) \times O_{n_2}(q)$ of G preserving an orthogonal decomposition $V = V_1 \oplus V_2$. Say $g = g_1 \oplus g_2$, where $g_i \in O(V_i)$. We need to be a little careful in applying induction in this case. Let $n_1 \geq n_2$, so $n_1 \geq 4$.

Suppose $g_1 \notin Z(O(V_1))$. If $n_1 \geq 5$, we can apply induction to find 12 conjugates of $g_1^{\pm 1}$ with product a non-central involution in $\Omega(V_1)$, giving the conclusion in the usual way. If $n_1 = 4$, then $q > 3$ by the exclusions in (7), and so the conclusion follows in the same way, using [Lemma 4.1](#).

Now suppose $g_1 \in Z(O(V_1))$, so $g_1 = \delta I_{n_1}$ with $\delta \in \{1, -1\}$. Take any proper orthogonal decomposition $V_1 = W_1 \oplus W_2$ with $\dim W_1 = 2$. Now replacing g_1 by $g'_1 = \delta I_{W_2} \oplus g_2$, and g_2 by δI_{W_1} , the argument of the previous paragraph goes through.

(2) Now suppose g is indecomposable, and let $g = su$ be the Jordan decomposition. As in the previous section, we have

$$\begin{aligned} C_G(s) &= O(V_1) \times O(V_{-1}) \times \prod_{i=1}^k \text{GL}_{r_i}(q^{d_i}) \times \prod_{i=1}^l \text{GU}_{s_i}(q^{e_i}) \\ &\leq O(V_1) \times O(V_{-1}) \times \prod_{i=1}^k \text{O}_{2r_i d_i}(q) \times \prod_{i=1}^l \text{O}_{2s_i e_i}(q). \end{aligned}$$

Since g is indecomposable, there is only one factor in $C_G(s)$, and so one of the following holds:

- (i) $s = \pm I$, $C_G(s) = G$, and u is an indecomposable unipotent element of G ;
- (ii) $C_G(s) = \text{GL}_r(q^d)$ or $\text{GU}_r(q^d)$ with $2rd = n$, and u is a single Jordan block $J_r \in C_G(s)$.

In case (i), we see as in the previous section, using [7, Proposition 2.4, Theorem 3.1], that we may take g to be a single Jordan block $\pm V(2m+1)$ ($n = 2m+1$, q odd) or $V_\beta(2m)$ ($n = 2m$, q even). In both cases,

$|C_G(g)| \leq 2q^m$. In case (ii), as in the previous section we have $|C_G(g)| \leq (q+1)q^{m-1}$, where $n = 2m$. We conclude that for both (i) and (ii),

$$|C_G(g)| \leq 2q^m, \text{ where } n = 2m \text{ or } 2m+1. \quad (8)$$

We have $g^S = g^{G^*}$ for some G^* such that $S \leq G^* \leq G$ and $g \in G^*$. In order to apply the usual character-theoretic argument, we need lower bounds on the irreducible character degrees of G^* . These are provided by [18, Theorems 6.1 and 7.6]: for any nonlinear irreducible character χ of G^* , we have $\chi(1) \geq d_G$, where d_G is defined as follows:

(i) for $G = O_{2m+1}(q)$ with $m \geq 3$, q odd,

$$d_G = \begin{cases} (q^{2m} - 1)/(q^2 - 1), & \text{if } q \geq 5 \\ (q^m - 1)(q^m - q)/2(q + 1), & \text{if } q = 3 \end{cases}$$

(ii) for $G = O_{2m}^\epsilon(q)$ with $m \geq 4$ and $(m, q, \epsilon) \neq (4, 2, +)$,

$$d_G = \begin{cases} (q^m - \epsilon)(q^{m-1} + \epsilon q)/(q^2 - 1), & \text{if } (q, \epsilon) \neq (2, +), (3, +) \\ (q^m - 1)(q^{m-1} - 1)/(q^2 - 1), & \text{if } (q, \epsilon) = (2, +) \text{ or } (3, +) \end{cases}$$

Also $k(G^*) \leq 15q^m$ by [5, Theorems 3.14, 3.17, 3.21]. Using this, together with the bound $|\chi(g)| \leq |C_G(g)|^{1/2} \leq (2q^m)^{1/2}$, it follows that

$$\sum_{\chi \in \text{Irr}(G^*), \chi(1) > 1} \frac{|\chi(g)^6 \chi(g^{-1})^6|}{\chi(1)^{10}} \leq \frac{15q^m \cdot (2q^m)^6}{(d_G)^{10}}.$$

We check that this is less than 1 unless (n, q) is as in the exclusions (7), and the conclusion of the theorem follows in the usual way.

This completes the proof of [Theorem 1.3](#).

5. A constructive algorithm

In this section we give an alternative proof to the case $\epsilon = +1$ of [Theorem 1.1](#). Although it requires a larger number of conjugates of $g^{\pm 1}$, the conjugating elements are explicitly determined up to possibly passing to generalized Jordan form, for which algorithms are well-known (see for instance [16]). One might be able to apply the method to other groups of Lie type, although with considerably more work.

We fix some notation: I_d is the $d \times d$ identity matrix, E_{ij} is the matrix having ij -entry 1 and 0 elsewhere, and $A \oplus B$ denotes the diagonal join of the matrices A, B .

Theorem 5.1. *Let $G = GL_n(q)$ and $S = SL_n(q)$, with $n \geq 2$ and $(n, q) \neq (2, 2), (2, 3)$. Let $g \in G \setminus Z(G)$, and $C = g^S$. Then, for some $k \leq 48$, there exists $t \in (CC^{-1})^k \setminus Z(G)$ such that $t^2 \in \{I_n, -I_n\}$.*

Proof. Note first that there exists $h \in S$ such that $[g, h] \in S \setminus Z(S)$. Therefore it is enough to prove the conclusion of the theorem with $g \in S$ and $k \leq 24$.

Assume first that $n = 2$. For $x \in \mathbb{F}_q$, define $h(x) = I_2 + xE_{1,2}$. For every $g = (g_{ij}) \in SL_2(q)$, if $g_{21} \neq 0$ then $g' = h(-g_{11}g_{21}^{-1})gh(-g_{11}g_{21}^{-1})^{-1}$ is such that $g'_{11} = 0$. Thus, every class contains an element of at least one of the two forms

$$g = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \quad g = \begin{pmatrix} 0 & -a^{-1} \\ a & b \end{pmatrix}. \quad (9)$$

Suppose first that $g = h(x)$ with $x \neq 0$. If q is even, this element is an involution already. If q is odd, then there exists $\alpha \in \{-1, 2, -2\}$ that is a nonzero square in $\mathbb{F}_q$; let $\beta = \frac{2}{\alpha} \in \mathbb{Z}$, and let $\gamma \in \mathbb{F}_q^*$ satisfy $\gamma^2 x^2 = \alpha$. Define

$$s(x) := \begin{pmatrix} -\gamma x & x - \gamma^{-1} \\ \gamma & -1 \end{pmatrix}, \quad t(x) := h(x)s(x)h(x)^\beta s(x)^{-1} = \begin{pmatrix} 1 & x \\ -2x^{-1} & -1 \end{pmatrix}.$$

Then $t(x)^2 = -I_2$, proving the result in this case (with $k = 3$).

Now suppose that g is as in the first case of (9), with $a \neq 1$. Define

$$h_1 := h(1), \quad h_2 := h(a^{-1}b), \quad h_3 := \begin{pmatrix} c & (c^2 - 1)ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix},$$

where c is to be chosen below. If $a \neq \pm 1$, then $h_1gh_1^{-1}g^{-1} = h(1 - a^2)$ with $1 - a^2 \neq 0$. And if $a = -1$ then $b \neq 0$, and $g^2 = h(-2b)$ with $-2b \neq 0$ because q must be odd (or else we would have $a = 1$). Hence the result follows from the previous paragraph.

Finally, suppose that g is as in the second case of (9). If $b = 0$, then $g^2 = -I_2$. If $b \neq 0$ and q is odd, then $(h_2gh_2^{-1}g)^2 = h(4a^{-1}b)$ with $4a^{-1}b \neq 0$. If $b \neq 0$ and q is even, take any $c \neq 0$ such that $c^2 \neq 1$ (note that c exists because $(n, q) \neq (2, 2)$ by hypothesis). Then $h_3gh_3^{-1}g^{-1}$ is as in the first case of (9) with c^2, c^{-2} on the diagonal; also $c^2 \neq \pm 1$, so this case is covered by the previous paragraph, and gives the conclusion with $k = 12$. This completes the argument for $n = 2$.

Now assume that $n > 2$. The cases $(n, q) \in \{(3, 2), (3, 4), (4, 2), (4, 3)\}$ can be treated by direct calculation, so exclude these from consideration. Following the proof of Theorem 1.1, we argue by induction on n and descend by decomposing g or by going to the pairs (n, q) above, unless we are in one of the following situations, corresponding respectively to $m = 1, 2, n$:

- (1) $g = C(f)$, the companion matrix of an irreducible polynomial $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$ of degree $d = n$ (in particular $c_0 \neq 0$);
- (2) $g = \begin{pmatrix} C(f) & C(f) \\ 0 & C(f) \end{pmatrix}$, where $f(x)$ has degree $d = \frac{1}{2}n$;
- (3) $g = \lambda I_n + \lambda \sum_{i=1}^{n-1} E_{i,i+1}$ for some $\lambda \in \mathbb{F}_q^*$.

Start with case (1), and let us do all the calculations as an example. Take

$$s := I_{n-2} \oplus \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$

and note that $sg^{-1}s^{-1} = g^{-1} + c_0^{-1}E_{n-1,1} + E_{n-2,n}$. Then

$$\begin{aligned} sg^{-1}s^{-1}g &= (g^{-1} + c_0^{-1}E_{n-1,1} + E_{n-2,n})g \\ &= I_n + E_{n-2,n-1} - c_{n-1}E_{n-2,n} - E_{n-1,1} \\ &= I_{n-3} \oplus \begin{pmatrix} 1 & 1 & -c_{n-1} \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \\ &=: I_{n-3} \oplus r. \end{aligned}$$

Then for

$$r(y) := \begin{pmatrix} 0 & -1 & y \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad s(y) := I_{n-3} \oplus r(y),$$

we get

$$r(-1)r^{-1}r(-1)^{-1} \cdot r(0)rr(0)^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

and putting everything together we obtain in the end

$$\begin{aligned} &s(-1)g^{-1}s(-1)^{-1} \cdot s(0)gs(0)^{-1} \cdot s(1)g^{-1}s(1)^{-1} \cdot s(0)gs(0)^{-1} \\ &= s(-1) \cdot (sg^{-1}s^{-1}g)^{-1} \cdot s(-1)^{-1} \cdot s(0) \cdot (sg^{-1}s^{-1}g) \cdot s(0)^{-1} \end{aligned}$$

$$\begin{aligned}
&= I_{n-3} \oplus (r(-1)r^{-1}r(-1)^{-1} \cdot r(0)rr(0)^{-1}) \\
&= I_{n-2} \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},
\end{aligned}$$

reducing the problem to the case $n = 2$. Note that in the case $n = 2$ we obtained the conclusion for $h(1)$ with $k = 3$, so it follows here for g with $k = 12$.

In case (2), n must be even. Assume $n \geq 8$, take $s(y)$ as in the previous case and

$$\begin{aligned}
t_1 &:= I_{n-2} \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\
t_2 &:= E_{1,n} + (-1)^{n/2+1}E_{1,n/2+1} + \sum_{i=2}^{n/2-2} E_{i,n/2+i} + \sum_{i=1}^{n/2} E_{n/2-2+i,i} \\
&\quad - E_{n-2,n-2} - E_{n-1,n-1} + (1 + c_{n/2-1})E_{n-1,n} + E_{n,n}.
\end{aligned}$$

Then

$$h := t_2^{-1}g^{-1}t_2 \cdot (t_2^{-1}t_1)g(t_2^{-1}t_1)^{-1}, \quad s(0)hs(0)^{-1} \cdot s(-1)h^{-1}s(-1)^{-1} = t_1,$$

reducing again to $n = 2$; as above, this gives the conclusion with $k = 12$. For $n = 6$, use the same procedure replacing

$$t_2 := E_{1,4} + E_{2,3} + E_{2,6} + E_{3,1} + E_{4,2} + E_{6,6} - E_{4,4} - E_{5,5} + (1 + c_2)E_{5,6}.$$

For $n = 4$, take instead

$$t(y) := E_{2,1} + E_{3,3} + E_{4,4} - E_{1,4} - E_{2,1} + yE_{3,4}$$

and

$$t(0)gt(0)^{-1} \cdot t(-1)g^{-1}t(-1)^{-1} = I_2 \oplus \begin{pmatrix} 1 & 1 \\ c_0^{-1} & 1 + c_0^{-1} \end{pmatrix},$$

reducing again to $n = 2$; in this $n = 2$ case we only obtained the conclusion with $k = 12$, so it follows for g with $k = 24$.

In case (3), define

$$v(y) := E_{n-1,1} + E_{n-2,2} + \sum_{i=3}^n E_{n+1-i,i} + \sum_{i=3}^n (-1)^{i+1}E_{n,i} + yE_{n-1,2}.$$

Then

$$v(1)gv(1)^{-1} \cdot v(0)g^{-1}v(0)^{-1} = I_2 \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

reducing again to $n = 2$. □

6. Proof of Theorem 1.5

Let $1 \neq g \in S_n$. The result is easily verified for $n = 5$, so assume that $n \geq 6$. We can write $g = g_0g'$, where g_0 is as in the table below, and the cycles of g' are disjoint from those of g_0 . In the table, for each possible g_0 we provide an element $h \in A_n$ such that $[g, h]$ has order 2, as required. □

g_0	h	extra conditions
$(a_1, a_2, \dots, a_{k-1}, a_k)$	$(a_2, a_5)(a_3, a_6)$	$k \geq 6$
(a_1, a_2, a_3, a_4)	$(a_1, a_4)(a_2, a_3)$	
$(a_1, a_2, a_3, a_4, a_5)(a_6)$	(a_4, a_6, a_5)	
$(a_1, a_2, a_3, a_4, a_5)(a_6, a_7)$	(a_5, a_7, a_6)	
$(a_1, a_2, a_3, a_4, a_5)(a_6, a_7, a_8)$	$(a_4, a_8)(a_5, a_6)$	
$(a_1, a_2, a_3, a_4, a_5)(a_6, a_7, a_8, a_9, a_{10})$	$(a_4, a_{10})(a_5, a_6)$	
$(a_1, a_2, a_3)(a_4)$	(a_2, a_4, a_3)	
$(a_1, a_2, a_3)(a_4, a_5)$	$(a_1, a_3, a_2, a_5, a_4)$	
$(a_1, a_2, a_3)(a_4, a_5, a_6)$	$(a_2, a_6)(a_3, a_4)$	
$(a_1, a_2)(a_3, a_4)$	(a_2, a_4, a_3)	
$(a_1, a_2)(a_3)(a_4)$	$(a_1, a_3)(a_2, a_4)$	

7. A consequence on orbital diameters

Let G be a finite group acting transitively on set Ω . The orbitals of G are its orbits on $\Omega \times \Omega$, and the diagonal orbital is $\{(\alpha, \alpha) : \alpha \in \Omega\}$. For a non-diagonal orbital Γ , we define the corresponding orbital graph to be the undirected graph with vertex set Ω and edge set $\{(\alpha, \beta) : (\alpha, \beta) \in \Gamma\}$. By [2, Theorem 3.2A], the orbital graphs are all connected if and only if G acts primitively on Ω , in which case the *orbital diameter* of G is defined to be the supremum of the diameters of its orbital graphs (see [9]). Let us denote this by $\text{orbdiam}(G)$.

In [15], a study is made of the orbital diameters of primitive groups of simple diagonal type. We are able to use our results to improve one of the theorems in that paper, namely [15, Theorem 6.1], as follows. Let T be a non-abelian simple group, $k \geq 2$ an integer, and let $S(T, k) := T^k.S_k$ denote the semidirect product in which S_k permutes the coordinates in T^k naturally. Define $D = \{(t, \dots, t) : t \in T\}$, a diagonal subgroup of T^k , and let $\Omega = (T^k : D)$ be the set of right cosets of D in T^k . Then $S(T, k)$ acts primitively on Ω , where T^k acts by right multiplication, and S_k by permuting the components of coset representatives, and this is a primitive group of simple diagonal type (see [10]).

The following result determines the orbital diameter of $S(T, k)$ up to a multiplicative constant. Recall our definition $d_T := \max_{C \neq 1} \text{diam}(\Gamma_C)$ from Section 1.

Proposition 7.1. *Let $G = S(T, k) \cong T^k.S_k$ in the simple diagonal action defined above. Write $C = d(\text{Inv}(T))$. Then*

$$\frac{1}{2}(k-1)d_T \leq \text{orbdiam}(G) \leq 24C(k-1)d_T.$$

Proof. The lower bound is given by [15, Theorem 3.1]. An upper bound of $24(k-1)d_T^2$ is proved in [15, Theorem 6.1]. However, in the proof of that result, it is necessary to construct an involution as a product of length d_T of conjugates of some element, which accounts for one of the factors d_T in the upper bound. This factor can therefore be replaced by C , giving the required upper bound. $\square$

Note that d_T grows linearly in the rank of T for groups of Lie type, and linearly in the degree n of $T = A_n$, whereas C is bounded absolutely in all cases. The previous upper bound [15, Theorem 6.1] was quadratic in d_T .

Funding

Daniele Dona was funded by a Young Researcher Fellowship from the Alfréd Rényi Institute of Mathematics. Kamilla Rekvényi was supported by the UK Engineering and Physical Sciences Research Council grant number EP/W522673/1.

References

- [1] Arad, Z., Herzog, M., eds. *Products of Conjugacy Classes in Groups*, Springer Lecture Notes, 1112. Berlin: Springer-Verlag.
- [2] Dixon, J. D., Mortimer, B. (1996). *Permutation Groups*, volume 163 of Graduate Texts in Mathematics. New York: Springer-Verlag.
- [3] Dornhoff, L. (1971). *Group Representation Theory, Part A*. New York: Marcel Dekker Inc.
- [4] Ennola, V. (1963). On the characters of the finite unitary groups. *Ann. Acad. Sci. Fenn. Ser. A I* 323:35 pp.
- [5] Fulman, J., Guralnick, R. (2012). Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Amer. Math. Soc.* 364:3023–3070.
- [6] GAP — Groups. (2018). Algorithms, and Programming, Version 4.9.2, <http://www.gap-system.org>.
- [7] Gonshaw, S., Liebeck, M. W., O'Brien, E. A. (2017). Unipotent class representatives for finite classical groups. *J. Group Theory* 20:505–525.
- [8] Lawther, R., Liebeck, M. W. (1998). On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class. *J. Combin. Theory Ser. A* 83:118–137.
- [9] Liebeck, M. W., Macpherson, H. D., Tent, K. (2010). Primitive permutation groups of bounded orbital diameter. *Proc. London Math. Soc.* 100:216–248.
- [10] Liebeck, M. W., Praeger, C. E., Saxl, J. (1988). On the O’Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A* 44:389–396.
- [11] Liebeck, M. W., Seitz, G. M. (2012). *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*. Mathematical Surveys and Monographs, 180. Providence, RI: American Mathematical Society.
- [12] Liebeck, M. W., Shalev, A. (2001). Diameters of simple groups: sharp bounds and applications. *Ann. Math.* 154: 383–406.
- [13] Liebeck, M. W., Shalev, A. (2005). Character degrees and random walks in finite groups of Lie type. *Proc. London Math. Soc.* 90:61–86.
- [14] Simpson, W. A., Frame, J. S. (1973). The character tables for $SL(3, q)$, $SU(3, q^2)$, $PSL(3, q)$, $PSU(3, q^2)$. *Can. J. Math.* 25:486–494.
- [15] Rekvényi, K. (2022). On the orbital diameter of groups of diagonal type. *J. Combin. Theory Ser. A* 190:Paper No. 105636, 26 pp.
- [16] Steel, A. (1997). A new algorithm for the computation of canonical forms of matrices over fields. *J. Symbolic Comput.* 24:409–432.
- [17] Steinberg, R. (1951). The representations of $GL(3, q)$, $GL(4, q)$, $PGL(3, q)$, and $PGL(4, q)$. *Can. J. Math.* 3:225–235.
- [18] Tiep, P. H., Zalesskii, A. (1996). Minimal characters of the finite classical groups. *Commun. Algebra* 24:2093–2167.
- [19] Zisser, I. (1989). The covering numbers of the sporadic simple groups. *Israel J. Math.* 67(2):217–224.