

*Pacific
Journal of
Mathematics*

**FINITE SIMPLE GROUPS HAVE
MANY CLASSES OF p -ELEMENTS**

MICHAEL GIUDICI, LUKE MORGAN AND CHERYL E. PRAEGER

Volume 336 No. 1-2

May 2025

FINITE SIMPLE GROUPS HAVE MANY CLASSES OF p -ELEMENTS

MICHAEL GIUDICI, LUKE MORGAN AND CHERYL E. PRAEGER

Dedicated with admiration and thanks to the memory of our colleague Gary M. Seitz

For an element x of a finite group T , the $\text{Aut}(T)$ -class of x is $\{x^\sigma \mid \sigma \in \text{Aut}(T)\}$. We prove that the order $|T|$ of a finite nonabelian simple group T is bounded above by a function of the parameter $m(T)$, where $m(T)$ is the maximum, over all primes p , of the number of $\text{Aut}(T)$ -classes of elements of T of p -power order. This bound is a substantial generalisation of the results of Pyber (1992) and of Héthelyi and Külshammer (2005), and it has implications for relative Brauer groups of finite extensions of global fields.

1. Introduction

In 1992 Pyber [33] showed that a group of order n contains at least $O\left(\frac{\log n}{(\log \log n)^8}\right)$ conjugacy classes of elements. This solved a problem of Brauer from 1963 [3], who had asked for a significant improvement on his lower bound of $\log \log n$. In Section 1.1 we briefly discuss the interesting story around these bounds, which date back to work of Landau in 1903 and extend to recent work in 2017. The special case of Pyber’s bound for a nonabelian simple group T could be turned around to state that $|T| < c^{f(m)}$ where m is the number of $\text{Aut}(T)$ -classes in T , c is a constant, and f is the particular function $f(m) = (\log m)^2 \cdot \log \log m$. This alternative statement of Pyber’s result was used in [32, Theorem 4.4] to prove a conjecture about maximal subgroups of a finite group which are “covering subgroups”, and in turn, this application had consequences for Kronecker classes of algebraic number fields (see [32, Section 4]).

Many classical results concerning conjugacy classes of elements in groups have analogues in the case where the conjugacy classes are restricted to those consisting of elements of prime power order. For example, given a core-free subgroup H of a group G , not only is there a conjugacy class of elements of G that does not meet H , but Fein, Kantor and Schacher [9] showed that there is a conjugacy class of elements of prime power order that avoids H . Similarly, not only does every

MSC2020: 20D06, 20E32.

Keywords: finite simple group, p -elements, conjugacy classes, order bounds.

nonlinear irreducible character of a finite group vanish on some conjugacy class of elements, but Malle, Navarro and Olsson [27] showed that each such character must vanish on some conjugacy class of elements of prime power order. Such analogues usually have interesting applications: for example, the Fein–Kantor–Schacher result is equivalent (see [9, Section 3]) to the fact that the relative Brauer group of a nontrivial finite extension of global fields is infinite.

In this paper we prove a new bound (Theorem 1.1) on the order of a finite simple group related to its p -elements, that is, elements of p -power order for various primes p . The bound is a substantial generalisation of the results of Pyber and others, in that the parameter m above is replaced by

$$(1) \quad m(T) = \max_{p \text{ prime}} m_p(T),$$

where $m_p(T) = \#\{\text{Aut}(T)\text{-classes of elements of } p\text{-elements in } T\}$.

Theorem 1.1. *There exists an increasing function f on the natural numbers such that, for a finite nonabelian simple group T , the order of T is at most $f(m(T))$.*

In the proof of Theorem 1.1 for exceptional groups of Lie type, we are indebted to the work of Gary Seitz, to whose memory this paper is dedicated, and his coauthors Martin Liebeck and Jan Saxl, for their classification of the subgroups of maximal rank of these groups [25]. Their results gave us the detailed information about certain tori and their normalisers on which our proof is based. In addition, in the proof of Theorem 1.1 for classical groups, we use the description by Aschbacher and Seitz [1] of conjugacy classes of involutions in Chevalley groups of even characteristic to bound the dimension (Lemma 4.1).

The function $f(n)$ we obtain in the proof of Theorem 1.1 involves an $n!$ term. It is possible that a better function might be obtained, see Remark 4.3 for further comments. Since the function $f(n)$ in Theorem 1.1 is increasing, the bound can be turned around to give a lower bound in terms of $|T|$ for the number of $\text{Aut}(T)$ -classes of p -elements in T .

Corollary 1.2. *There exists an increasing function g on the natural numbers such that, for a finite nonabelian simple group T , there is a prime p dividing $|T|$ such that the number of $\text{Aut}(T)$ -classes of elements of p -power order in T is at least $g(|T|)$.*

There are numerous bounds in the literature that relate $|T|$ with various parameters concerning numbers of conjugacy classes or $\text{Aut}(T)$ -classes. For example, by [28, Theorems 1.2 and 1.4], for a given prime p dividing $|T|$, the order $|T|$ is bounded above in terms of the number of its p -regular conjugacy classes (elements of order coprime to p) and also, apart from certain rank 1 Lie type simple groups, $|T|$ is bounded above in terms of the number of its p -singular conjugacy classes (elements of order a multiple of p). One motivation for proving Theorem 1.1 is a conjecture

concerning finite groups G with a proper subgroup that meets all $\text{Aut}(G)$ -classes of elements of G of prime power order [32, Conjecture 4.3']. Thus, rather than considering p -singular or p -regular elements for some fixed prime p , we must work with all elements of prime power order. In future work [12] we apply Theorem 1.1 to prove an important case of [32, Conjecture 4.3'], which has consequences for relative Brauer groups of field extensions as discussed in [9; 12; 14].

Finally we note that many bounds of this type in the literature are available for general finite groups, and it would be interesting to know if the bounds in Theorem 1.1 and Corollary 1.2 can be used to obtain similar bounds for larger families of finite groups.

This paper is organised as follows. In Section 2 we prove some preliminary numerical results and a result relating the normalisers of cyclic subgroups S of a group G with our parameter $m(G)$ (1). We treat the alternating groups in Section 3 and the bulk of the work takes place in Sections 4 and 5 where we consider the classical groups and the exceptional groups of Lie type, respectively. Finally in Section 6 we complete the proof of Theorem 1.1.

1.1. *Commentary on Landau's and Pyber's theorems.* Landau's theorem [23] from 1903 states that, for a given positive integer k , there are only finitely many finite groups having exactly k conjugacy classes of elements, and so such a group must have order bounded in terms of k . Brauer [3] made this bound explicit in 1963, showing that a group of order n has at least $\log \log n$ conjugacy classes, and asked for a substantially better bound. Providing an improvement was the main focus of Pyber's 1992 paper [33], where he proved that a group of order $n \geq 4$ must have at least $c \log n / (\log \log n)^8$ conjugacy classes for some "computable constant" c . The relevance for this paper is Pyber's bound for nonabelian simple groups [33, Lemma 4.4]: if T is a finite nonabelian simple group and $a = |\text{Aut}(T)|$, then the number of $\text{Aut}(T)$ -classes in T is at least

$$2^{c(\log a / \log \log a)^{1/2}} \quad \text{for some constant } c.$$

Since 1992 there have been numerous contributions that strengthened these bounds (see [2] for an overview). Currently the best lower bound for the number $k(G)$ of conjugacy classes of an arbitrary finite group G is given by Baumeister, Maróti and Tong-Viet in 2018 [2, Theorem 1.1]:

$$\forall \epsilon > 0, \exists \delta > 0 \text{ such that } \forall \text{ finite groups } G \text{ with } |G| \geq 3, k(G) \geq \frac{\delta \log |G|}{(\log \log |G|)^{3+\epsilon}}.$$

Many better lower bounds are available for restricted classes of groups, for example, for G soluble then Keller [19] proved that $k(G) \geq \frac{c \log |G|}{\log \log |G|}$ for some constant c ; a purely logarithmic lower bound $k(G) > \log_3 |G|$ was given in [2, Theorem 1.2] for groups with trivial soluble radical; and a better than logarithmic lower bound

was obtained for nilpotent groups by Jaikin-Zapirain [18]. These bounds have been exploited to obtain related bounds concerning irreducible complex representations, for example, bounding the number of irreducible characters of odd degree [11; 16] in connection with the McKay conjecture. Also, as mentioned above, there are various results in [28] that give lower bounds for the number of conjugacy classes of p -regular elements, or p -singular elements, or the total number of classes of elements of prime power order (adding over the prime divisors) in [15], but to our knowledge our bound in terms of classes of p -elements, for a certain single prime p , is new.

Remark 1.3. Our proof of Theorem 1.1 for simple classical groups hints towards a possible bound for the order of a simple group in terms of another property. For a group G and a prime s we define

$$m_{s\text{-exp}}(G) = \#\{\text{Aut}(G)\text{-classes of elements of order } \exp(G)_s\},$$

where $\exp(G)_s$ is the s -part of the exponent $\exp(G)$, and set $m_{\text{exp}}(G)$ to be the maximum of $m_{s\text{-exp}}(G)$ over all primes s dividing $|G|$. In addition, for a set \mathcal{S} of primes we set $m_{\mathcal{S}\text{-exp}}(G)$ to be the maximum of $m_s(G)$ over all primes $s \in \mathcal{S}$.

The above concepts are motivated by choices made in the proof of Proposition 4.2. It turns out that for simple classical groups T , apart from the characteristic p , the set $\mathcal{S}(T)$ of primes s we consider all have the property that the Sylow s -subgroups are cyclic and hence have order $\exp(T)_s$, and the s -elements we consider are those of maximal order $\exp(T)_s$. Thus for a simple classical group T of characteristic p , we prove that $|T|$ is bounded above by a function of

$$m'(T) = \max\{m_p(T), m_{\mathcal{S}(T)\text{-exp}}(T)\},$$

where $m_p(T)$ is as in (1). See Remark 4.4 for further details. This motivated us to consider whether a similar bound holds for other simple groups. In Remark 3.2 we show, using the prime number theorem, that for large enough m , $|\text{Alt}(m)|$ is bounded above by a function of $m_{\text{exp}}(\text{Alt}(m))$. We believe this style of bound has not previously been studied. It would be interesting to know if such a bound holds also for the simple exceptional groups of Lie type.

2. Preparatory lemmas

For a prime s and integer n , let n_s denote the s -part of n , that is, the highest power of s dividing n , and let $n_{s'} = n/n_s$ denote the part of n prime to s . For an integer m define $\mathcal{S}(m)$ to be the set of all prime divisors s of $q^m - 1$ such that $(q^m - 1)_s$ does not divide $q^t - 1$ for any $t < m$. In our analysis we need that

$$\text{Prod}(m, q) := \prod_{s \in \mathcal{S}(m)} (q^m - 1)_s$$

is large enough, for example, larger than q or some constant multiple of q . We use the following lemma to treat the classical groups.

Lemma 2.1. *Let q be a prime power and m a positive integer:*

- (i) *Suppose that s is a prime divisor of $q^m - 1$. If t is the smallest positive integer such that $(q^m - 1)_s$ divides $q^t - 1$, then t divides m .*
- (ii) *$q + 1$ divides $\text{Prod}(2, q)$, and $q^2 + 1$ divides $\text{Prod}(4, q)$.*
- (iii) *If m is odd and $m > 1$, then $2 \notin \mathcal{S}(2m)$ and $\text{Prod}(2m, q)$ divides $q^m + 1$.*
- (iv) *Suppose that m is an odd prime. Then:*
 - (1) *If $s \in \mathcal{S}(m)$ and $s | q - 1$, then $s = m$; if $s \in \mathcal{S}(2m)$ and $s | q^2 - 1$, then $s = m$ and $m | q + 1$.*
 - (2) *$(q^m - 1)/(q - 1)$ divides $\text{Prod}(m, q)$.*
 - (3) *$(q^m + 1)/(q + 1)$ divides $\text{Prod}(2m, q)$.*

Proof. (i) Let $s^b = (q^m - 1)_s$ and let t be the least positive integer such that s^b divides $q^t - 1$. Then $t \leq m$. Write $m = kt + r$, where $1 \leq r \leq t$. Then s^b divides $\gcd(q^m - 1, q^t - 1) = q^{\gcd(m, t)} - 1$, and $\gcd(m, t) = \gcd(r, t) \leq r \leq t$. By the minimality of t we have $r = t$, and hence t divides m .

(ii) If a prime $s | q^2 - 1$ then either $s \in \mathcal{S}(2)$ or $(q^2 - 1)_s$ divides $q - 1$, and hence $q^2 - 1$ divides $(q - 1) \cdot \text{Prod}(2, q)$, so $\text{Prod}(2, q)$ is divisible by $q + 1$. Similarly, if a prime $s | q^4 - 1$ then, by part (i), either $s \in \mathcal{S}(4)$ or $(q^4 - 1)_s$ divides $q^2 - 1$, and hence $q^2 + 1$ divides $\text{Prod}(4, q)$.

(iii) Next assume that m is odd and $m > 1$. If q is even then $2 \notin \mathcal{S}(2m)$ by the definition of $\mathcal{S}(2m)$. It turns out that this also holds if q is odd: by [13, Lemma 2.5],

$$(q^{2m} - 1)_2 = ((q^2)^m - 1)_2 = (q^2 - 1)_2$$

and as $m > 1$, again $2 \notin \mathcal{S}(2m)$ by the definition of $\mathcal{S}(2m)$. Thus, for any q , $\mathcal{S}(2m)$ consists of odd primes. Since $\gcd(q^m - 1, q^m + 1) = (2, q - 1)$, it follows that for any odd prime s , $(q^{2m} - 1)_s$ divides exactly one of $q^m + 1$ and $q^m - 1$. Moreover, if $s \in \mathcal{S}(2m)$ then $(q^{2m} - 1)_s$ does not divide $q^m - 1$ by definition, and hence, for each $s \in \mathcal{S}(2m)$, we have that $(q^{2m} - 1)_s$ divides $q^m + 1$. Hence $\text{Prod}(2m, q)$ divides $q^m + 1$, proving (iii).

(iv) Now assume that m is an odd prime and let s be a prime dividing $q^m - 1$. Then either $s \in \mathcal{S}(m)$ or $(q^m - 1)_s$ divides $q - 1$, and hence $q^m - 1$ divides $(q - 1) \cdot \text{Prod}(m, q)$, so $\text{Prod}(m, q)$ is divisible by $(q^m - 1)/(q - 1)$. Furthermore, if $s \in \mathcal{S}(m)$ and $s | q - 1$, then s must divide $(q^m - 1)/(q - 1)$ by the definition of $\mathcal{S}(m)$, and hence s divides

$$\gcd\left(\frac{q^m - 1}{q - 1}, q - 1\right) = \gcd(m, q - 1).$$

Since m is prime this implies $s = m$. Similarly, if $s \in \mathcal{S}(2m)$ and s divides $q^2 - 1$, then s must divide $(q^{2m} - 1)/(q^2 - 1)$ by the definition of $\mathcal{S}(2m)$, and hence s divides

$$\gcd\left(\frac{q^{2m} - 1}{q^2 - 1}, q^2 - 1\right) = \gcd(m, q^2 - 1).$$

Since m is prime this implies that $s = m$ divides $q^2 - 1$. Further, by part (iii), $s \mid q^m + 1$ and hence s divides $\gcd(q^m + 1, q^2 - 1) = q + 1$. Thus parts (1) and (2) are proved.

Finally, if a prime s divides $q^{2m} - 1$ and t is minimal such that $(q^{2m} - 1)_s$ divides $q^t - 1$, then either $s \in \mathcal{S}(2m)$, or $t \in \{m, 2, 1\}$. Thus $q^{2m} - 1$ divides

$$\text{Prod}(2m, q) \cdot \frac{(q^m - 1)(q^2 - 1)}{\gcd(q^m - 1, q^2 - 1)} = \text{Prod}(2m, q) \cdot (q^m - 1)(q + 1).$$

It follows that $(q^m + 1)/(q + 1)$ divides $\text{Prod}(2m, q)$. \square

Definition 2.2. We say that a group G is *prime power bounded by n* , or simply, *pp-bounded by n* , if $m(G) \leq n$, where $m(G)$ is as in (1). In other words, for each prime p dividing $|G|$, the number of $\text{Aut}(G)$ -classes of elements of p -power order in G is at most n .

In the following lemma ϕ denotes the Euler ϕ -function, namely for a positive integer m , $\phi(m)$ is the number of positive integers at most m and coprime to m .

Lemma 2.3. *Suppose that G is a group that is pp-bounded by n . Let $S \leq G$ be a nontrivial cyclic s -subgroup of order s^b , where s is prime, and let $N = N_{\text{Aut}(G)}(S)$. Then there is a bijection $\mathcal{C} \rightarrow \mathcal{D}$, where*

$$\mathcal{C} := \{x^{\text{Aut}(G)} \mid x \in S, o(x) = s^b\}, \quad \mathcal{D} := \{x^N \mid x \in S, o(x) = s^b\}$$

and $|\mathcal{C}| = \phi(|S|)/r$ with $r = |N_{\text{Aut}(G)}(S) : C_{\text{Aut}(G)}(S)|$. Furthermore,

$$\phi(|S|) = s^{b-1}(s - 1) \leq rn \quad \text{and} \quad \phi(|S|) \text{ divides } r(n!).$$

Proof. Note that if $x_1, x_2 \in S$ have order s^b and are such that $x_1^g = x_2$ for some $g \in \text{Aut}(G)$, then $S^g = \langle x_1 \rangle^g = \langle x_1^g \rangle = \langle x_2 \rangle = S$, so that $g \in N$. Conversely, if $x_1, x_2 \in S$ are conjugate by an element of N , then they are also conjugate under the action of $\text{Aut}(G)$. This gives a bijection $\mathcal{C} \rightarrow \mathcal{D}$ as claimed.

For $x^N \in \mathcal{D}$, we know $\langle x \rangle = S$, so $|x^N| = |N : C_N(x)| = |N : C_N(S)|$. Note that $C_{\text{Aut}(G)}(S) \leq N_{\text{Aut}(G)}(S) = N$ so that $C_{\text{Aut}(G)}(S) = C_N(S)$. Hence $|N : C_N(S)| = r$. Thus each N -class in \mathcal{D} has length exactly r . Since S contains $\phi(|S|)$ elements of order $|S|$ (where ϕ is Euler's function), r divides $\phi(|S|)$ and $|\mathcal{D}| = \phi(|S|)/r$. Since G is pp-bounded by n , we have $\phi(|S|)/r = |\mathcal{D}| \leq n$, and hence $\phi(|S|)$ divides $r(n!)$. \square

Notation 2.4. Throughout the paper $\log x$ denotes the natural logarithm of x .

Lemma 2.5. *For all $a > 1$ we have*

$$\frac{a^{1/4}}{4} < \frac{\sqrt{a}}{\log a}.$$

Proof. The inequality in the statement is equivalent to $\log a < 4a^{1/4}$. Exponentiating both sides, we see the latter inequality is equivalent to $a < e^{4a^{1/4}}$, that is,

$$f(a) := e^{4a^{1/4}} - a > 0.$$

Now

$$f'(a) = \frac{e^{4a^{1/4}}}{a^{3/4}} - 1 \quad \text{and} \quad f''(a) = \frac{e^{4a^{1/4}}}{a^{3/2}} \left(1 - \frac{3}{4a^{1/4}}\right).$$

For $a \geq 1$ we have $f''(a) > 0$, so that $f'(a)$ is increasing for $a \geq 1$. Further, $f'(1) = e^4 - 1 > 0$, so $f'(a) > 0$ for all $a \geq 1$. Thus $f(a)$ is increasing for $a \geq 1$, and since $f(1) = e^4 - 1 > 0$, we have $f(a) > 0$ for all $a \geq 1$, as required. \square

Lemma 2.6. *Suppose that $q = p^a$, $p \geq 2$ and $a \geq 1$. Then*

$$\frac{\sqrt{q} \log 2}{2} \leq \frac{q}{a}.$$

Proof. Note that $a = \log q / \log p \leq \log q / \log 2$. Now since $\log x \leq 2\sqrt{x}$ for all $x \in \mathbb{R}$ with $x > 0$, we have

$$a \leq \frac{2\sqrt{q}}{\log 2}$$

and thus $a\sqrt{q} \leq 2q / \log 2$, which yields

$$\frac{\sqrt{q} \log 2}{2} \leq \frac{q}{a}. \quad \square$$

3. The alternating groups

We first consider the alternating groups.

Lemma 3.1. *If $T \cong \text{Alt}(m)$ is pp -bounded by n , then $|T| \leq \frac{1}{2}(3n+2)!$.*

Proof. Suppose that $T \cong \text{Alt}(m)$ is pp -bounded by n . If $m \neq 6$, we note that T has $\lfloor m/3 \rfloor$ $\text{Aut}(T)$ -classes of elements of order 3. This gives $m \leq 3n+2$, and hence $|T| = \frac{1}{2} \cdot m! \leq \frac{1}{2} \cdot (3n+2)!$. If $m = 6$, then T has two classes of 2-elements, so $n \geq 2$. Then certainly $|T| = 360 \leq \frac{1}{2} \cdot (3n+2)!$ holds. \square

Remark 3.2. As discussed in Remark 1.3, another type of bound on $|T|$ for a simple group T is in terms of the number of $\text{Aut}(T)$ -classes of elements with order equal to $\exp(T)_p$, the p -part of the exponent of T . We explain briefly that there is such a bound when $T \cong \text{Alt}(m)$, for sufficiently large m . Recall that $\exp(\text{Alt}(m)) = \text{lcm}\{m' : 1 \leq m' \leq m\}$.

Let $\pi(x)$ denote the number of integers less than or equal to x that are prime. Based on the prime number theorem, we know (for sufficiently large x) that

$$(2) \quad c \frac{x}{\log x} < \pi(x) < d \frac{x}{\log x}$$

for explicit constants c and d . For example, if $x \geq 11$, then we can take $c = 1$, and for x “sufficiently large” we can take $d = 1.04423$; see [34, pp. 176–177]. These bounds allow us to prove existence of primes in certain intervals, somewhat analogously to Bertrand’s postulate which asserts that there is a prime between m and $2m$ for all positive integers m . We are interested here in the existence of a prime p such that $\sqrt{m/3} < p \leq \sqrt{m/2}$; and we claim that such a prime exists for sufficiently large m . Indeed, if $\sqrt{m/3}$ is large enough so that (2) holds with $c = 1$, then we have

$$\pi(\sqrt{m/2}) > \frac{\sqrt{m/2}}{\log \sqrt{m/2}} \quad \text{and} \quad \pi(\sqrt{m/3}) < d \frac{\sqrt{m/3}}{\log \sqrt{m/3}},$$

and a sufficient condition for p to exist is that

$$\frac{\sqrt{m/2}}{\log \sqrt{m/2}} > d \frac{\sqrt{m/3}}{\log \sqrt{m/3}},$$

which is equivalent to

$$\log m > \frac{\frac{1}{\sqrt{2}} \log 3 - \frac{1}{\sqrt{3}} d \log 2}{\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}} d}$$

and since d is a constant, this holds for sufficiently large m .

Thus, if m is large enough we may choose a prime p such that $\sqrt{m/3} < p \leq \sqrt{m/2}$, or equivalently, $2p^2 \leq m < 3p^2$. We may assume that $p > 3$ (by taking $m > 27$) and then we see that the p -part $\exp(T)_p$ of the exponent is exactly p^2 . Meanwhile, the inequality $2p^2 \leq m$ implies that T has at least p $\text{Aut}(T)$ -classes of elements of order p^2 , namely, for $1 \leq i \leq p$, elements that have a single p^2 -cycle and exactly i cycles of length p . Such elements with different values of i cannot be conjugate in $\text{Aut}(T) \cong \text{Sym}(m)$ because they have different cycle types, so there are at least p $\text{Aut}(T)$ -classes of elements with exponent $\exp(T)_p$, that is, $m_{\exp(T)} \geq p$. Thus $m < 3p^2 \leq 3(m_{\exp(T)})^2$, and hence $|T|$ is bounded above by $\frac{1}{2}(3(m_{\exp(T)})^2)!$.

4. Finite simple classical groups

Let T be a finite simple classical group defined over a field of order $q = p^a$, as in one of the lines of Table 1. The table records also the natural module V for T and its dimension, and the covering group G of T in $\text{GL}(V)$.

Lemma 4.1. *Let T and d be as in Table 1. Then the number of unipotent conjugacy classes is at least d .*

T	d	V	G	conditions
$\mathrm{PSL}(d, q)$	$d \geq 2$	\mathbb{F}_q^d	$\mathrm{SL}_d(q)$	$(d, q) \neq (2, 2)$ or $(2, 3)$
$\mathrm{PSU}(d, q)$	$d \geq 3$	$\mathbb{F}_{q^2}^d$	$\mathrm{SU}_d(q)$	$(d, q) \neq (3, 2)$
$\mathrm{PSp}(2d, q)$	$d \geq 2$	\mathbb{F}_q^{2d}	$\mathrm{Sp}_{2d}(q)$	$(d, q) \neq (2, 2)$
$\mathrm{P}\Omega^\circ(2d+1, q)$	$d \geq 3$	\mathbb{F}_q^{2d+1}	$\Omega_{2d+1}^\circ(q)$	q odd
$\mathrm{P}\Omega^\epsilon(2d, q)$	$d \geq 4$	\mathbb{F}_q^{2d}	$\Omega_{2d}^\epsilon(q)$	$\epsilon \in \{+, -\}$

Table 1. Simple classical groups, their covering groups and natural modules.

Proof. Note that the identity element forms a unipotent conjugacy class, and since there is always a nonidentity unipotent conjugacy class, the assertion holds if $d = 2$. Thus we may assume that $d \geq 3$. Furthermore, making use of the identity, we need to show the existence of $d - 1$ nonidentity unipotent classes. The unipotent conjugacy classes in classical groups are well known; see, e.g., [5; 10; 24; 36] or [1] for unipotent elements of order 2.

Let J_i denote an $i \times i$ Jordan block with all 1's down the diagonal. Then for each i such that $2 \leq i \leq d$, the group $T = \mathrm{PSL}(d, q)$ contains an element corresponding to the matrix that is the direct sum of J_i and I_{d-i} . These are clearly not conjugate under any element of $\mathrm{P}\Gamma\mathrm{L}(d, q)$ or under the inverse transpose map, so the number of $\mathrm{Aut}(T)$ -conjugacy classes of nonidentity unipotent elements is at least $d - 1$. Each of these conjugacy classes meets $\mathrm{PSU}(d, q)$ nontrivially and so for $T = \mathrm{PSU}(d, q)$ the number of $\mathrm{Aut}(T)$ -conjugacy classes of nonidentity unipotent elements is also at least $d - 1$.

Suppose now that $T = \mathrm{PSp}(2d, q)$ (with $d \geq 3$). For each $i \leq d$, the group T contains an element whose corresponding matrix has Jordan canonical form that is the direct sum of i copies of J_2 and $I_{2(d-i)}$. This gives us d different conjugacy classes in T that are clearly not fused in $\mathrm{P}\Gamma\mathrm{Sp}(2d, q)$. Since $2d > 4$, we have $\mathrm{Aut}(T) = \mathrm{P}\Gamma\mathrm{Sp}(2d, q)$, and the result is proved.

Next suppose that $T = \mathrm{P}\Omega^\circ(2d + 1, q)$ and q is odd. For each even i with $1 \leq i \leq 2d + 1$, there are unipotent elements whose corresponding matrix has Jordan canonical form being the direct sum of J_i and I_{2d+1-i} . This gives d distinct classes that are clearly not fused in $\mathrm{P}\Gamma\mathrm{O}(2d + 1, q) = \mathrm{Aut}(T)$, as required.

Finally, we have $T = \mathrm{P}\Omega^\epsilon(2d, q)$ with $\epsilon \in \{\pm\}$. First suppose that q is odd. For each i with $1 \leq i \leq d$, there are unipotent elements in T whose corresponding matrix has Jordan canonical form being the direct sum of J_{2i} and $I_{2(d-i)}$. This gives d distinct classes that are clearly not fused under inner, diagonal or field automorphisms of T . Moreover, when $2d = 8$ and $\epsilon = +$, from [4, Proposition 3.55] we see that none of these classes are fused under a triality automorphism. Hence T has at least d $\mathrm{Aut}(T)$ -classes of unipotent elements. Suppose now that q is

even. We again follow the notation of [1, Section 8] for involutions in T and use the geometric description in [5, Section 3.5.4]. For each even $i < d$ we get two T -classes of involutions with Jordan canonical form consisting of i copies of J_2 . When $i = d$ and d is even, we get one such T -class when $\epsilon = -$ and three when $\epsilon = +$. Fusing of these classes in $\text{P}\Gamma\text{O}^\pm(2d, q)$ occurs only when $\epsilon = +$ and $i = d$ is even, in which case two of the three classes fuse. When d is odd we have $\text{Aut}(T) = \text{P}\Gamma\text{O}^\pm(2d, q)$ and so we see that T has at least $d - 1$ $\text{Aut}(T)$ -classes of involutions as required. Suppose now that d is even. Then the number of T -classes of involutions is $2(\lfloor (d-1)/2 \rfloor) + 3 = d + 1$ when $\epsilon = +$ and $2(\lfloor (d-1)/2 \rfloor) + 1 = d$ when $\epsilon = -$. Thus if $\epsilon = -$, or if $\epsilon = +$ and $2d \neq 8$, we see that T has at least d $\text{Aut}(T)$ -classes of involutions. Finally, if $2d = 8$ and $\epsilon = +$, then two of the classes with $i = 4$ (denoted a_4 and a'_4 in [5]) are fused with one of the classes with $i = 2$ (denoted c_2 in [5]) under triality [4, Proposition 3.55]. Hence in this final case we also get at least $d - 1$ $\text{Aut}(T)$ -classes of involutions, as required. \square

Proposition 4.2. *There is an increasing integer function g such that, if T is a finite simple classical group as in Table 1, and T is pp-bounded by n , then $|T| < g(n)$.*

Proof. The group T has a natural module V as in Table 1, and it is convenient to work with the preimage $G \leq \text{GL}(V)$ acting linearly on V . We set $q = p^a$ with p prime. Let φ denote the natural map $\varphi : G \rightarrow T$, and for a subgroup H of T let \hat{H} denote the full preimage of H under φ . We first observe that, by Lemma 4.1, the number of $\text{Aut}(T)$ -classes of unipotent elements of T is at least d , and hence $d \leq c_1(n)$ with $c_1(n) = n$.

There is a prime m satisfying $\frac{d}{2} < m \leq d$, and we choose the smallest possible value for m , except that we choose $m = 3$ if $d = 3$. Then one of the following holds:

- (i) $m < d$.
- (ii) $d = m = 2$ with $T = \text{PSL}(2, q)$ or $\text{PSp}(4, q)$.
- (iii) $d = m = 3$ with $T = \text{PSL}(3, q)$, $\text{PSU}(3, q)$, $\text{PSp}(6, q)$, or $\text{P}\Omega^\circ(7, q)$.

Choice of decomposition. If $m < d$ then we choose a decomposition $V = U \oplus W$, with $\dim(U) = m$ in the linear and unitary cases, and $\dim(U) = 2m$ in the symplectic and orthogonal cases (and possibly $\dim(W) = 0$). Additionally, if G preserves a form, we choose U to be nondegenerate and $W = U^\perp$. Finally, in the orthogonal case, we choose U of minus-type.

Choice of cyclic subgroup. In our arguments we will work with a cyclic subgroup of G that stabilises the decomposition $V = U \oplus W$ and acts trivially on W (see [30, Section 3] for a description of the linear action of these tori). More specifically:

- (L) If $T = \text{PSL}(d, q)$ we consider a cyclic subgroup H of order $\frac{q^m - 1}{(q-1) \cdot (m, q-1)}$ such that \hat{H}^U is a Singer cycle of $\text{SL}(U)$ and \hat{H} fixes W pointwise.

case	G	$ \hat{H} $	\hat{H}^U	\hat{H}^W	notes
(L)	$\mathrm{SL}(d, q)$	$(q^m - 1)/(q - 1)$	$\leq \mathrm{GL}(1, q^m)$	1	$m = d$ if $d = 2$ or 3
(U)	$\mathrm{SU}(d, q)$	$(q^m + 1)/(q + 1)$	$\leq \mathrm{GU}(1, q^m)$	1	$m = d$ if $d = 3$
(Sp)	$\mathrm{Sp}(2d, q)$	$q^m + 1$	$\leq \mathrm{Sp}(2, q^m)$	1	$m = d$ if $d = 2$ or 3
(O)	$\Omega(2d + 1, q)$	$(q^m + 1)_{2'}$	$\leq \mathrm{GO}^-(2, q^m)$	1	$m = d$ if $d = 3$
(O)	$\Omega^\pm(2d, q)$	$(q^m + 1)_{2'}$	$\leq \mathrm{GO}^-(2, q^m)$	1	

Table 2. Choices for a cyclic subgroup \hat{H} of G .

(U) If $T = \mathrm{PSU}(d, q)$ then m is an odd prime and we consider a cyclic subgroup H of order $\frac{q^m + 1}{(q + 1) \cdot (m, q + 1)}$ such that \hat{H}^U is a Singer cycle of $\mathrm{SU}(U)$ and \hat{H} fixes W pointwise.

(Sp) If $T = \mathrm{PSp}(2d, q)$ we consider a cyclic subgroup \hat{H} of order $q^m + 1$ such that \hat{H}^U is a maximal torus of $\mathrm{Sp}(2m, q)$ and \hat{H} fixes W pointwise.

(O) If $T = \mathrm{P}\Omega^\epsilon(2d, q)$ or $\mathrm{P}\Omega^\circ(2d + 1, q)$ with $m < d$, and also in the exceptional case where $T = \mathrm{P}\Omega^\circ(7, q)$ with q odd and $d = m = 3$, then the parameter m is an odd prime and U is of minus-type and dimension $2m$. By [22, Lemma 4.1.1(ii)], the stabiliser in G of the decomposition $V = U \oplus W$ contains the subgroup

$$\Omega(U) \times 1 \cong \Omega^-(2m, q),$$

which fixes W pointwise. We consider a cyclic subgroup \hat{H} of $\Omega(U) \times 1$ of order $\frac{q^m + 1}{(q + 1)_2}$ such that \hat{H}^U is contained in a Singer cycle of $\Omega(U)$. Note that

$$|\mathrm{O}(U) : \Omega(U)| = 2 \cdot (2, q - 1)$$

(see [22, Table 2.1.C]) and that $(q^m + 1)/(q + 1)$ is odd since m is odd, so the 2-part $(q^m + 1)_2 = (q + 1)_2$ and $|\hat{H}| = (q^m + 1)_{2'}$.

Thus the cyclic subgroup \hat{H} has the properties given in the appropriate row of Table 2. First we consider the linear case.

Case 1. $T = \mathrm{PSL}(d, q)$.

Here $|\hat{H}| = (q^m - 1)/(q - 1)$ and we set $H = \varphi(\hat{H})$. Also $H \cong \hat{H}$ if $m < d$, or if $m = d = 3$ with $\mathrm{gcd}(3, q - 1) = 1$, or if $m = d = 2$ with q even, since in these cases \hat{H} contains no nontrivial scalar matrix. We assume first that $|H| = (q^m - 1)/(q - 1)$, and comment at the end on how to adjust our argument to deal with the exceptional cases when $m = d = 2$ or 3 and m divides $q - 1$.

The centraliser of \hat{H}^U in $\mathrm{GL}(U)$ is the full Singer cycle $C = \mathrm{GL}(1, q^m)$ and $N_{\mathrm{GL}(U)}(\hat{H}) = C \cdot m$ (see [29, Lemma 2.1] or [17, Satz II.7.3, p. 187]). Setting $q = p^a$ with p prime, we have

$$N_{\mathrm{GL}(d, q)}(\hat{H}) = (\mathrm{GL}(1, q^m) \cdot m \times \mathrm{GL}(d - m, q)) \cdot a$$

(or $GL(1, q^m) \cdot ma$ if $m = d$). It follows that $r := |N_{\text{Aut}(T)}(H)/C_{\text{Aut}(T)}(H)|$ divides $2am$ (noting that in general an outer automorphism corresponding to the “inverse transpose map” will act nontrivially on H if $d > 2$).

Let $s \in \mathcal{S}(m)$ as defined in Section 2, and let \hat{S} be the Sylow s -subgroup of \hat{H} and $S = \varphi(\hat{S})$. Since $|\hat{S}|$ does not divide $q - 1$ by the definition of $\mathcal{S}(m)$, we have $|S| = s^b$ for some $b \geq 1$ and $\phi(|S|) = s^{b-1}(s - 1)$. Also \hat{S} is irreducible on U , and S and H have the same centraliser and normaliser in $\text{Aut}(T)$ (see [29, Lemma 2.1]). Hence $|N_{\text{Aut}(T)}(S)/C_{\text{Aut}(T)}(S)| = |N_{\text{Aut}(T)}(H)/C_{\text{Aut}(T)}(H)| = r$ divides $2am$. Further, by Lemma 2.3, the number of $\text{Aut}(T)$ -classes of elements of T of order $|S|$ is $\phi(|S|)/r$ and divides $n!$. Thus $\phi(|S|)$ divides $r \cdot n!$, which divides $2am \cdot n!$. Since $m \leq d$ and $d \leq c_1(n) = n$, it follows that $2m \leq 2n$ and hence $2m$ divides $(2n)!$. Thus

$$(3) \quad \phi(|S|) = s^{b-1}(s - 1) \quad \text{divides } c_2(n) a,$$

where $c_2(n) = (2n)! \cdot n!$. Note that the bound $c_2(n) a$ is independent of the prime $s \in \mathcal{S}(m)$. The condition (3) implies that $s - 1$ is a divisor of $c_2(n) a$, and since the number of divisors of $c_2(n) a$ is less than $2\sqrt{c_2(n) a}$ (see [31, Section 8.3]), it follows that $|\mathcal{S}(m)| < 2\sqrt{c_2(n) a}$.

Now $|H| = |\varphi(\hat{H})| = (q^m - 1)/(q - 1)$ and recall that m is prime. If $s \in \mathcal{S}(m)$ and s does not divide $q - 1$, then $(q^m - 1)_s = |H|_s$ and in this case by (3) we have

$$(q^m - 1)_s = |S| = s^b = \frac{s\phi(|S|)}{(s - 1)} \leq 2c_2(n) a.$$

On the other hand if $s \in \mathcal{S}(m)$ and s divides $q - 1$, then $s = m$ by Lemma 2.1(iv). In this case,

$$\frac{(q^m - 1)_m}{(q - 1)_m} = |S| = \frac{m\phi(|S|)}{(m - 1)} \leq 2c_2(n) a.$$

Putting this together we see that

$$\text{Prod}(m, q) = \prod_{s \in \mathcal{S}(m)} (q^m - 1)_s \leq (q - 1)_m \cdot (2c_2(n) a)^{2\sqrt{c_2(n) a}}.$$

Thus we have

$$\frac{\text{Prod}(m, q)}{(q - 1)_m} \leq (2c_2(n) a)^{2\sqrt{c_2(n) a}}.$$

By Lemma 2.1(iv), we obtain a lower bound:

$$\frac{\text{Prod}(m, q)}{(q - 1)_m} \geq \frac{1}{(q - 1)_m} \cdot \frac{q^m - 1}{q - 1} \geq \frac{q^m - 1}{(q - 1)^2}.$$

Suppose first that $m \geq 3$. Then $(q^m - 1)/(q - 1)^2 > q = p^a$. If $a = 1$, this gives the upper bound $q < (2c_2(n))^{2\sqrt{c_2(n) a}}$ and we are done. Suppose that $a > 1$. Now

$$(2c_2(n) a)^{2\sqrt{c_2(n) a}} = ((2c_2(n))^{2\sqrt{c_2(n) a}})^{\sqrt{a}} (e^{2\sqrt{c_2(n) a}})^{\log(a)\sqrt{a}} \leq c_3(n)^{\sqrt{a} \log a}$$

for some function $c_3(n)$. Hence $a \log p < \sqrt{a} \log a \log(c_3(n))$ which yields

$$\frac{\sqrt{a} \log p}{\log a} < \log(c_3(n)).$$

Since $a > 1$, we have $\sqrt{a}/\log a \geq 1$, so $\log p \leq \log c_3(n)$ and hence $p \leq c_3(n)$. Also, for all $a > 1$, Lemma 2.5 gives

$$\frac{a^{1/4} \log 2}{4} \leq \frac{\sqrt{a} \log 2}{\log a} \leq \frac{\sqrt{a} \log p}{\log a},$$

and hence $a \leq \left(\frac{4}{\log 2} \log(c_3(n))\right)^4$. Thus, when $m \geq 3$, we have shown that all of a , p and d are bounded above by functions of n , and hence $|T|$ is also bounded above by some function of n . If $m = d = 2$ with q even, then $(q-1)_m = 1$ and, by Lemma 2.1(ii), $p^a < q + 1 \leq \text{Prod}(m, q)$. Our arguments therefore give

$$p^a < \text{Prod}(m, q) \leq c_3(n)^{\sqrt{a} \log a},$$

and the same argument yields the required bound.

Now we treat the two exceptional cases: if $m = d = 3$ with 3 dividing $q-1$, then \hat{H} has order $(q^3-1)/(q-1) = q^2+q+1$ and its image $H = \varphi(\hat{H})$ has order $\frac{1}{3}(q^2+q+1)$. Also, by Lemma 2.1(iv), we have $(q^3-1)/(q-1) \leq \text{Prod}(m, q)$. Thus the argument above yields

$$p^a = q < \frac{(q^3-1)}{(q-1)^2} \leq \frac{\text{Prod}(3, q)}{(q-1)_3} = 3 \cdot |H| \leq c'_3(n)^{\sqrt{a} \log a},$$

and the required bound.

Finally assume that $m = d = 2$ with q odd. Here T has unique conjugacy classes of cyclic subgroups of orders $\frac{1}{2}(q+1)$ and $\frac{1}{2}(q-1)$, and one of these orders is odd, say $\frac{1}{2}(q+\delta)$. We choose $H < T$ with H cyclic of odd order $\frac{1}{2}(q+\delta)$, and for each prime s dividing $\frac{1}{2}(q+\delta)$, we consider the Sylow s -subgroup S of H . The index $|N_{\text{Aut}(T)}(S) : C_{\text{Aut}(T)}(S)|$ is $2a$, and hence by Lemma 2.3, the number of $\text{Aut}(T)$ -classes of elements of T of order $|S|$ divides $2a \cdot n!$. Now a very similar argument to that above shows that the product over the primes s of the orders of these Sylow subgroups of H (which equals $|H|$) is bounded above by $c_3(n)^{\sqrt{a} \log a}$ for some function $c_3(n)$, and since $|H| \geq \frac{1}{2}(q-1) \geq p^a/3$, we conclude that p and a , and hence also q are bounded by some function of n . Thus $|T|$ is bounded by a function of n , which completes the proof in the linear case.

Case 2. *The remaining cases with $m = d$ in (ii) and (iii).*

Here T and m are as in Table 3; in each case T contains a cyclic subgroup H with order as in the respective row of Table 3. For each prime s dividing $|H|$, we consider the Sylow s -subgroup S of H . Then H and S have the same centralisers and normalisers in $\text{Aut}(T)$ and the index $r = |N_{\text{Aut}(T)}(S) : C_{\text{Aut}(T)}(S)|$ is as in Table 3.

T	m	$ H $	r
$\mathrm{PSp}(4, q)$	2	$(q^2 + 1)/(2, q - 1)$	$4a \cdot (2, q)$
$\mathrm{PSU}(3, q)$	3	$(q^2 - q + 1)/(3, q + 1)$	$6a$
$\mathrm{PSp}(6, q)$	3	$(q^3 + 1)/(2, q + 1)$	$6a$
$\mathrm{P}\Omega^{\circ}(7, q)$	3	$(q^3 + 1)_{2'}$	$6a$

Table 3. Orders of cyclic subgroups of T in the remaining cases for $m = d$.

By Lemma 2.3, the number of $\mathrm{Aut}(T)$ -classes of elements of T of order $|S|$ is equal to $\phi(|S|)/r$ and hence $\phi(|S|)$ divides $r \cdot n!$, which divides $24a \cdot n!$ in each of these four cases, and this bound is independent of s . Thus in each case

$$|S| = s \cdot \frac{\phi(|S|)}{s - 1} < 2\phi(|S|) \leq 48a \cdot n!.$$

The number of divisors of $24a \cdot n!$ is less than $2\sqrt{24a \cdot n!}$ by [31, Section 8.3], so $|H|$, which is the product of $|S|$ over all s , satisfies

$$|H| \leq (48a \cdot n!)^{2\sqrt{24a \cdot n!}}.$$

On the other hand, in all cases $|H| > q = p^a$. If $a = 1$, then this bounds q by a function of n and we are done. Suppose that $a > 1$. Then

$$|H| \leq (48a \cdot n!)^{2\sqrt{24a \cdot n!}} = ((48 \cdot n!)^{2\sqrt{24 \cdot n!}})^{\sqrt{a}} (e^{2\sqrt{24 \cdot n!}})^{\log(a)\sqrt{a}} \leq c(n)^{\sqrt{a} \log a}$$

for some function $c(n)$. Thus $p^a = q < |H| \leq c(n)^{\sqrt{a} \log a}$, and so taking logs we obtain $(\sqrt{a} \log p)/\log a \leq \log c(n)$. Arguing as in the previous case, this bounds both a and p , and hence also q and $|T|$, by some function of n .

Case 3. *The other classical groups with $m < d$.*

Here m is an odd prime, $d \geq 4$, and the preimage G of T has a cyclic subgroup \hat{H} as in case (U), (Sp), or (O) of Table 2. Since $m < d$, \hat{H} has nontrivial fixed point space in V and hence contains no nontrivial scalars, so $H := \varphi(\hat{H}) \cong \hat{H}$. In all cases $|H|$ divides $q^m + 1$.

By (iii) and (iv) of Lemma 2.1, we have $2 \notin \mathcal{S}(2m)$, and $\mathrm{Prod}(2m, q)$ divides $q^m + 1$ and is divisible by $(q^m + 1)/(q + 1)$. Moreover, by Lemma 2.1(iv)(1), if $s \in \mathcal{S}(2m)$ then s divides $q^m + 1$, and either $(q^m + 1)_s = \mathrm{Prod}(2m, q)_s$ divides $(q^m + 1)/(q + 1)$, or $s = m$ divides $q + 1$. In the former case we have

$$(q^m + 1)_s = |H|_s = \mathrm{Prod}(2m, q)_s,$$

while if $s = m$ divides $q + 1$ then, since m is odd, either we again have

$$(q^m + 1)_s = |H|_s = \mathrm{Prod}(2m, q)_s,$$

or $T = \mathrm{PSU}(m, q)$ and $|H|_m = (q^m + 1)_m/(q + 1)_m$.

Now we argue as in the linear case for the primes in $\mathcal{S}(2m)$ (rather than $\mathcal{S}(m)$). Let $s \in \mathcal{S}(2m)$ and let \hat{S} be the Sylow s -subgroup of \hat{H} and $S = \varphi(\hat{S})$ the Sylow s -subgroup of H . An identical argument to that in the linear case shows that the number of $\text{Aut}(T)$ -classes of elements of T of order $|S|$ is $\phi(|S|)/r$ and divides $n!$, where $r = |N_{\text{Aut}(T)}(H)/C_{\text{Aut}(T)}(H)|$, and for each of the groups in this case r divides $12ma$. The argument thus shows that $\phi(|S|)$ divides $c_2(n)a$ for some function $c_2(n)$, and that there are at most $2\sqrt{c_2(n)a}$ primes in $\mathcal{S}(2m)$. For each prime s where $(q^m + 1)_s = |H|_s = \text{Prod}(2m, q)_s$, we therefore have

$$(q^m + 1)_s = |S| = \frac{s\phi(|S|)}{(s-1)} < 2c_2(n)a.$$

There is at most one prime in $\mathcal{S}(2m)$ for which this condition fails, namely the prime $s = m$ if $m|q+1$ and $T = \text{PSU}(d, q)$. In this exceptional case we have instead that

$$\frac{(q^m + 1)_m}{(q + 1)_m} = |S| = \frac{m\phi(|S|)}{(m-1)} < 2c_2(n)a.$$

Since s is odd, s divides exactly one of $q^m + 1$ and $q^m - 1$. Since $s \in \mathcal{S}(2m)$, we must therefore have that $(q^m + 1)_s = (q^{2m} - 1)_s$. Thus in the case where m does not arise as an exceptional prime in $\mathcal{S}(2m)$, we have

$$\begin{aligned} \text{Prod}(2m, q) &= \prod_{s \in \mathcal{S}(2m)} (q^{2m} - 1)_s \\ &= \prod_{s \in \mathcal{S}(2m)} (q^m + 1)_s \leq (2c_2(n)a)^{2\sqrt{c_2(n)a}} \leq c_3(n)^{\sqrt{a} \log a} \end{aligned}$$

for some $c_3(n)$, and as $\text{Prod}(2m, q) \geq (q^m + 1)/(q + 1) > q = p^a$, we obtain the required bound on q and $|T|$ as before. On the other hand, if m does arise as an exception, so in particular $T = \text{PSU}(d, q)$, then we obtain

$$\frac{\text{Prod}(2m, q)}{(q + 1)_m} = \frac{1}{(q + 1)_m} \prod_{s \in \mathcal{S}(2m)} (q^m + 1)_s \leq (2c_2(n)a)^{2\sqrt{c_2(n)a}} \leq c'_3(n)^{\sqrt{a} \log a}$$

for some $c'_3(n)$. Now

$$\frac{\text{Prod}(2m, q)}{(q + 1)_m} \geq \frac{(q^m + 1)}{(q + 1)^2} \geq \frac{(q^3 + 1)}{(q + 1)^2} > q - 2$$

and the usual argument yields the required bound. \square

Remark 4.3. We comment on the function $f(n)$ which appears in Theorem 1.1. This function is the maximum over the functions for different families of simple groups. From the linear case when $d > 2$ and $q = p$, we have $c_1(n) = n$ so that $c_2(n) = (2n)! \cdot n!$. Then

$$c_3(n) = 2((2n)! \cdot n!)^{2\sqrt{(2n)! \cdot n!}}$$

and so we obtain

$$\log p \leq \log c_3(n) = (2\sqrt{(2n)! \cdot n!}) \log(2 \cdot (2n)! \cdot n!).$$

Since we have $|T| \leq p^{d^2}$, we have shown $\log |T| \leq d^2 \log p$, which gives

$$\log |T| \leq n^2 (2\sqrt{(2n)! \cdot n!}) \log(2 \cdot (2n)! \cdot n!).$$

The functions arising from the other cases of classical simple groups are similar.

Remark 4.4. In the course of the proof of Proposition 4.2 for simple classical groups T , we make use of s -elements, for carefully chosen primes s . One of these primes is the characteristic $s = p$, and for all the other primes s , we bound the number of $\text{Aut}(T)$ -classes of elements of maximal order $\exp(T)_s = |T|_s$, as discussed in Remark 1.3. Thus if $S(T)$ is the set of these primes s , then in our proof of Proposition 4.2 we have bounded $|T|$ by a function of the parameter

$$m'(T) = \max\{m_p(T), m_{S(T)-\exp(T)}\}$$

defined in Remark 1.3. We showed in Remark 3.2 that a similar bound holds for alternating groups. However, our approach to the exceptional groups of Lie type is different from the classical case (see Section 5 below), and it is an open question if such a bound holds for the simple exceptional groups of Lie type.

5. The exceptional groups

In this section we complete the proof of Theorem 1.1 for the simple groups of Lie type that are exceptional. Our treatment is divided into two cases, depending on whether or not there is a torus subgroup whose normaliser is maximal. Remarkably, most families have this property.

Lemma 5.1. *For each simple group T in Table 4, there exists a cyclic subgroup H of the claimed order. Let s be prime dividing $|H|$, H_s be the Sylow s -subgroup of H and z be the corresponding value from Table 4. Then one of the following holds:*

- (1) H_s is characteristic in $N_T(H)$, $N_{\text{Aut}(T)}(H) = N_{\text{Aut}(T)}(H_s)$ and

$$|N_{\text{Aut}(T)}(H) : C_{\text{Aut}(T)}(H_s)|$$

divides $z|\text{Out}(T)|$.

- (2) $T = E_7(q)$, q is odd, $s = 2$ and there is a nontrivial characteristic cyclic 2-subgroup Y_2 of $N_T(H)$ of order at least $|H|_2/2$ such that

$$N_{\text{Aut}(T)}(H) = N_{\text{Aut}(T)}(Y_2) \quad \text{and} \quad |N_{\text{Aut}(T)}(H) : C_{\text{Aut}(T)}(Y_2)|$$

divides $z|\text{Out}(T)|$.

- (3) $T = E_7(q)$, q is odd, $s = 2$ and $|H|_2 \leq 2$.

T	$ H $	$N_T(H)$	z	$ \text{Out}(T) $	notes
${}^2B_2(q)$	$q \pm \sqrt{2q} + 1$	$H.4$	4	a	$q = 2^{2t+1}$ [35, Theorem 9]
${}^2G_2(q)$	$q \pm \sqrt{3q} + 1$	$H.6$	6	a	$q = 3^{2t+1}$ [20, Theorem C]
${}^2F_4(q)$	$q^2 + q + 1 \pm \sqrt{2q}(q + 1)$	$H.12$	12	a	$q = 2^{2t+1}$ [26, Main Theorem]
${}^3D_4(q)$	$q^4 - q^2 + 1$	$H.4$	4	a	[21, Theorem]
$F_4(q)$	$q^4 - q^2 + 1$	$H.12$	12	$2a$	$q > 2$ even [8, Table 8]
$E_6(q)$	$(q^2 + q + 1)/e$	$({}^3D_4(q) \times H).3$	3	$2ae$	[8, Table 9]
${}^2E_6(q)$	$(q^2 - q + 1)/e'$	$({}^3D_4(q) \times H).3$	3	ae'	$q > 2$ [8, Table 10]
$E_7(q)$	$(q - 1)/d$	$(E_6(q) \times H).2$	2	ad	$q \equiv 2 \pmod{3}$ [25, Table 5.1]
$E_7(q)$	$(q + 1)/d$	$({}^2E_6(q) \times H).2$	2	ad	$q \not\equiv 2 \pmod{3}$ [25, Table 5.1]
$E_8(q)$	$(q^4 - 1)(q^4 - q^3 + q) + 1$	$H.30$	30	a	[25, Table 5.2]

Table 4. Choices for a cyclic subgroup H for exceptional groups T defined over a field of size $q = p^a$, p a prime, with $N_T(H)$ maximal, $d = (2, q - 1)$, $e = (3, q - 1)$, $e' = (3, q + 1)$.

Proof. The existence of a cyclic subgroup H of T of the prescribed order is given by the reference in the notes column of Table 4. (For $T = E_7(q)$ see also [7, Table 4.1].) Further, each reference proves that $N_{\text{Aut}(T)}(H)$ is a maximal subgroup of $\text{Aut}(T)$.

Let s be a prime dividing $|H|$ and let H_s be the Sylow s -subgroup of H . We claim that s is coprime to z , except for the case $T = E_7(q)$, q is odd and $s = 2$. This is easy to verify, for example, when $T = E_6(q)$ we have $|H|$ is coprime to 3 unless $q \equiv 1 \pmod{3}$, in which case $q \equiv 1, 4, 7 \pmod{9}$ and so $q^2 + q + 1 \equiv 3 \pmod{9}$, which implies that $|H| = \frac{1}{3}(q^2 + q + 1)$ is coprime to 3; or, for example, when $T = E_8(q)$ then $|H| = (q^4 - 1)(q^4 - q^3 + q) + 1$ is coprime to 30.

Suppose first that $T = E_7(q)$, q is odd and $s = 2$. We may assume that $|H|_2 > 2$ otherwise statement (3) of Lemma 5.1 holds. If $O_2(N_T(H)) \leq H$, then $O_2(N_T(H)) = H_2$ and we set $Y_2 = H_2$. Otherwise, $O_2(N_T(H)) = (H_2).2$. Write $H_2 = \langle y \rangle$. Then since $\langle y^2 \rangle$ is a normal subgroup of $O_2(N_T(H)) = \langle y \rangle.2$ of index 4, we have that $\Phi(O_2(N_T(H))) = \langle y \rangle$ or $\langle y^2 \rangle$ (depending on whether $O_2(N_T(H))/\langle y^2 \rangle$ is cyclic or elementary abelian, respectively). Hence in this case we set $Y_2 = \Phi(O_2(N_T(H)))$. In both cases, Y_2 is a characteristic cyclic subgroup of $N_T(H)$ of order at least $|H|_2/2$ (in particular, $Y_2 \neq 1$). It follows that $N_{\text{Aut}(T)}(H) \leq N_{\text{Aut}(T)}(Y_2)$ and the maximality of $N_{\text{Aut}(T)}(H)$ in $\text{Aut}(T)$ gives equality. Finally, $C_T(H)$ contains $(N_T(H))'' \cong E_6(q)$ or ${}^2E_6(q)$, and $H \leq C_T(H)$, so we have that $|N_{\text{Aut}(T)}(H) : C_{\text{Aut}(T)}(H)|$ divides $z|\text{Out}(T)|$. This proves that statement (2) of Lemma 5.1 holds.

Assume now that T is any of the groups in Table 4, but that if $T = E_7(q)$ and q is odd, then $s \neq 2$. Let H_s be the Sylow s -subgroup of H . Now $N_T(H) = (D \times H).Z$, where D is either trivial or nonabelian simple and Z is a cyclic group of order z , as in Table 4. Since we have excluded the case $s = 2$ when $T = E_7(q)$ and q is

T	$ H $	M	$N_T(H)$	z	$ \text{Out}(T) $	notes
$G_2(q)$	$q^2 + q + 1$	$\text{SL}(3, q) : 2$	$H : 6$	6	$\leq 2a$	[6, Theorem 2.3; 20, Theorem A]
$F_4(q)$	$q^4 + 1$	$2.\Omega_9(q)$	$H.4$	4	a	q odd [8, Table 7; 25, Table 5.1]

Table 5. Choices for a cyclic subgroup H of exceptional groups T when $N_T(H)$ is not maximal, but $N_T(H) < M$ for a unique class of maximal M , $q = p^a$ with p prime.

odd, we have that s is coprime to z . It follows that $H_s = O_s(N_T(H))$, and so H_s is characteristic in $N_T(H)$. Thus

$$N_{\text{Aut}(T)}(H) \leq N_{\text{Aut}(T)}(H_s)$$

and the maximality of $N_{\text{Aut}(T)}(H)$ gives equality. Finally, since $C_T(H)$ contains $D \times H$, we conclude that $|N_{\text{Aut}(T)}(H) : C_{\text{Aut}(T)}(H)|$ divides $z|\text{Out}(T)|$. This proves that statement (1) of Lemma 5.1 holds. \square

Lemma 5.2. *For each simple group T in Table 5, there exists a cyclic subgroup H of the claimed order. Let s be a prime dividing $|H|$, H_s be the Sylow s -subgroup of H and z be the corresponding value in Table 5. Then one of the following holds:*

- (1) H_s is characteristic in $N_T(H)$, $N_{\text{Aut}(T)}(H) = N_{\text{Aut}(T)}(H_s)$ and

$$|N_{\text{Aut}(T)}(H) : C_{\text{Aut}(T)}(H_s)|$$

divides $z|\text{Out}(T)|$.

- (2) $T = G_2(q)$, $q \equiv 1 \pmod{3}$, $s = 3$ and $|H_3| = 3$.
- (3) $T = F_4(q)$, $s = 2$ and $|H_2| = 2$.

Proof. The proof is similar to that of Lemma 5.1, with adjustments since $N_T(H)$ is not maximal in T . Let $T = G_2(q)$ or $T = F_4(q)$ with q odd. For each row of Table 5, take H to be a cyclic subgroup of the specified order inside the specified maximal subgroup M of T (the maximality of M in T is justified by the references in the notes column of Table 5).

Claim. $N_T(H) = N_M(H)$, and the structure of the normaliser is as displayed in the respective column of Table 5.

Proof of Claim. Suppose first that $T = G_2(q)$ and note that $|H|$ has order divisible by a prime t that is a primitive prime divisor of $q^3 - 1$ (and therefore $t \geq 5$). Choose $q_0 = p^b$ with b a minimal divisor of a such that $N_T(H) \leq G_2(q_0) =: T_0$. Now, since T_0 contains no normal cyclic subgroups, we have $N_T(H) \leq L$ for some maximal subgroup L of T_0 (and note that L cannot be a subfield subgroup by the minimality of q_0). From the references in the notes column, we see that L and t are as in Table 6.

L	q_0	t	notes	$q_0^2 + q_0 + 1 \geq$
$2^3.\text{PSL}(3, 2)$	p	7	p odd	13
$\text{PSL}(2, 13)$	4	7		21
J_2	4	7		21
J_1	11	7, 19		133
$\text{PSL}(2, 13)$	$q_0 = p$	7, 13	$p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$	13
$\text{PSL}(2, 13)$	$q_0 = p^2$	7, 13	$p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$	21
$\text{PSL}(2, 8)$	$q_0 = p$	7	$p \equiv 1, 8 \pmod{9}$	307
$\text{PSL}(2, 8)$	$q_0 = p^3$	7	$p \equiv 2, 4, 5, 7 \pmod{9}$	73
$\text{PSU}(3, 3) : 2$	$q_0 = p$	7	$p \geq 5$	31
$\text{SL}(3, q_0) : 2$		t		

Table 6. Possibilities for L with $N_T(H) \leq L$ for $T = G_2(q)$.

L	t
$\text{PGL}(2, 13)$	13
$\text{PSL}(2, 17)$	17
$\text{PSL}(2, 25).2$	13
$\text{PSL}(2, 27).(3)$	13
$3^3 \rtimes \text{SL}(3, 3)$	13
$2.\Omega_9(q_0)$	

Table 7. Possibilities for L with $N_T(H) \leq L$ for $T = F_4(q)$.

Now H is cyclic of order $q^2 + q + 1 \geq q_0^2 + q_0 + 1$, and on comparing the entry for L in Table 6 with the bound in the last column of that table, we see that L contains a cyclic subgroup of order $|H|$ only if either $L = \text{PSL}(2, 13)$, $t = 13$ and $q = q_0 = p = 3$, or $L = \text{SL}(3, q_0) : 2$. In the first case, we have $|H| = 13 = q^2 + q + 1$ and $N_{\text{PSL}(2,13)}(H) = H : 6$, as in Table 5. In the latter case, we have

$$|N_{\text{SL}(3,q_0):2}(H)| = (q_0^2 + q_0 + 1).6 \leq |N_M(H)|.$$

Hence $q = q_0$ and $N_T(H) = N_M(H) = H.6$, again as in Table 5.

Suppose now that $T = F_4(q)$, where q is odd, and note that there is a primitive prime divisor t of $q^8 - 1$ that divides $|H|$ (from which it follows that $t \geq 11$). As above, choose $q_0 = p^b$ with b a minimal divisor of a such that $N_T(H) \leq F_4(q_0) =: T_0$, and let L be a maximal subgroup of T_0 containing $N_T(H)$. Then t divides $|L|$, and so from [8, Tables 1 and 8] we see that L and t are as in Table 7.

For the groups in the first 5 rows of Table 7, we have that a subgroup of L of order t is self-centralising, and thus $|H| = t = q^4 + 1$. Now, since q is odd, we have $|H| = t = q^4 + 1 \geq q_0^4 + 1 \geq 82$, a contradiction. Hence the only possibility

is that $L \cong 2.\Omega_9(q_0)$, and comparing the orders of $N_{2.\Omega_9(q_0)}(H)$ and $N_M(H)$, we have $q = q_0$ and $N_T(H) = N_M(H) = H.4$ as in Table 5. \square

We now turn to the statements of the lemma. First consider the case $T = G_2(q)$. Then s is coprime to z , unless $s = 3$ and $q \equiv 1 \pmod{3}$. If $s = 3$ and $q \equiv 1 \pmod{3}$, then $q^2 + q + 1 \equiv 3 \pmod{9}$, and so $|H|_3 = (q^2 + q + 1)_3 = 3$, and statement (2) of the lemma holds. Suppose now that if $s = 3$ holds, then $q \not\equiv 1 \pmod{3}$. Then $|H| = q^2 + q + 1$ is coprime to 3 and odd, so $O_s(N_T(H)) = H_s$ is a characteristic subgroup of $N_T(H)$, and thus $N_{\text{Aut}(T)}(H) = N_{\text{Aut}(T)}(H_s)$. Arguing similarly to Lemma 5.1, we see that statement (1) of the lemma holds.

Consider now the case $T = F_4(q)$. Since q is odd, we have that $q \equiv \pm 1 \pmod{4}$, and hence $q^4 + 1 \equiv 2 \pmod{4}$. Thus $|H|_2 = 2$ and part (3) of this lemma holds if $s = 2$. If s is odd, then s is coprime to z and hence $O_s(N_T(H)) = H_s$ satisfies part (1) of the lemma, similarly to the previous cases. \square

Proposition 5.3. *There is an increasing integer function h such that, if T is a simple exceptional group of Lie type, and T is pp-bounded by n , then $|T| < h(n)$.*

Proof. Let T be a simple exceptional group of Lie type defined over the field with q elements. Note that since the rank of T is bounded by a constant, we simply need to prove that q is bounded by a function of n . In particular, we may assume that $q > 2$ so that we may use all rows of Table 4.

Case 1. *T is one of the groups appearing in Table 4.*

We apply Lemma 5.1 and consider the outcomes in turn. Let H be the cyclic subgroup of T defined in Lemma 5.1 and let $\pi(H)$ be the set of prime divisors of $|H|$. For $s \in \pi(H)$ let H_s be the Sylow s -subgroup of H . Then, in all cases,

$$(4) \quad \frac{q-1}{2} \leq |H| \quad \text{and} \quad |H| = \prod_{s \in \pi(H)} |H_s|.$$

Case 1(i). *If $T = E_7(q)$, we assume that q is even.*

Now H_s is cyclic and $|H_s| = s^b$ for some $b \geq 1$. Let $\mathcal{C}(s)$ be the set of $\text{Aut}(T)$ -classes of elements $g \in T$ such that $g^{\text{Aut}(T)} \cap H \neq \emptyset$ and $|g| = s^b$. Since T is pp-bounded by n , it follows from Lemma 2.3 that $|\mathcal{C}(s)|$ divides $z|\text{Out}(T)|n!$, which implies that $(s-1)$ divides $360a(n!)$ (using the lowest common multiple of the entries in the z column of Table 4). Since the number of divisors of $360a(n!)$ is at most $2\sqrt{360an!}$, and different values of s give distinct divisors, we have

$$(5) \quad |\pi(H)| \leq 2\sqrt{360a(n!)}.$$

Further, for each $s \in \pi(H)$, Lemma 2.3 combined with the value of the index $|N_{\text{Aut}(T)}(H) : C_{\text{Aut}(T)}(H)|$ from Lemma 5.1 yields

$$(6) \quad |H_s| = s^b = s^{b-1}(s-1)\frac{s}{s-1} = \phi(|H_s|)\frac{s}{s-1} \leq 2z|\text{Out}(T)|n \leq 60an.$$

Thus putting (4), (5) and (6) together, we have

$$\frac{q}{4} \leq \frac{q-1}{2} \leq |H| \leq |\pi(H)| \max_{s \in \pi(H)} (|H_s|) \leq 120an\sqrt{360a(n!)}.$$

This gives

$$\frac{q}{a^{3/2}} \leq f(n),$$

with $f(n) = 480n\sqrt{360a(n!)}$. By Lemma 2.6,

$$\frac{q}{a^{3/2}} = \left(\frac{q}{a}\right)^{3/2} q^{-1/2} \geq \left(\frac{\log 2}{2} q^{1/2}\right)^{3/2} q^{-1/2} = Cq^{1/4}$$

for a constant C . Thus we obtain $q^{1/4} \leq f(n)/C$, which shows that q is bounded by a function of n , and hence $|T| \leq h_1(n)$, for a computable function h_1 .

Case 1(ii). $T = E_7(q)$ and q is odd.

From parts (2) and (3) of Lemma 5.1 we have

$$|H| = |H_2| \left(\prod_{s \in \pi(H), s \text{ odd}} |H_s| \right) \leq \begin{cases} 2(\prod_{s \in \pi(H), s \text{ odd}} |H_s|) & \text{if } |H_2| = 2, \\ 2|Y_2|(\prod_{s \in \pi(H), s \text{ odd}} |H_s|) & \text{if } |H_2| > 2. \end{cases}$$

Since T is pp-bounded by n , an identical argument to that given above shows that

$$|\pi(H)| \leq 2\sqrt{z|\text{Out}(T)|(n!)} \leq 2\sqrt{4a(n!)}.$$

Further, for $s \in \pi(H)$ with s odd, since T is pp-bounded by n , Lemmas 2.3 and 5.1 give, exactly as above, $|H_s| \leq z|\text{Out}(T)|n \leq 4an$. For $s = 2$, suppose that $|H_2| > 2$, so that Lemma 5.1(2) holds. Then Lemma 2.3 gives

$$\frac{|Y_2|}{2} = \phi(|Y_2|) \leq z|\text{Out}(T)|n = 4an,$$

so that $|Y_2| \leq 8an$. Thus

$$|H| \leq 2(8an)(2\sqrt{4a(n!)})$$

and since $|H| \geq \frac{q-1}{2}$, we obtain

$$\frac{q-1}{a^{3/2}} \leq 64n\sqrt{4a(n!)}.$$

Similarly to the above, q is bounded by a function of n , and hence $|T| \leq h_2(n)$, for a computable function h_2 .

Case 2. T appears in Table 5.

Here $T = G_2(q)$ or $T = F_4(q)$ with q odd. We apply Lemma 5.2 and consider the outcomes in turn. Let H be the cyclic subgroup of T defined in Lemma 5.1 and let H_s be the Sylow s -subgroup of H and let $\pi(H)$ be the set of prime divisors of $|H|$.

From parts (2) and (3) of Lemma 5.2, we may write

$$|H| = \begin{cases} (3, q-1) \left(\prod_{s \in \pi(H), s \neq 3} |H_s| \right) & \text{if } T = G_2(q), \\ 2 \left(\prod_{s \in \pi(H), s \neq 2} |H_s| \right) & \text{if } T = F_4(q). \end{cases}$$

Now for any $s \in \pi(H)$ such that $(T, s) \neq (G_2(q), 3)$ or $(F_4(q), 2)$, Lemma 5.2(1) applies, and we argue similarly to the previous cases to obtain $|\pi(H)| \leq 2\sqrt{12an!}$. Further, we have $|H_s| \leq 2z|\text{Out}(T)|n \leq 24an$. This gives

$$q \leq \frac{|H|}{3} \leq 2\sqrt{12an!}(24an)$$

and therefore $|T|$ is bounded by a computable function $h_3(n)$.

Finally, we define $h(n)$ to be the maximum over the functions h_1, h_2 and h_3 , and thus in any of the cases above, we have $|T| \leq h(n)$, as required. \square

6. Proof of Theorem 1.1

We set

$$f(n) = \max\left\{\frac{1}{2}(3n+2)!, g(n), h(n)\right\} + |M|,$$

where $g(n)$ is the function in Proposition 4.2, $h(n)$ is the function in Proposition 5.3 and M is the Monster sporadic simple group. It is clear from the functions g and h that f is an increasing function. Let T be a nonabelian finite simple group. If T is sporadic, then $|T| \leq |M| \leq f(n)$. If T is alternating, classical or an exceptional group of Lie type, then Lemma 3.1, Propositions 4.2 and 5.3, respectively, shows that $|T| \leq f(n)$. This completes the proof of Theorem 1.1.

Acknowledgements

The third author thanks Laci Babai for early discussions about an approach to proving the bound in Theorem 1.1 for Lie type groups of rank one. This research was supported by the Australian Research Council Discovery Project grant DP230101268. We thank the referee for comments on our manuscript.

References

- [1] M. Aschbacher and G. M. Seitz, “Involutions in Chevalley groups over fields of even order”, *Nagoya Math. J.* **63** (1976), 1–91. MR Zbl
- [2] B. Baumeister, A. Maróti, and H. P. Tong-Viet, “Finite groups have more conjugacy classes”, *Forum Math.* **29**:2 (2017), 259–275. MR Zbl
- [3] R. Brauer, “Representations of finite groups”, pp. 133–175 in *Lectures on modern mathematics, I*, edited by T. L. Saaty, Wiley, New York, 1963. MR Zbl
- [4] T. C. Burness, “Fixed point ratios in actions in finite classical groups, II”, *J. Algebra* **309**:1 (2007), 80–138. MR Zbl
- [5] T. C. Burness and M. Giudici, *Classical groups, derangements and primes*, Australian Mathematical Society Lecture Series **25**, Cambridge University Press, Cambridge, 2015. MR Zbl

- [6] B. N. Cooperstein, “Maximal subgroups of $G_2(2^n)$ ”, *J. Algebra* **70**:1 (1981), 23–36. MR Zbl
- [7] D. A. Craven, “On the maximal subgroups of $E_7(q)$ and related almost simple groups”, preprint, 2022. arXiv 2201.07081
- [8] D. A. Craven, “The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ and related almost simple groups”, *Invent. Math.* **234**:2 (2023), 637–719. MR Zbl
- [9] B. Fein, W. M. Kantor, and M. Schacher, “Relative Brauer groups, II”, *J. Reine Angew. Math.* **328** (1981), 39–57. MR Zbl
- [10] G. D. Franceschi, M. W. Liebeck, and E. A. O’Brien, *Conjugacy in finite classical groups*, Springer, 2025. arXiv 2401.07557
- [11] Y. Gao and Y. Yang, “Lower bound for the number of conjugacy classes and irreducible characters”, *Monatsh. Math.* **203**:2 (2024), 341–355. MR Zbl
- [12] M. Giudici, L. Morgan, and C. E. Praeger, “Prime power coverings of groups”, preprint, 2024. arXiv 2412.15543
- [13] S. Guest and C. E. Praeger, “Proportions of elements with given 2-part order in finite classical groups of odd characteristic”, *J. Algebra* **372** (2012), 637–660. MR Zbl
- [14] R. M. Guralnick, “Zeroes of permutation characters with applications to prime splitting and Brauer groups”, *J. Algebra* **131**:1 (1990), 294–302. MR Zbl
- [15] L. Héthelyi and B. Külshammer, “Elements of prime power order and their conjugacy classes in finite groups”, *J. Aust. Math. Soc.* **78**:2 (2005), 291–295. MR Zbl
- [16] N. N. Hung, T. M. Keller, and Y. Yang, “A lower bound for the number of odd-degree representations of a finite group”, *Math. Z.* **298**:3-4 (2021), 1559–1572. MR Zbl
- [17] B. Huppert, *Endliche Gruppen, I*, Grundle. Math. Wissen. **134**, Springer, Berlin, 1967. MR Zbl
- [18] A. Jaikin-Zapirain, “On the number of conjugacy classes of finite nilpotent groups”, *Adv. Math.* **227**:3 (2011), 1129–1143. MR Zbl
- [19] T. M. Keller, “Finite groups have even more conjugacy classes”, *Israel J. Math.* **181** (2011), 433–444. MR Zbl
- [20] P. B. Kleidman, “The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups”, *J. Algebra* **117**:1 (1988), 30–71. MR Zbl
- [21] P. B. Kleidman, “The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups”, *J. Algebra* **115**:1 (1988), 182–199. MR Zbl
- [22] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990. MR Zbl
- [23] E. Landau, “Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante”, *Math. Ann.* **56** (1903), 671–676. Zbl
- [24] M. W. Liebeck and G. M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs **180**, American Mathematical Society, Providence, RI, 2012. MR Zbl
- [25] M. W. Liebeck, J. Saxl, and G. M. Seitz, “Subgroups of maximal rank in finite exceptional groups of Lie type”, *Proc. London Math. Soc.* (3) **65**:2 (1992), 297–325. MR Zbl
- [26] G. Malle, “The maximal subgroups of ${}^2F_4(q^2)$ ”, *J. Algebra* **139**:1 (1991), 52–69. MR Zbl
- [27] G. Malle, G. Navarro, and J. B. Olsson, “Zeros of characters of finite groups”, *J. Group Theory* **3**:4 (2000), 353–368. MR Zbl

- [28] A. Moretó and H. N. Nguyen, “Variations of Landau’s theorem for p -regular and p -singular conjugacy classes”, *Israel J. Math.* **212**:2 (2016), 961–987. MR Zbl
- [29] P. M. Neumann and C. E. Praeger, “A recognition algorithm for special linear groups”, *Proc. London Math. Soc.* (3) **65**:3 (1992), 555–603. MR Zbl
- [30] A. C. Niemeyer and C. E. Praeger, “Estimating proportions of elements in finite groups of Lie type”, *J. Algebra* **324**:1 (2010), 122–145. MR Zbl
- [31] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991. MR Zbl
- [32] C. E. Praeger, “Kronecker classes of fields and covering subgroups of finite groups”, *J. Austral. Math. Soc. Ser. A* **57**:1 (1994), 17–34. MR Zbl
- [33] L. Pyber, “Finite groups have many conjugacy classes”, *J. London Math. Soc.* (2) **46**:2 (1992), 239–249. MR Zbl
- [34] P. Ribenboim, *The little book of bigger primes*, 2nd ed., Springer, New York, 2004. MR Zbl
- [35] M. Suzuki, “On a class of doubly transitive groups”, *Ann. of Math.* (2) **75** (1962), 105–145. MR Zbl
- [36] G. E. Wall, “On the conjugacy classes in the unitary, symplectic and orthogonal groups”, *J. Austral. Math. Soc.* **3** (1963), 1–62. MR Zbl

Received July 31, 2024. Revised November 26, 2024.

MICHAEL GIUDICI
DEPARTMENT OF MATHEMATICS AND STATISTICS
THE UNIVERSITY OF WESTERN AUSTRALIA
PERTH
AUSTRALIA
michael.giudici@uwa.edu.au

LUKE MORGAN
DEPARTMENT OF MATHEMATICS AND STATISTICS
THE UNIVERSITY OF WESTERN AUSTRALIA
PERTH
AUSTRALIA
luke.morgan@uwa.edu.au

CHERYL E. PRAEGER
DEPARTMENT OF MATHEMATICS AND STATISTICS
THE UNIVERSITY OF WESTERN AUSTRALIA
PERTH
AUSTRALIA
cheryl.praeger@emeriti.uwa.edu.au

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Fakultät für Mathematik
Universität Wien
Vienna, Austria
matthias.aschenbrenner@univie.ac.at

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Atsushi Ichino
Department of Mathematics
Kyoto University
Kyoto 606-8502, Japan
atsushi.ichino@gmail.com

Robert Lipshitz
Department of Mathematics
University of Oregon
Eugene, OR 97403
lipshitz@uoregon.edu

Kefeng Liu
School of Sciences
Chongqing University of Technology
Chongqing 400054, China
liu@math.ucla.edu

Sucharit Sarkar
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
sucharit@math.ucla.edu

Dimitri Shlyakhtenko
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
shlyakht@ipam.ucla.edu

Ruixiang Zhang
Department of Mathematics
University of California
Berkeley, CA 94720-3840
ruixiang@berkeley.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2025 is US \$677/year for the electronic version, and \$917/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2025 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 336 No. 1-2 May 2025

In memoriam Gary Seitz

Gary Seitz (1943–2023): In memoriam	1
MARTIN W. LIEBECK, GERHARD RÖHRLE and DONNA TESTERMAN	
Intrinsic components in involution centralizers of fusion systems	7
MICHAEL ASCHBACHER	
On good A_1 subgroups, Springer maps, and overgroups of distinguished unipotent elements in reductive groups	29
MICHAEL BATE, SÖREN BÖHM, BENJAMIN MARTIN and GERHARD RÖHRLE	
The q -Schur category and polynomial tilting modules for quantum GL_n	63
JONATHAN BRUNDAN	
The binary actions of simple groups of Lie type of characteristic 2	113
NICK GILL, PIERRE GUILLOT and MARTIN W. LIEBECK	
Finite simple groups have many classes of p -elements	137
MICHAEL GIUDICI, LUKE MORGAN and CHERYL E. PRAEGER	
Monogamous subvarieties of the nilpotent cone	161
SIMON M. GOODWIN, RACHEL PENGELLY, DAVID I. STEWART and ADAM R. THOMAS	
An extension of Gow's theorem	181
ROBERT M. GURALNICK and PHAM HUU TIEP	
On dimensions of RoCK blocks of cyclotomic quiver Hecke superalgebras	191
ALEXANDER KLESHCHEV	
Representation growth of Fuchsian groups and modular forms	217
MICHAEL J. LARSEN, JAY TAYLOR and PHAM HUU TIEP	
D_4 -type subgroups of $F_4(q)$	249
R. LAWThER	
Constructible representations and Catalan numbers	339
GEORGE LUSZTIG and ERIC SOMMERS	
A reduction theorem for simple groups with $e(G) = 3$	351
RICHARD LYONS and RONALD SOLOMON	
Decomposition numbers in the principal block and Sylow normalisers	367
GUNTER MALLE and NOELIA RIZO	
Levi decompositions of linear algebraic groups and nonabelian cohomology	379
GEORGE J. MCNINCH	
On the intersection of principal blocks	399
GABRIEL NAVARRO, A. A. SCHAEFFER FRY and PHAM HUU TIEP	
Hesselink strata in small characteristic and Lusztig–Xue pieces	415
ALEXANDER PREMÉT	
Multiplicity-free representations of the principal A_1 -subgroup in a simple algebraic group	433
ALUNA RIZZOLI and DONNA TESTERMAN	