Journal of Algebra 322 (2009) 802–832

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Large element orders and the characteristic of Lie-type simple groups ☆

William M. Kantor [a], Ákos Seress [b,*]

[a] University of Oregon, Department of Mathematics, Eugene, OR 97403, United States
[b] The Ohio State University, Department of Mathematics, 231 W 18th Avenue, Columbus, OH 43210, United States

ARTICLE INFO

Article history:
Received 21 January 2009
Available online 19 May 2009
Communicated by Eamonn O'Brien

To John Cannon and Derek Holt on the occasions of their birthdays, in recognition of their important research contributions

Keywords:
Element orders in Lie-type groups
Computation of characteristics

ABSTRACT

We show that the three largest element orders determine the characteristic of Lie-type simple groups of odd characteristic. This result was motivated by algorithmic needs in computations with matrix groups.

1. Introduction

Given a matrix group $G = \langle X\rangle \leqslant \mathrm{GL}(d,q)$, specified by a set X of generators, it seems that a full structural exploration of G is necessary in order to answer even the simplest questions concerning G, such as finding $|G|$ or testing the membership of any given matrix in G (cf. [LG,BB]). Currently, the standard approach to such an exploration is to set up a recursive scheme of homomorphisms, breaking the input into the image and kernel [LG,NS,O'B,Se]. This reduction bottoms out at an absolutely irreducible matrix group G that is simple modulo scalars. At this terminal stage of the recursion, one finds the name (i.e., the isomorphism type) of G, and then sets up an identification with a standard quasisimple group.

For a prime power $q = p^e$, we write $\mathrm{ch}(q) = p$, and for a Lie-type simple group G defined over $\mathrm{GF}(q)$ we write $\mathrm{ch}(G) = p$. For a quasisimple matrix group G one proceeds using the following steps.

☆ This research was partially supported by the NSF and the NSA.

* Corresponding author.
E-mail address: akos@math.ohio-state.edu (Á. Seress).

0021-8693/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2009.05.004

(1) Find the characteristic ch(G) of G. Our previous method for this step [KS2] found the characteristic by examining interactions among the orders of a random selection of group elements. This ran in polynomial time, but was not practical.
(2) Determine the "name" of G. At present, the principal approach for this step is the black box Monte Carlo algorithm in [BKPS], which once again involves examining properties of the orders of a collection of randomly chosen elements.
(3) Produce a "constructive isomorphism" $H \to G$ from the (probable) concrete group H to G, for example using [BLGNPS], [KS1] or [KM]. This allows computations in G to be performed using the natural permutation or matrix representation (if H is alternating or classical), or the Lie algebra or Bruhat decomposition in the case of an exceptional group of Lie type.

The purpose of the present paper is to produce a practical algorithm for Step (1) that once again uses only arithmetic. In the algorithmic part of [KS2] we had to compute element orders and in [BKPS] we worked with *primitive prime divisor properties* of element orders without needing to compute the orders. In this paper, we need to determine whether the orders of random group elements are greater than a bound N linear in the input dimension, and then compute the exact orders only if they are less than N. As a practical consideration, we mention that, similarly to [BKPS] and [KS2], the present methodology involves only one preprocessing to find random group elements, since we never leave the original group.

There is, however, a very different approach to Step (1). A recent algorithm [LO] recursively passes to smaller and smaller subgroups by using random element selections to compute centralizers of involutions in Lie-type groups of odd characteristic; it is efficient both in the polynomial-time and practical senses. Moreover, it is a black-box algorithm that assumes the availability of an oracle to compute element orders. By contrast, in this paper we use arithmetic rather than group theory; but our algorithm is restricted to matrix groups since its proof of correctness depends on results on cross-characteristic representations of Lie-type groups. Our algorithm has the added benefit that, if the input group is a cross-characteristic projective representation of a Lie-type group G, then the algorithm also provides a short list for the possible isomorphism types of G.

Our new approach to Step (1) is motivated by the following observation, which was obtained by extensive computer calculation:

Fact 1.1. *For a simple group G, let*

$$m_1 = m_1(G) \quad \textit{and} \quad m_2 = m_2(G), \quad m_1 > m_2,$$

denote the two largest element orders of G. Let $\mathcal{F}$ be the family of simple groups G of Lie type of rank at most 66 *and defined over a field of size at most* 10^5, excluding the cases $\mathrm{P\Omega}^+(d,2^e)$, $\mathrm{P\Omega}^-(d,2^e)$, *and* $\mathrm{PSp}(d,2^e)$ *for $d > 36$.*

If $G, H \in \mathcal{F}$ with nonisomorphic G, H of different defining characteristics, and if $m_1(G) = m_1(H)$ and $m_2(G) = m_2(H)$, then $\{G,H\} = \{\mathrm{PSL}(2,25), G_2(3)\}$ *with $m_1 = 13$ and $m_2 = 12$,* $\{G,H\} = \{{}^2B_2(8), \mathrm{PSL}(2,13)\}$ *with $m_1 = 13$ and $m_2 = 7$, or* $\{G,H\} = \{\mathrm{PSp}(4,3) \cong \mathrm{PSU}(4,2), \mathrm{PSU}(4,3)\}$ *with $m_1 = 12$ and $m_2 = 9$.*

The computer verification of Fact 1.1, as well as all other computations in this paper, were performed using *GAP* [GAP4]. We programmed formulae as in Appendix A for $m_1(G)$ and $m_2(G)$ for all Lie-type groups G except $\mathrm{PSp}(d,2^e)$, $\mathrm{P\Omega}^+(d,2^e)$ and $\mathrm{P\Omega}^-(d,2^e)$ with $d > 36$, and evaluated them in the indicated range. The difficulties with formulae encountered in characteristic 2 are described at the end of Section 2, where we also observe that there are no such difficulties with special linear, unitary and exceptional groups. Then we collected the pairs $\{G,H\}$ with $m_1(G) = m_1(H)$ and $m_2(G) = m_2(H)$, and discarded those with $\mathrm{ch}(G) = \mathrm{ch}(H)$.

The goal of this paper is to turn the observation in Fact 1.1 into a general theorem and to provide an algorithm for Step (1). Along the way, we have obtained nonalgorithmic results interesting in their own right, and the bulk of the paper consists of the proofs of those results.

Let $m_3(G)$ denote the third largest element order for G.

Theorem 1.2. *Let G and H be simple groups of Lie type of odd characteristic. If $m_i(G) = m_i(H)$ for $1 \leqslant i \leqslant 3$, then* $\mathrm{ch}(G) = \mathrm{ch}(H)$.

We can “almost” prove that the two largest element orders determine the characteristic. Our main result is the following

Theorem 1.3. *Let G and H be simple groups of Lie type of odd characteristic. If $m_1(G) = m_1(H)$ and $m_2(G) = m_2(H)$, then one of the following holds*:

(i) $\mathrm{ch}(G) = \mathrm{ch}(H)$;
(ii) $\{G, H\} = \{\mathrm{PSL}(2, q), G_2(p)\}$ *with q composite, p prime, and $q = 2p^2 + 2p + 1$; or*
(iii) *G and H are symplectic of dimension at least* 8 *or unitary of dimension at least* 4*, defined over a prime field* (*the groups G, H need not be of the same type*).

In the proof of Theorem 1.2, we consider the third largest element order only in the ambiguous cases listed in parts (ii) and (iii) of Theorem 1.3. There are infinite families of pairs of nonisomorphic groups satisfying (i), for example $\mathrm{PSp}(2m, q)$ and $\Omega(2m + 1, q)$ for odd composite q, and $\mathrm{PSU}(q, q)$ and $\mathrm{PSU}(q + 1, q)$ for any odd prime power $q \notin \{3, 9\}$. We conjecture that the only example in (ii) is $\{G, H\} = \{\mathrm{PSL}(2, 25), G_2(3)\}$, and that there are no examples in (iii); both of these conjectures seem to involve difficult number theory.

Our main proof method is to consider the first three terms of the continued fraction expansion of $m_1/(m_1 - m_2)$, and determine the characteristic as a function of these terms. We include the rather large set of groups in (iii) because, for these groups, $m_1/(m_1 - m_2)$ is an integer and hence the continued fraction expansion provides only one term and our method breaks down. The brute force approach, trying to prove that the Diophantine system of equations $m_1(G) = m_1(H)$, $m_2(G) = m_2(H)$, has no solution for two sets of $\{m_1, m_2\}$ formulae taken from different characteristics, seems to be hopeless. Of course there are a few groups that can be defined over fields of different characteristics (and one might, in fact, argue that the groups $\mathrm{PSU}(4, 2) \cong \mathrm{PSp}(4, 3)$ and $\mathrm{PSU}(4, 3)$ mentioned in Fact 1.1 do not constitute a genuine counterexample to the claim that m_1, m_2 determine the characteristic). If we include the sporadic groups then there are a few more examples of groups with the same m_1, m_2 values: for M_{11} and M_{12} we have $m_1 = 11$ and $m_2 = 8$; for $\mathrm{P}\Omega^+(8, 2)$ and J_2 we have $m_1 = 15$ and $m_2 = 12$; for ${}^3D_4(2)$ and He we have $m_1 = 28$ and $m_2 = 21$; for $\mathrm{PSp}(8, 2)$, Co_3, and Fi_{22} we have $m_1 = 30$ and $m_2 = 24$; and for Co_1 and Fi_{23} we have $m_1 = 60$ and $m_2 = 42$.

The two largest orders of *semisimple* elements (i.e., elements whose order is not divisible by $\mathrm{ch}(G)$) also determine the characteristic:

Theorem 1.4. *Let $m'_1 = m'_1(G)$ and $m'_2 = m'_2(G)$, $m'_1 > m'_2$, denote the two largest orders of semisimple elements in a simple group G of Lie type. If G and H are simple groups of Lie type of odd characteristic such that $m'_1(G) = m'_1(H)$ and $m'_2(G) = m'_2(H)$, then either* $\mathrm{ch}(G) = \mathrm{ch}(H)$ *or* $\{G, H\} \subset \{G_2(2)' \cong \mathrm{PSU}(3, 3), \mathrm{PSU}(4, 3), \mathrm{PSU}(3, 5)\}$ *with $m'_1 = 8$ and $m'_2 = 7$.*

In Section 2, we give the two largest element orders in Lie-type simple groups defined over fields of odd characteristic, and explain why we had to exclude the groups of characteristic 2 from our theorems. Section 3 contains the proof of Theorem 1.3. Theorem 1.2 is proved in Section 4. The proof of Theorem 1.4 is in Section 5. That section also introduces a variant (m_1^*, m_2^*) of (m_1, m_2), and formulae for these pairs (m_1^*, m_2^*) are the basis of the algorithmic application. The algorithm is described in Section 6, where we prove the following

Theorem 1.5. *There is a Monte Carlo algorithm which, when given an absolutely irreducible group $K \leqslant \mathrm{GL}(d, p^e)$ such that $K/Z(K)$ is isomorphic to a simple group G of Lie type, outputs a list of numbers which contains the characteristic of G. The running time is $O(\xi \log^2 d \log\log d + \mu d^3(\log^3 d(\log\log d)^2 + \log^2 d \log\log d \log p^e))$, where ξ is the cost of constructing a* (*nearly*) *uniformly distributed random element of K and μ is the cost of a field operation in* $\mathrm{GF}(p^e)$.

The output list has at most 6*d members. Moreover, if $d < 3 \cdot 10^5$ then the output list has length one*: *the algorithm computes* $\mathrm{ch}(G)$.

In *polynomial time*, this algorithm *returns a list of at most* 6*d numbers including* ch(*G*) *that are candidates for the characteristic*. The estimate 6*d* is very crude, and is irrelevant for practical performance. In fact, the algorithm of Theorem 1.5 computes ch(*G*) if $d < 973\,455/3 = 324\,485$, where 973 455 is a lower bound for the largest semisimple element order in groups $\mathrm{PSp}(d, 2^e)$, $\mathrm{P\Omega}^+(d, 2^e)$ and $\mathrm{P\Omega}^-(d, 2^e)$ of characteristic 2 and rank greater than 18. Moreover, in Remark 6.6 we shall indicate how to lower the output length to at most two (either to p, or to 2 and at most one odd number) for any value of d. This improvement is asymptotically slower, but still runs in polynomial time. It is even likely that the algorithm of Theorem 1.5 computes the characteristic for inputs in all dimensions. This would follow from proving the purely group-theoretic Conjecture 5.9.

If $\mathrm{ch}(G) \neq p$ then our algorithm has an added benefit: it also outputs a very short list for the possible isomorphism types of the simple group G, so Step (2) at the beginning of this introduction becomes far easier. The algorithm has been implemented in *GAP*: since 2006 it has been part of the matrix recognition package `recog` [NS].

Recall that a randomized algorithm is called *Monte Carlo* if its output may be incorrect, but the probability of erroneous output can be bounded from above by the user. The *projective order* of $g \in \mathrm{GL}(d, p^e)$ is the smallest nonnegative integer $k = \|g\|$ such that g^k is a scalar matrix. For a prime power q and prime r, we say that r is a *primitive prime divisor of* $q^m - 1$, in notation r is a $\mathrm{ppd}^\#(q; m)$ number, if $r \mid q^m - 1$ and $r \nmid q^i - 1$ for all $i < m$.

2. The two largest element orders

Appendix A to this paper contains tables that list the two largest element orders in simple groups G of Lie type with ch(G) odd. We often have to distinguish between the cases where q is prime or composite.

Theorem 2.1. *Tables* A.1–A.7 *are correct.*

Proof. We give a general indication how these formulae were derived, and then provide details in two cases: $\mathrm{P\Omega}^-(2m, q)$ (which is the most complicated of the classical group cases) and the exceptional groups of Lie type.

Semisimple elements. These are contained in maximal tori. In the classical (linear) groups $\mathrm{GL}(d, q)$, $\mathrm{Sp}(d, q)$, $\mathrm{GU}(d, q)$, and $\mathrm{SO}^\varepsilon(d, q)$, maximal tori are direct products of cyclic groups Z_i of order $q^{j_i} + 1$ or $q^{j_i} - 1$ for exponents j_i whose sum is d in the special linear and unitary cases, and $\lfloor d/2 \rfloor$ in the symplectic and orthogonal cases; moreover, there are restrictions on the ± signs occurring in the terms $q^{j_i} \pm 1$ [Ca].

In the special linear and unitary cases, let $T = \prod_{i=1}^k Z_i$, $|Z_i| = q^{j_i} \pm 1$, be a maximal torus in $\mathrm{GL}(d, q)$ or $\mathrm{GU}(d, q)$ (only minus signs occur in the special linear case, while $q^{j_i} \pm 1 = q^{j_i} - (-1)^{j_i}$ in the unitary case). Let $g \in T \cap \mathrm{SL}(d, q)$ or $T \cap \mathrm{SU}(d, q)$. Let M be the least common multiple of the numbers $(q^{j_i} - 1)/(q - 1)$ in the special linear and $(q^{j_i} \pm 1)/(q + 1)$ in the unitary case, for $i = 1, \ldots, k$. Then g^M is a scalar matrix on each g-invariant subspace in the natural representation of $\mathrm{GL}(d, q)$ or $\mathrm{GU}(d, q)$, so $g^{(q\pm1)M} = 1$. Note that $(q^{i_1} - 1, q^{i_2} - 1)$ is divisible by $q - 1$ in the special linear case, while $(q^{i_1} \pm 1, q^{i_2} \pm 1)$ is divisible by $q + 1$ in the unitary case. Here $q \pm 1$ is factored out of $|T|$ because we consider $T \cap \mathrm{SL}(d, q)$ or $T \cap \mathrm{SU}(d, q)$, and after that the center (of order $(d, q \pm 1)$) of the resulting group is also factored out. We need the resulting subgroup $\overline{T}$ of G to be cyclic, as otherwise the largest element order in $\overline{T}$ would be at least a factor $q \pm 1$ smaller than $|\overline{T}|$ and hence too small. Therefore, there are $k \leqslant 3$ factors $q^{j_i} \pm 1$, and $k \leqslant 2$ except when $(d, q + 1) = q + 1$ in the unitary case. Straightforward calculations show that the projective image of $g \in T \cap \mathrm{SL}(d, q)$ or $T \cap \mathrm{SU}(d, q)$ in the corresponding simple group G has order at most the numbers $m_1(G), m_2(G)$ in Table A.1 or A.2, and those numbers occur as orders.

Similarly, in the symplectic and orthogonal cases, as above $T = \prod_{i=1}^k Z_i \leqslant \mathrm{Sp}(d, q)$ or $\mathrm{SO}^\epsilon(d, q)$, $|Z_i| = q^{j_i} \pm 1$, and M denotes the least common multiple of the numbers $(q^{j_i} \pm 1)/2$. If $g \in T$ then $g^M = \pm 1$ on each g-invariant subspace and so $g^{2M} = 1$. If $k \geqslant 4$, or if there are two cyclic groups with

$(q^{i_1} \pm 1, q^{i_2} \pm 1) > 2$, then $2M$ is either a polynomial in q of degree less than $\lfloor d/2 \rfloor$, or the leading coefficient of $2M$ is at most $1/8$ and so $2M < m_2$ in the corresponding table. (In the polynomials that arise here, all nonzero coefficients have absolute value one or two times the leading coefficient, so the leading term dominates.) Once we know that we have to consider tori that are products of at most three cyclic subgroups Z_i, it is straightforward to discover how to choose the exponents j_i in order to maximize the corresponding element orders m_1, m_2. We will do this below for $\mathrm{P}\Omega^-(2m,q)$.

The maximal tori of the exceptional groups are more explicitly known than in the classical groups, and the above process is therefore easier (see below).

Nonsemisimple elements. We also have to consider the maximal orders of nonsemisimple elements. Such elements are in parabolic subgroups, which are obtained by deleting sets of nodes from the Dynkin diagram. Also, if $q = p^e$ and the maximal semisimple order, written as a polynomial in p, is a polynomial of degree k, then the maximal order of a nonsemisimple element is a polynomial of degree at most $k - e + 1$. (More details of such arguments will be given below for the groups $\mathrm{P}\Omega^-(2m,q)$ and for the exceptional groups.) In particular, *for composite q, the numbers m_1, m_2 are orders of semisimple elements.*

The group $\mathbf{P\Omega^-(2m, q)}$: semisimple elements. Each semisimple element of $\mathrm{SO}^-(2m,q) = \mathrm{SO}^-(V)$ lies in a maximal torus T, and T is a direct product arising from an orthogonal decomposition of V:

$$\begin{aligned} V &= (2a_1)^+ \perp \cdots \perp (2a_s)^+ \perp (2b_1)^- \perp \cdots \perp (2b_t)^- \\ T &= \left(q^{a_1} - 1\right) \times \cdots \times \left(q^{a_s} - 1\right) \times \left(q^{b_1} + 1\right) \times \cdots \times \left(q^{b_t} + 1\right) \end{aligned} \tag{2.1}$$

with t odd and the integers in parentheses representing cyclic groups of the indicated orders. We are looking for elements of large order in such a torus, and the existence of elements whose orders are in Table A.6 shows that the two largest semisimple element orders in the simple group are at least $(q^m + 1)/(4, q^m + 1)$.

When $q = 3$ any terms $q \pm 1$ can disappear due to factoring by $(4, 3^m + 1)$. Therefore this case requires additional care and leads to a small number of special situations listed in Table A.6, so here we will only deal with the case $q \geqslant 5$.

There are various elementary requirements:

(i) The gcd of any two terms $q^c \pm 1$ must be 2, since we seek elements of order $\geqslant (q^m + 1)/(4, q^m + 1)$. Therefore we cannot have two factors of the form $q^{a_i} - 1$, since $q > 3$.
(ii) If $|T| = (q^j - 1)(q^{m-j} + 1)$, then $j > m - j$ since $|T| > q^m$. In particular, there is no $q - 1$ factor.
(iii) There are at most 3 factors $q^c \pm 1$, since each factor is even and we are only factoring from $|T|$ by $(4, q^m + 1)$.
There are only two such factors when $(4, q^m + 1) = 2$.
Therefore, in (2.1) we have to consider only the following three possibilities:

$$\begin{array}{llll} V\colon & (2j_1)^- & (2j_1)^- \perp (2j_2)^+ & (2j_1)^- \perp (2j_2)^- \perp (2j_3)^- \\ T\colon & (q^{j_1} + 1) & (q^{j_1} + 1)(q^{j_2} - 1) & (q^{j_1} + 1)(q^{j_2} + 1)(q^{j_3} + 1). \end{array}$$

(iv) If $|T| = (q^a + 1)(q^b + 1)(q^c + 1)$, then 4 divides exactly one of the indicated factors. (In fact, three factors can occur precisely when a Sylow 2-subgroup of T has the form $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^a}$ with $a \geqslant 2$. For then the spinor norm condition produces a subgroup $\mathbb{Z}_2 \times \mathbb{Z}_{2^a}$, and factoring out -1 produces a *cyclic* group $\mathbb{Z}_{2^a}$. Note that it is essential to have $a \geqslant 2$ here so that the product of the three involutions in the indicated cyclic factors of T is in the subgroup of index 2 corresponding to spinor norm 0.)
It follows that $q \equiv 3 \pmod 4$ and exactly one of the exponents a, b, c is odd.

We need to handle small dimensions separately, as is evident from Table A.6. When $8 \leqslant 2m \leqslant 14$, we list the possibilities for T allowed by the above requirements:

$$\begin{array}{llll}
\mathrm{P\Omega}^-(8,q) & q^4+1 & \big(q^3-1\big)(q+1) & \\
\mathrm{P\Omega}^-(10,q) & q^5+1 & \big(q^3-1\big)\big(q^2+1\big) & \\
\mathrm{P\Omega}^-(12,q) & q^6+1 & \big(q^5-1\big)(q+1) & \\
\mathrm{P\Omega}^-(14,q) & q^7+1 & \big(q^5-1\big)\big(q^2+1\big) & (q+1)\big(q^2+1\big)\big(q^4+1\big).
\end{array}$$

In each of the first three cases, the listed orders, divided by $(q^m+1,4)$, are the two largest semisimple element orders and appear in Table A.6. For $\mathrm{P\Omega}^-(14,q)$, the first two are largest when $q \equiv 1 \pmod 4$, while the second and third are largest when $q \equiv 3 \pmod 4$.

Suppose now that m is even. Then $(q^{m-1}-1)(q+1)$ is the largest order. By (i) and (ii), since $m > 6$ we see that $(q^{m-3}-1)(q^3+1)$ or $(q^{m-2}-1)(q^2+1)$ is the second largest order depending on whether 4 divides $m-2$ or not. Thus, Table A.6 holds for semisimple elements when m is even.

As Table A.6 indicates, the situation is more complicated when m is odd. Here $(q^{m-1}-1)(q+1)$ is not allowed by (i), but $(q^{m-2}-1)(q^2+1)$ can occur. The next smallest possible factorization using just two factors is $(q^{m-4}-1)(q^4+1)$. When $q \equiv 1 \pmod 4$ there are only 2 factors by (iii), and the 2 largest element orders are $(q^{m-2}-1)(q^2+1)/2$ and $(q^{m-4}-1)(q^4+1)/2$, as in Table A.6.

We are left with the case $q \equiv 3 \pmod 4$, where we can obtain larger element orders using three factors. For example, if $(m-3)/2$ is even then $|T|$ can be $(q^{m-3}+1)(q^2+1)(q+1)$; and it is easy to check that the next largest possibility is $|T| = (q^{m-5}+1)(q^4+1)(q+1)$, as in Table A.6.

Finally, assume that $m \equiv 1 \pmod 4$, and write $m = 2^{e-1}a+1$ with $e \geqslant 2$ and a odd. We search for a suitable torus of order $(q+1)(q^i+1)(q^j+1)$ with $i+j = 2^{e-1}a$ and $i > j$. Here (i) forces $i/(i,j)$ or $j/(i,j)$ to be even, and then $i+j = 2^{e-1}a$ implies that i and j are even. By a similar argument, assuming that $a \geqslant 3$ we have $i = 2^{e-1}i_*$, $j = 2^{e-1}j_*$ with $i_*+j_* = a$. This produces a torus of largest order when $i_* = a-1$; the order is $(q+1)(q^{2^{e-1}(a-1)}+1)(q^{2^{e-1}}+1)$, yielding an entry in Table A.6. The next order of this form is $(q+1)(q^{2^{e-1}(a-2)}+1)(q^{2^e}+1)$, which is recorded in Table A.6 if $a > 3$. If $a = 3$ then the preceding order is the same as the largest one, and we need a different type of order. The next possibilities use $(q^2+1)(q^i+1)(q^j+1)$ with $i+j = 2^{e-1}3-1$. Since $2m > 14$, the largest of these occurs when $\{i,j\} = \{3, 2^{e-1}3-4\}$, as in Table A.6. The same type of argument takes care of the case $a = 1$.

The groups $\mathbf{P\Omega^-(2m,q)}$: all elements. It remains to deal with nonsemisimple elements $g = us = su$ with s semisimple and $u \neq 1$ unipotent. Previously we dealt with a torus first and then sought an element g, now we need to be slightly more careful. Let Z denote the center of $\Omega^-(2m,q) = \Omega^-(V)$, of order $(4,q^m+1)/2$. We have $|g| > q^m/2$ and $|gZ| > 2q^m/(4,q^m+1)$ (since g is in $\Omega^-(V)$ rather than $\mathrm{SO}^-(V)$).

The various eigenvalues of s over the algebraic closure of $\mathrm{GF}(q)$ cannot all be distinct, since u must act nontrivially on some eigenspace of s. Thus, s decomposes V as $V = V_1 \perp V_2$ with V_1 and V_2 sharing no eigenvalue over any extension field, where V_1 is the perpendicular sum of r copies of a nondegenerate $2c$-space W on each of which s acts the same: as a linear transformation of order dividing $q^c \pm 1$ and hence of determinant 1. Let g_i denote the restriction of g to V_i. Then g_1 is the commuting product of $s|_{V_1}$ and a unipotent element, and hence has determinant 1: g_i is in $\mathrm{SO}^-(V_i)$ though not necessarily in $\Omega^-(V_i)$.

If W has type $\Omega^-(2c,q)$, then the homogeneity of g_1 implies that V_1 can be viewed as a $\mathrm{GF}(q^{2c})$-space. Then $|g_1| \leqslant (q^c+1)p^k$, where $k = \lceil \log_p(rc) \rceil$ using the p-exponent of $\Omega^\pm(2rc,q^c)$. Similarly, if W has type $\Omega^+(2c,q)$, then $|g_1| \leqslant (q^c-1)p^k$.

By induction, $|g_2| < 2q^{m-rc}$ since $\dim V_2 = 2(m-rc)$, so that $|g| < (q^c+1)p^k 2q^{m-rc}$. Also $|g| > q^m/(q^m+1,4)$. It follows that $q = p$, $c = 1$ and $r = 2$.

Moreover, V_1 is of type $\mathrm{P\Omega}^+(4,q)$ and $|g_1|$ divides $q \pm 1$. Consequently, we cannot repeat this argument using g_2 in place of g, so that p cannot divide $|g_2|$. Thus, u has order p and $[V,u] \subseteq V_1$.

Since $|g_1|$ divides $q \pm 1$, this means that u is a long root element of G and $|g_1| = p(q \pm 1)$. Now $|g| > q^m/(q^m+1, 4)$ implies that $|g_1| = p(q+1)$.

At this point we again need to examine semisimple elements $g_2 \in \mathrm{SO}^-(2m-4, q)$ with $|g_2| > q^{m-2}$, where there are at most two factors in the decomposition (2.1) associated to g_2, neither of which has order $q+1$. The latter additional information greatly simplifies the preceding semisimple case, and leads to the remaining entries in Table A.6.

Exceptional groups of Lie type. First consider the largest two semisimple orders. Here the structure of maximal tori was collected in [KS2] from the literature; this information was also recently recomputed in [H]. With one exception, it is easy to read off the two largest orders of semisimple elements from the tables in [KS2] or [H]. The only difficulty concerns the maximal torus $\mathbb{Z}_{q^4+1} \times \mathbb{Z}_{(q+1)(q^2+1)}$ in $2.E_7(q)$. If $q \equiv 3 \pmod 4$ then this torus has a cyclic homomorphic image in $E_7(q)$, while if $q \equiv 1 \pmod 4$ then the homomorphic image is noncyclic, leading to different polynomials for m_1 in the two congruence classes modulo 4 in Table A.7.

Note that each of the two largest semisimple orders is larger than q^k, where k is the absolute rank of G (the rank over the algebraic closure of $\mathrm{GF}(q)$).

It remains to deal with nonsemisimple elements. Here we can write such an element using its Jordan decomposition: $g = su = us$ with s semisimple and $u \neq 1$ unipotent. The centralizers of unipotent elements of exceptional groups of odd characteristic were described in [LiS, pp. 185–198]. It is straightforward to deduce that, for a nontrivial unipotent $u \in G$, $C_G(u)$ has an element of order greater than q^k only if u belongs to a long root group (or a short root group in the case $G_2(3^e)$, where there is a graph automorphism interchanging the long and short root groups); recall that the maximal semisimple order, written as a polynomial in p, is a polynomial of degree k.

Thus, suppose that u belongs to a long root group X. Then $N_G(X)$ is a maximal parabolic subgroup, and has a Levi decomposition $N_G(X) = QL$ with Q unipotent and L a Levi factor. We may assume that $g = us$ with $u \in Q$ and $s \in O^{p'}(L)$. Therefore, $|g|$ is largest when s is an element of largest order in $O^{p'}(L)$, a group of Lie type of rank one less than that of G.

Moreover, L is a classical group except when $G = E_8(q)$ and $L = 2.E_7(q)$. Thus, using the classical group case, or the semisimple case for $2.E_7(q)$, it is straightforward to verify that Table A.7 contains all instances where nonsemisimple elements have largest or second largest order.

Characteristic 2. We next describe the obstacles for groups of characteristic 2. For special linear and unitary groups, the above argument remains valid: semisimple elements of the two largest orders must come from tori that are the products of at most 3 cyclic groups, and usually at most 2.

Exceptional groups also do not cause any problems in characteristic 2. Explicit lists of the maximal tori are known (collected in [KS2] from the literature, and also calculated independently in [H]), making a list as in Table A.7 straightforward in the semisimple case. Nonsemisimple elements need to be considered only in exceptional groups defined over GF(2), for which all element orders are known.

However, for symplectic and orthogonal groups there is no bound on the number of cyclic factors in the tori we have to consider, because there are arbitrarily large collections of pairwise relatively prime integers of the form $2^j \pm 1$, and we have to consider partitions of $\lfloor d/2 \rfloor$ into a sum of such integers j. For each concrete value of d, in principle it is possible to determine the tori giving the two largest semisimple element orders. However, we do not have general formulae for all d: these depend in some manner on delicate number-theoretic data involving partitions of the integer $\lfloor d/2 \rfloor$. Moreover, when $q = 2$, m_1 and m_2 can be even and divisible by different powers of 2. For example, $m_1(\mathrm{PSp}(26,2)) = 2(2^1+1)(2^2+1)(2^4+1)(2^5-1)$, $m_2(\mathrm{PSp}(26,2)) = 2^2(2^1+1)(2^2+1)(2^8+1)$ and $m_1(\mathrm{PSp}(36,2)) = 2^3(2^1+1)(2^2+1)(2^4+1)(2^8+1)$, $m_2(\mathrm{PSp}(36,2)) = (2^1+1)(2^2+1)(2^4+1)(2^{11}-1)$. Hence, although groups of characteristic 2 were included in the computations establishing Fact 1.1, we had to exclude such groups from Theorem 1.3.

Computer checks. The order formulae in Tables A.1–A.7 were also checked experimentally using *GAP*, by constructing the appropriate quasisimple matrix groups over a large variety of fields and computing the projective orders of large samples of random elements.

3. Proof of Theorem 1.3

Before going into the details of the proof, we outline the basic idea. As we have seen in Section 2, the maximal orders m_1, m_2 can be viewed as polynomials in the underlying field size q. Our goal is to construct low-degree polynomials in q as functions of m_1 and m_2. We use these polynomials to read off the value of q (or at least $\mathrm{ch}(q)$). For example, we consider the greatest common divisor (m_1, m_2), and $a_0 := \lfloor m_1/(m_1 - m_2) \rfloor$. Here are some examples where q can be found as a simple function of m_1, m_2 and a_0. For most d and q, if q is prime and G is an orthogonal group defined over $\mathrm{GF}(q)$ then $2(m_1 - m_2)/(m_1, m_2) - 1 = q$; if G is orthogonal or symplectic and q is composite, then $a_0 - 2 \in \{q, q^2\}$; and if G is unitary and q is composite then $a_0 - 1 = q$. There are exceptions to these rules, mostly in low rank, that we have to recognize; and of course we also have to identify the exceptional groups from the pair (m_1, m_2). To help identify which family of groups the input belongs to, we not only consider a_0 but the first three terms a_0, a_1, a_2 of the continued fraction decomposition

$$\frac{m_1}{m_1 - m_2} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots}}}. \tag{3.1}$$

We also consider variants

$$\begin{aligned}
\frac{m_1}{m_1 - m_2} &= b_0 - \frac{1}{b_1 + \frac{1}{b_2 + \frac{1}{\cdots}}}\\
\frac{m_1}{m_1 - m_2} &= a_0 + \frac{1}{a_1 + 1 - \frac{1}{a_2' + \frac{1}{\cdots}}}\\
\frac{m_1}{m_1 - m_2} &= b_0 - \frac{1}{b_1 + 1 - \frac{1}{b_2' + \frac{1}{\cdots}}}.
\end{aligned} \tag{3.2}$$

We use connections between the quantities (m_1, m_2), a_0, b_0, a_1, b_1, a_2, a_2', b_2, b_2' to determine $\mathrm{ch}(G)$. Some of these connections are trivial and provide no useful information regarding $\mathrm{ch}(G)$ (for example, if $m_1/(m_1 - m_2)$ is not an integer then $b_0 = a_0 + 1$, and if $a_1 = 1$ then $a_2 = b_1 - 1$); moreover, the continued fraction decompositions may end before a_2, a_2', b_2, b_2' are defined. If the continued fraction terminates before a_i is defined then we write "$a_i = \mathrm{fail}$." We also use the notation "$a_i \neq \mathrm{fail}$" if the continued fraction has an ith term. Similar definitions hold for a_i', b_i, b_i'.

Examining Tables A.1–A.7, we see that low-rank classical groups often have different formulae for m_1, m_2 than in the "generic" case. Also, small values of q (in particular, $q = 3$) often behave differently, and when we write the integers a_i, b_i as polynomials of q, for small values of q the leading term may not be the dominant one. When *both* q and the rank are small, the behavior of m_1 and m_2 is so different that we have to treat those cases individually.

For any fixed bound B, it is clear from Tables A.1–A.7 that there are only finitely many groups G with $m_1(G) < B$. Hence, we can check that Theorem 1.3 holds for the groups in the set

$$\begin{aligned}
\mathcal{S}_0 := \big\{ &\mathrm{PSL}(2,5), \mathrm{PSL}(2,7), \mathrm{PSL}(4,3), \mathrm{PSL}(4,5), \mathrm{PSL}(5,3), \mathrm{PSL}(5,5), \mathrm{PSL}(5,7),\\
&\mathrm{PSL}(5,19), \mathrm{PSL}(5,23), \mathrm{PSL}(5,25), \mathrm{PSL}(8,3), \mathrm{PSU}(3,3), \mathrm{PSU}(3,5), \mathrm{PSU}(3,9),\\
&\mathrm{PSU}(4,3), \mathrm{PSU}(10,9), \mathrm{PSp}(4,3), \mathrm{PSp}(6,3), \mathrm{PSp}(6,5), \mathrm{PSp}(6,7), \mathrm{PSp}(6,11),\\
&\mathrm{PSp}(8,3), \mathrm{PSp}(8,5), \mathrm{PSp}(8,7), \Omega(7,3), \mathrm{P\Omega}^+(8,3), \mathrm{P\Omega}^+(20,3), \mathrm{P\Omega}^+(20,5),\\
&\mathrm{P\Omega}^+(20,11), \mathrm{P\Omega}^-(10,3), \mathrm{P\Omega}^-(10,5), \mathrm{P\Omega}^-(10,7), \mathrm{P\Omega}^-(10,9), \mathrm{P\Omega}^-(10,13),\\
&\mathrm{P\Omega}^-(10,125), \mathrm{P\Omega}^-(18,3), \mathrm{P\Omega}^-(18,5), \mathrm{P\Omega}^-(18,7), \mathrm{P\Omega}^-(18,19), \mathrm{P\Omega}^-(18,31),\\
&{}^2G_2(3)', {}^3D_4(3), {}^3D_4(5), F_4(3), E_6(3), E_6(5), E_6(9), E_6(11), E_7(3), E_8(3) \big\}:
\end{aligned}$$

for $G \in \mathcal{S}_0$, with the exceptions mentioned in Fact 1.1, there is no simple group $H \not\cong G$ of Lie type with $m_1(G) = m_1(H)$, $m_2(G) = m_2(H)$, and $\mathrm{ch}(G) \neq \mathrm{ch}(H)$ (recall that Fact 1.1 includes groups of characteristic 2).

We will focus on the set $\mathcal{C} := \mathcal{S} \setminus \mathcal{S}_0$, where $\mathcal{S}$ denotes the set of simple groups of Lie type of odd characteristic. In the rest of this section, we prove Theorem 1.3 for the family $\mathcal{C}$ by providing an algorithm which, given $m_1(G)$, $m_2(G)$, identifies whether G belongs to the exceptions described in Theorem 1.3(ii), (iii), and computes $\mathrm{ch}(G)$ as a function of $m_1(G)$ and $m_2(G)$ if this is not the case.

We partition $\mathcal{C}$ based on properties of $m_1(G)$ and $m_2(G)$, so that all groups within a partition class have a common formula to compute $\mathrm{ch}(G)$. This partition is not natural, and its definition was aided by extensive computer experiments.

We first partition $\mathcal{C}$ into five sets:

$$\begin{aligned}
\mathcal{C}_1 &:= \bigl\{G \in \mathcal{C} \bigm| m_1 - m_2 > (m_1, m_2)^2 > 1\bigr\}\\
\mathcal{C}_2 &:= \bigl\{G \in \mathcal{C} \bigm| (m_1, m_2)^2 \geqslant m_1 - m_2 > (m_1, m_2) > 1\bigr\}\\
\mathcal{C}_3 &:= \bigl\{G \in \mathcal{C} \bigm| m_1 - m_2 = (m_1, m_2) > 1\bigr\}\\
\mathcal{C}_4 &:= \bigl\{G \in \mathcal{C} \bigm| (m_1, m_2) = 1 \,\&\, m_1 \leqslant (m_1 - m_2)^{3/2}\bigr\}\\
\mathcal{C}_5 &:= \bigl\{G \in \mathcal{C} \bigm| (m_1, m_2) = 1 \,\&\, m_1 > (m_1 - m_2)^{3/2}\bigr\}.
\end{aligned}$$

The set $\mathcal{C}_1$ contains most orthogonal, symplectic and unitary groups defined over fields of composite size, and for most of these groups either $a_0 - 1$ or $a_0 - 2$ is a power of q. Our task is to separate those groups in $\mathcal{C}_1$ that do not satisfy this last condition. To this end, we further partition $\mathcal{C}_1$ as follows:

$$\begin{aligned}
\mathcal{C}_{11} &:= \bigl\{G \in \mathcal{C}_1 \bigm| a_1 > 1 \,\&\, (3a_1)^2 < a_0\bigr\}\\
\mathcal{C}_{12} &:= \bigl\{G \in \mathcal{C}_1 \bigm| (3a_1)^2 \geqslant a_0 \,\&\, a_2 = \text{fail} \,\&\, a_0 = a_1\bigr\}\\
\mathcal{C}_{13} &:= \bigl\{G \in \mathcal{C}_1 \bigm| (3a_1)^2 \geqslant a_0 \,\&\, a_2 = \text{fail} \,\&\, a_0 \neq a_1\bigr\}\\
\mathcal{C}_{14} &:= \bigl\{G \in \mathcal{C}_1 \bigm| (3a_1)^2 \geqslant a_0 \,\&\, a_2 \neq \text{fail} \,\&\, a_0 = a_1 + 1\bigr\}\\
\mathcal{C}_{15} &:= \bigl\{G \in \mathcal{C}_1 \bigm| a_1 = 1 \,\&\, b_1 = (m_1, m_2)\bigr\}\\
\mathcal{C}_{16} &:= \bigl\{G \in \mathcal{C}_1 \bigm| a_1 = 1 \,\&\, b_1 < a_0 \,\&\, b_2' = 2\bigr\}\\
\mathcal{C}_{17} &:= \bigl\{G \in \mathcal{C}_1 \bigm| a_1 = 1 \,\&\, b_1 < a_0 \,\&\, b_2' = 9\bigr\}\\
\mathcal{C}_{18} &:= \{G \in \mathcal{C}_1 \mid a_1 = 1 \,\&\, b_1 < a_0 \,\&\, b_2 = 4\}\\
\mathcal{C}_{19} &:= \{G \in \mathcal{C}_1 \mid a_1 = 1 \,\&\, b_1 < a_0 \,\&\, b_1 - 4b_2 = 6\}\\
\mathcal{C}_{110} &:= \bigl\{G \in \mathcal{C}_1 \bigm| a_1 = 1 \,\&\, b_1 > a_0 > 5 \,\&\, a_0 \equiv 1 \pmod 2\bigr\}\\
\mathcal{C}_{111} &:= \mathcal{C}_1 \setminus \bigcup_{i=1}^{10} \mathcal{C}_{1i}.
\end{aligned}$$

Remark 3.1. The assertions in Propositions 3.2–3.10 can be verified by straightforward but tedious checking using the formulae in Tables A.1–A.7. We express the integers a_i, b_i as polynomials in q. These expressions may not be valid for small values of q. For example, for $G = E_6(q)$, if $q \geqslant 5$ is prime then $a_0 = q^2 - 1$, $a_1 = 1$, and $a_2 = q$; but for $q = 3$ we have $a_2 = q + 1$, so we placed the group $E_6(3)$ in $\mathcal{S}_0$. It is also possible that the parameters of a group "accidentally" satisfy a condition designed for another class. Still considering the set of groups $\mathcal{G} = \{E_6(q) \mid q \geqslant 5 \text{ prime}\}$, all groups in $\mathcal{G}$ belong to $\mathcal{C}_{15}$. However, $E_6(5)$ also satisfies the defining condition of $\mathcal{C}_{16}$ so we placed $E_6(5)$ in $\mathcal{S}_0$. It is also possible that infinite subfamilies satisfy some accidental numerical property, and in this case we have to devise a refinement of our partition classes $\mathcal{C}_{ij\ldots}$. The primary example is the subfamily $\mathrm{PSL}(16k+14, q)$, where the generic behavior occurs only for $q > 151$ (cf. Proposition 3.10 and the class $\mathcal{C}_{549a}$). The exact determination of which groups had to be placed in $\mathcal{S}_0$, and the check of validity of Propositions 3.2–3.10 for small rank and field size, were aided by computer calculations. Computer experiments also helped to find the appropriate definitions of the classes $\mathcal{C}_{ij\ldots}$.

Proposition 3.2. *For $G \in \mathcal{C}$,*

(1) *$G \in \mathcal{C}_{11}$ if and only if $G = \mathrm{P}\Omega^-(2^e+2, q)$ for some $e \geqslant 5$ and composite $q \equiv 3 \pmod 4$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(2a_1+3)$.

(2) *$G \in \mathcal{C}_{12}$ if and only if $G = \mathrm{PSp}(6, q)$ or $G = \Omega(7, q)$ for some composite q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.

(3) *$G \in \mathcal{C}_{13}$ if and only if $G = G_2(q)$ for some composite $q \equiv 1 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0+1)$.

(4) *$G \in \mathcal{C}_{14}$ if and only if $G = {}^2E_6(q)$ for some prime q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.

(5) *$G \in \mathcal{C}_{15}$ if and only if $G = E_6(q)$ for some prime q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(b_1-1)$.

(6) *$G \in \mathcal{C}_{16}$ if and only if $G = \mathrm{P}\Omega^+(16, 3^e)$ for some $e \geqslant 2$. In this case,* $\mathrm{ch}(G) = 3$.

(7) *$G \in \mathcal{C}_{17}$ if and only if either $G = \mathrm{P}\Omega^+(16, q)$ for some composite $q \equiv 1 \pmod 3$ or $G = \mathrm{P}\Omega^-(18, q)$ for some prime $q \equiv 7 \pmod{12}$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(3b_1+1)$.

(8) *$G \in \mathcal{C}_{18}$ if and only if either $G = \mathrm{P}\Omega^+(16, q)$ for some composite $q \equiv 2 \pmod 3$ or $G = \mathrm{P}\Omega^-(18, q)$ for some prime $q \equiv 11 \pmod{12}$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(3b_1-1)$.

(9) *$G \in \mathcal{C}_{19}$ if and only if $G = \mathrm{P}\Omega^-(18, q)$ for some composite $q \equiv 3 \pmod 4$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(b_1-3)$.

(10) *$G \in \mathcal{C}_{110}$ if and only if $G = \mathrm{P}\Omega^-(14, q)$ for some composite $q \equiv 3 \pmod 4$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.

(11) *$G \in \mathcal{C}_{111}$ if and only if G is on the following list*: $\mathrm{PSp}(2k, q)$ *or* $\Omega(2k+1, q)$ *with $k \geqslant 5$ and q composite*; $\mathrm{PSU}(d, q)$ *with $d \geqslant 8$, $d \notin \{9, 15\}$ and q composite*; $\mathrm{P}\Omega^+(8k, q)$ *with $k \geqslant 3$ and q composite*; $\mathrm{P}\Omega^+(8k+4, q)$ *with $k \geqslant 1$*; $\mathrm{P}\Omega^+(4k+2, q)$ *with $k \geqslant 2$ and q composite,* except $\mathrm{P}\Omega^+(16k+2, q)$ *with $k \geqslant 2$ and $q \equiv 1 \pmod 4$ composite*; $\mathrm{P}\Omega^-(8k, q)$ *with $k \geqslant 2$ and q composite*; $\mathrm{P}\Omega^-(18, q)$ *with $q \equiv 1 \pmod 4$*; $\mathrm{P}\Omega^-(8k+2, q)$ *with $k \geqslant 3$ and all q,* except *$k \in \{2^e \mid e \geqslant 2\} \cup \{7 \cdot 2^e \mid e \geqslant 0\} \cup \{3\}$ and $q \equiv 3 \pmod 4$ composite*; $\mathrm{P}\Omega^-(8k+4, q)$ *with $k \geqslant 2$ and q composite*; $\mathrm{P}\Omega^-(8k+6, q)$ *with $k \geqslant 2$ and $q \equiv 1 \pmod 4$*; $\mathrm{P}\Omega^-(8k+6, q)$ *with $k \geqslant 2$ and composite $q \equiv 3 \pmod 4$ except $k = 3$*; ${}^3D_4(q)$ *with q prime*; $F_4(q)$ *with q composite*; $E_8(q)$ *with $q \not\equiv 1 \pmod 3$ composite and $q \not\equiv 1 \pmod{12}$ prime.*
In this case, $a_0 = q^{2^m}+2$ or $a_0 = q^{2^m}+1$ for some $m \geqslant 0$, and so $\mathrm{ch}(G) = \mathrm{ch}(a_0-2)$ *if a_0 is odd and* $\mathrm{ch}(G) = \mathrm{ch}(a_0-1)$ *if a_0 is even.*

The set $\mathcal{C}_2$ contains most orthogonal groups defined over prime fields. Let $r := 2(m_1-m_2)/(m_1,m_2)-1$; for most such groups, $r = q$. However, we need to separate those groups in $\mathcal{C}_2$ that do not satisfy $r = q$. Partition $\mathcal{C}_2$ as follows:

$$\mathcal{C}_{21} := \{G \in \mathcal{C}_2 \mid a_1 > a_0\}$$

$$\mathcal{C}_{22} := \bigl\{G \in \mathcal{C}_2 \bigm| (m_1,m_2) = 4\bigr\}$$

$$\mathcal{C}_{23} := \{G \in \mathcal{C}_2 \mid 2a_0 - r = 1\}$$

$$\mathcal{C}_{24} := \{G \in \mathcal{C}_2 \mid 2a_0 - r = 3\}$$

$$\mathcal{C}_{25} := \bigl\{G \in \mathcal{C}_2 \bigm| (m_1,m_2) \neq 4 \,\&\, 2 \leqslant a_0/a_1 < 4\bigr\}$$

$$\mathcal{C}_{26} := \mathcal{C}_2 \setminus \bigcup_{i=1}^{5} \mathcal{C}_{2i}.$$

Proposition 3.3. *For $G \in \mathcal{C}$,*

(1) *$G \in \mathcal{C}_{21}$ if and only if $G = \mathrm{PSU}(15, q)$ for some composite q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0-1)$.

(2) *$G \in \mathcal{C}_{22}$ if and only if either $G = \Omega(2k+1,3)$ for some $k \geqslant 4$, or $G = \mathrm{P}\Omega^+(4k+2,3)$ for some $k \geqslant 2$, or $G = \mathrm{P}\Omega^-(4k,3)$ for some $k \geqslant 2$. In this case,* $\mathrm{ch}(G) = 3$.
(3) *$G \in \mathcal{C}_{23}$ if and only if $G = {}^2E_6(q)$ for some composite q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(4) *$G \in \mathcal{C}_{24}$ if and only if either $G = \mathrm{PSU}(7,q)$ for some composite q or $G = E_8(q)$ for some composite $q \equiv$* $7 \pmod{12}$ *or some $q \equiv 1 \pmod{12}$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$.
(5) *$G \in \mathcal{C}_{25}$ if and only if $G = \mathrm{P}\Omega^-(2k,q)$ for some $k \in \{13\} \cup \{7 \cdot 2^e + 1 \mid e \geqslant 1\}$ and composite $q \equiv$* $3 \pmod 4$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 2)$.
(6) *$G \in \mathcal{C}_{26}$ if and only if G is on the following list: $F_4(q)$ for some prime q; $\Omega(2k+1,q)$ for some $k \geqslant 4$ and prime $q \geqslant 5$; $\mathrm{P}\Omega^+(2k,q)$ for some $k \geqslant 5$, $k \not\equiv 2 \pmod 4$ and prime $q \geqslant 5$; $\mathrm{P}\Omega^+(8k,3)$ for some $k \geqslant 2$; $\mathrm{P}\Omega^-(8k,q)$ for some $k \geqslant 1$ and prime $q \geqslant 5$; $\mathrm{P}\Omega^-(8k+6,q)$ for some $k \geqslant 1$ and prime $q \equiv 3 \pmod 4$. In this case, $r = q$ and so* $\mathrm{ch}(G) = \mathrm{ch}(r)$.

The set $\mathcal{C}_3$ contains most symplectic and unitary groups defined over prime fields. In $\mathcal{C}_3$, we lose our major tool because the continued fraction expansion of $m_1/(m_1 - m_2)$ does not provide numbers a_i, b_i for $i \geqslant 1$. Partition the set $\mathcal{C}_3$ as follows; $\mathcal{C}_{38}$ isolates the potential examples in Theorem 1.3(iii).

$$\mathcal{C}_{31} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ a_0 = 2\bigr\}$$
$$\mathcal{C}_{32} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ 2 < a_0 = (m_1, m_2) - 1\bigr\}$$
$$\mathcal{C}_{33} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ 2 < a_0 < (m_1, m_2) - 1 \ \&\ 4a_0 - 2 = (m_1, m_2)\bigr\}$$
$$\mathcal{C}_{34} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ 2 < a_0 < (m_1, m_2) - 1 \ \&\ 4a_0 - 2 \neq (m_1, m_2)\bigr\}$$
$$\mathcal{C}_{35} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ a_0 = 3(m_1, m_2) - 1\bigr\}$$
$$\mathcal{C}_{36} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ a_0 > 3(m_1, m_2) - 1 \ \&\ 8a_0 - 4 = (m_1, m_2)^2\bigr\}$$
$$\mathcal{C}_{37} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 > a_0^{3/2} \ \&\ a_0 > 3(m_1, m_2) - 1 \ \&\ 8a_0 - 4 \neq (m_1, m_2)^2\bigr\}$$
$$\mathcal{C}_{38} := \bigl\{G \in \mathcal{C}_3 \bigm| m_1 \leqslant a_0^{3/2}\bigr\}.$$

Proposition 3.4. *For $G \in \mathcal{C}$,*

(1) *$G \in \mathcal{C}_{31}$ if and only if $G = \mathrm{P}\Omega^+(8,q)$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(4m_1 + 1)$.
(2) *$G \in \mathcal{C}_{32}$ if and only if $G = \mathrm{PSU}(3,q)$ for some prime $q \equiv 1 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(3) *$G \in \mathcal{C}_{33}$ if and only if $G = \mathrm{PSp}(4,q)$ for some prime q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(2a_0 - 1)$.
(4) *$G \in \mathcal{C}_{34}$ if and only if $G = \Omega_7(q)$ for some prime q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$.
(5) *$G \in \mathcal{C}_{35}$ if and only if $G = \mathrm{PSU}(3,q)$ for some prime $q \equiv 2 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(6) *$G \in \mathcal{C}_{36}$ if and only if $G = \mathrm{PSp}(6,q)$ for some prime q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(2a_0 - 1)$.
(7) *$G \in \mathcal{C}_{37}$ if and only if $G = E_7(q)$ for some prime $q \equiv 1 \pmod 4$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(2(m_1, m_2) + 1)$.
(8) *$G \in \mathcal{C}_{38}$ if and only if $G = \mathrm{PSp}(2k,q)$ for some $k \geqslant 4$ and prime q or $G = \mathrm{PSU}(d,q)$ for some $d \geqslant 4$ and prime q.*

The set $\mathcal{C}_4$ contains mostly low-rank groups, and the characteristics of its members are easy to determine. Partition $\mathcal{C}_4$ as follows:

$$\mathcal{C}_{41} := \bigl\{G \in \mathcal{C}_4 \bigm| b_1 > 1 \ \&\ a_0 \equiv 0 \pmod 2\bigr\}$$
$$\mathcal{C}_{42} := \bigl\{G \in \mathcal{C}_4 \bigm| b_1 > 1 \ \&\ a_0 \equiv 1 \pmod 2\bigr\}$$
$$\mathcal{C}_{43} := \bigl\{G \in \mathcal{C}_4 \bigm| b_1 = 1 \ \&\ a_0 \equiv 1 \pmod 2 \ \&\ a_1 \equiv 1 \pmod 2\bigr\}$$
$$\mathcal{C}_{44} := \bigl\{G \in \mathcal{C}_4 \bigm| b_1 = 1 \ \&\ a_0 \equiv 1 \pmod 2 \ \&\ a_1 \equiv 0 \pmod 2\bigr\}$$

$$\mathcal{C}_{45} := \{G \in \mathcal{C}_4 \mid b_1 = 1 \;\&\; a_0 = 2\}$$
$$\mathcal{C}_{46} := \bigl\{G \in \mathcal{C}_4 \bigm| b_1 = 1 \;\&\; a_0 > 2 \;\&\; a_0 \equiv 0 \pmod 2\bigr\}.$$

Proposition 3.5. *For $G \in \mathcal{C}$,*

(1) *$G \in \mathcal{C}_{41}$ if and only if $G = \mathrm{PSL}(6,q)$ for some q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 + 1)$.
(2) *$G \in \mathcal{C}_{42}$ if and only if $G = \mathrm{PSU}(6,q)$ for some composite q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(3) *$G \in \mathcal{C}_{43}$ if and only if $G = \mathrm{P\Omega}^+(16k+2,q)$ for some $k \geqslant 2$ and composite $q \equiv 1 \pmod 4$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 2)$.
(4) *$G \in \mathcal{C}_{44}$ if and only if either $G = {}^3D_4(q)$ for some composite q or $G = E_7(q)$ for some composite $q \equiv 1 \pmod 4$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(5) *$G \in \mathcal{C}_{45}$ if and only if $G = \mathrm{PSL}(2,q)$ for some prime q. In this case,* $\mathrm{ch}(G) = m_1$.
(6) *$G \in \mathcal{C}_{46}$ if and only if G is on the following list*: $\mathrm{PSU}(d,q)$ *for some* $d \in \{5,9\}$ *and composite* q; $\mathrm{PSp}(8,q)$ *for some composite* q; $\Omega(9,q)$ *for some composite* q; $\mathrm{P\Omega}^-(2k,q)$ *for some* $k \in \{4,6\}$ *and composite* q; $\mathrm{P\Omega}^-(14,q)$ *for some* $q \equiv 1 \pmod 4$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$.

The set $\mathcal{C}_5$ contains most of the special linear groups. This is quite a difficult category to handle, because in special linear groups a_0 is not a small-degree polynomial in the size of the defining field. As a preliminary step, we partition $\mathcal{C}_5$ into four parts:

$$\mathcal{C}_{51} := \bigl\{G \in \mathcal{C}_5 \bigm| \mathrm{fail} \in \{a_1, a_2\} \text{ or } \max\{a_1, b_1\} = 2\bigr\}$$
$$\mathcal{C}_{52} := \{G \in \mathcal{C}_5 \setminus \mathcal{C}_{51} \mid b_1 > 2\}$$
$$\mathcal{C}_{53} := \bigl\{G \in \mathcal{C}_5 \setminus \mathcal{C}_{51} \bigm| a_1 > 2 \;\&\; a_2' > 1\bigr\}$$
$$\mathcal{C}_{54} := \bigl\{G \in \mathcal{C}_5 \setminus \mathcal{C}_{51} \bigm| a_1 > 2 \;\&\; a_2' = 1\bigr\}.$$

Now partition $\mathcal{C}_{51}$ as follows, where $\mathcal{C}_{511}$ isolates the potential examples in Theorem 1.3(ii).

$$\mathcal{C}_{511} := \{G \in \mathcal{C}_{51} \mid m_1 - m_2 = 1\}$$
$$\mathcal{C}_{512} := \{G \in \mathcal{C}_{51} \mid a_1 > 2 \;\&\; a_2 = \mathrm{fail} \;\&\; a_0 - 3a_1 = 4\}$$
$$\mathcal{C}_{513} := \{G \in \mathcal{C}_{51} \mid a_1 > 2 \;\&\; a_2 = \mathrm{fail} \;\&\; a_0 - 3a_1 = -3\}$$
$$\mathcal{C}_{514} := \{G \in \mathcal{C}_{51} \mid a_1 = 2 \;\&\; a_2 = 3\}$$
$$\mathcal{C}_{515} := \{G \in \mathcal{C}_{51} \mid a_1 = 2 \;\&\; a_2 = 11\}$$
$$\mathcal{C}_{516} := \bigl\{G \in \mathcal{C}_{51} \bigm| a_1 = 2 \;\&\; a_2' = 11\bigr\}$$
$$\mathcal{C}_{517} := \bigl\{G \in \mathcal{C}_{51} \bigm| a_1 = 2 \;\&\; a_2' = 5\bigr\}$$
$$\mathcal{C}_{518} := \bigl\{G \in \mathcal{C}_{51} \bigm| a_1 = 2 \;\&\; a_2' > 1 \;\&\; a_2' \notin \{5, 11\}\bigr\}$$
$$\mathcal{C}_{519} := \{G \in \mathcal{C}_{51} \mid b_1 = 2\}.$$

Proposition 3.6. *For $G \in \mathcal{C}$,*

(1) *$G \in \mathcal{C}_{511}$ if and only if $G = G_2(q)$ for some prime q or $G = \mathrm{PSL}(2,q)$ for some composite q or $G = \mathrm{PSp}(4,q)$ for some composite q.*
(2) *$G \in \mathcal{C}_{512}$ if and only if $G = \mathrm{PSU}(3,q)$ for some composite $q \equiv 2 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 2)$.
(3) *$G \in \mathcal{C}_{513}$ if and only if $G = \mathrm{PSL}(3,q)$ for some $q \equiv 1 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 + 1)$.
(4) *$G \in \mathcal{C}_{514}$ if and only if $G = \mathrm{PSL}(4k+3,5)$ for some $k \geqslant 0$. In this case,* $\mathrm{ch}(G) = 5$.

(5) *$G \in \mathcal{C}_{515}$ if and only if $G = \mathrm{PSL}(8k, 3)$ for some $k \geqslant 2$. In this case,* $\mathrm{ch}(G) = 3$.
(6) *$G \in \mathcal{C}_{516}$ if and only if $G = \mathrm{PSL}(4k+3, 7)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 7$.
(7) *$G \in \mathcal{C}_{517}$ if and only if $G = \mathrm{PSL}(16k+2, 3)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 3$.
(8) *$G \in \mathcal{C}_{518}$ if and only if $G = {}^2G_2(3^{2e+1})$ for some $e \geqslant 1$. In this case,* $\mathrm{ch}(G) = 3$.
(9) *$G \in \mathcal{C}_{519}$ if and only if $G = \mathrm{PSL}(4k+3, 3)$ for some $k \geqslant 0$. In this case,* $\mathrm{ch}(G) = 3$.

For the groups $G = G_2(3)$ and $H = \mathrm{PSL}(2,25)$ we have $m_1(G) = m_1(H) = 13$ and $m_2(G) = m_2(H) = 12$. *We conjecture that this is the only example in $\mathcal{C}_{511}$ where m_1 and m_2 do not determine the characteristic.* The following lemma, pointed out by László Seress, may be the first step toward proving this conjecture.

Partition $\mathcal{C}_{511}$ as follows.

$$\mathcal{C}_{5111} := \{G \in \mathcal{C}_{511} \mid m_1 = 13\}$$

$$\mathcal{C}_{5112} := \{G \in \mathcal{C}_{511} \mid m_1 \neq 13 \,\&\, 2m_1 - 1 \text{ square}\}$$

$$\mathcal{C}_{5113} := \{G \in \mathcal{C}_{511} \mid m_1 \neq 13 \,\&\, 2m_1 - 1 \text{ nonsquare}\}.$$

Lemma 3.7. *For $G \in \mathcal{C}_{511}$,*

(1) *$G \in \mathcal{C}_{5111}$ if and only if either $G = G_2(3)$ or $G = \mathrm{PSL}(2,25)$.*
(2) *$G \in \mathcal{C}_{5112}$ if and only if either $G = \mathrm{PSL}(2,q)$ for some square q or $G = \mathrm{PSp}(4,q)$ for some composite q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(2m_1 - 1)$.
(3) *$G \in \mathcal{C}_{5113}$ if and only if either $G = \mathrm{PSL}(2,q)$ for some composite but nonsquare q, or $G = G_2(q)$ for some prime $q > 3$.*

Proof. Suppose that $m_1 \neq 13$. If $G = \mathrm{PSL}(2,q)$ for some square (and so necessarily composite) q then, by Table A.1, $2m_1 - 1 = q$ and if $G = \mathrm{PSp}(4,q)$ for some composite q then $2m_1 - 1 = q^2$. Conversely, if $2m_1 - 1$ is a square then clearly $G \neq \mathrm{PSL}(2,q)$ for a nonsquare q and it is enough to prove that $G \neq G_2(p)$ for any prime $p > 3$.

If $G = G_2(p)$ then $2m_1 - 1 = 2p^2 + 2p + 1$, so it is enough to prove that the Diophantine equation $2p^2 + 2p + 1 = x^2$ has no solution for a prime $p > 3$. If $p^2 + (p+1)^2 = x^2$ then $(p, p+1, x)$ is a Pythagorean triple of relatively prime integers, so there exist integers u, v such that $p = u^2 - v^2$, $p + 1 = 2uv$, and $x = u^2 + v^2$. Since $p = (u-v)(u+v)$ is a prime, we must have $u - v = 1$ and $u + v = p$. This implies that $u = (p+1)/2$, $v = (p-1)/2$, and then $p + 1 = 2uv = (p^2 - 1)/2$, for which the only positive solution is $p = 3$. □

Partition $\mathcal{C}_{52}$ as follows, where $\mathcal{C}_{523}$, $\mathcal{C}_{524}$, and $\mathcal{C}_{527}$ are the first instances in our partitions that isolate special linear groups in infinitely many dimensions over infinitely many fields.

$$\mathcal{C}_{521} := \{G \in \mathcal{C}_{52} \mid b_1 - a_0 = -2\}$$

$$\mathcal{C}_{522} := \{G \in \mathcal{C}_{52} \mid b_1 - a_0 = 3\}$$

$$\mathcal{C}_{523} := \{G \in \mathcal{C}_{52} \mid b_1 - a_0 < -2 \,\&\, b_1 \leqslant b_2\}$$

$$\mathcal{C}_{524} := \bigl\{G \in \mathcal{C}_{52} \bigm| b_1 - a_0 < -2 \,\&\, b_1 - 5b_2 \in \{4,5,6,7,8\}\bigr\}$$

$$\mathcal{C}_{525} := \{G \in \mathcal{C}_{52} \mid b_1 - a_0 < -2 \,\&\, b_1 = 8 \,\&\, b_2 = 3\}$$

$$\mathcal{C}_{526} := \{G \in \mathcal{C}_{52} \mid b_1 - a_0 < -2 \,\&\, b_1 = 8 \,\&\, b_2 = 2\}$$

$$\mathcal{C}_{527} := \bigl\{G \in \mathcal{C}_{52} \bigm| b_1 - a_0 < -2 \,\&\, b_1 > b_2 \,\&\, b_1 \neq 8 \,\&\, b_1 - 5b_2 \notin \{4,5,6,7,8\}\bigr\}.$$

Proposition 3.8. *For $G \in \mathcal{C}$,*

(1) *$G \in \mathcal{C}_{521}$ if and only if $G = \mathrm{PSU}(4,q)$ for some composite q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.

(2) *$G \in \mathcal{C}_{522}$ if and only if $G = \mathrm{PSL}(4,q)$ for some q. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0+1)$.
(3) *$G \in \mathcal{C}_{523}$ if and only if $G = \mathrm{PSL}(16k+10,q)$ for some $k \geqslant 0$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(b_1)$.
(4) *$G \in \mathcal{C}_{524}$ if and only if $G = \mathrm{PSL}(8k+4,q)$ for some $k \geqslant 1$ and $q > 5$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(b_1-2)$.
(5) *$G \in \mathcal{C}_{525}$ if and only if $G = \mathrm{PSL}(8k+4,3)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 3$.
(6) *$G \in \mathcal{C}_{526}$ if and only if $G = \mathrm{PSL}(8k+4,5)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 5$.
(7) *$G \in \mathcal{C}_{527}$ if and only if $G = \mathrm{PSL}(16k+6,q)$ for some $k \geqslant 1$. In this case, let q_0 be the smallest integer such that $b_1 \leqslant q_0^3 + 2q_0^2 + 4q_0 + 30$. Then $q = q_0$ and so* $\mathrm{ch}(G) = \mathrm{ch}(q_0)$.

We are left with the most complicated cases: $\mathcal{C}_{53}$ and $\mathcal{C}_{54}$. Here, the groups $\mathrm{PSL}(16k+14,q)$ cause difficulties: if $q \geqslant 17$ then $a_2 = \lfloor (q+1)/17 \rfloor$ and if $q < 17$ then a_2 follows no simple pattern (but a_2 is independent of k). Moreover, if $17 \leqslant q \leqslant 31$ then a_2' follows no simple pattern. Hence the cases $q \leqslant 31$ have to be handled one at a time.

Define $\mathcal{C}_{53x} = \{G \in \mathcal{C}_{53} \mid a_2' = x\}$, $2 \leqslant x \leqslant 11$, and $\mathcal{C}_{5312} = \{G \in \mathcal{C}_{53} \mid a_2' > 11\}$. We partition $\mathcal{C}_{532}$ and $\mathcal{C}_{533}$ further:

$$\begin{aligned}
\mathcal{C}_{532a} &:= \{G \in \mathcal{C}_{532} \mid a_1 = 5\} \\
\mathcal{C}_{532b} &:= \{G \in \mathcal{C}_{532} \mid a_1 = 12\} \\
\mathcal{C}_{532c} &:= \{G \in \mathcal{C}_{532} \mid a_1 = 596\} \\
\mathcal{C}_{532d} &:= \bigl\{G \in \mathcal{C}_{532} \bigm| a_1 \in \{14\,467, 18\,325, 22\,815, 27\,985\}\bigr\} \\
\mathcal{C}_{532e} &:= \bigl\{G \in \mathcal{C}_{532} \setminus (\mathcal{C}_{532a} \cup \mathcal{C}_{532b} \cup \mathcal{C}_{532c} \cup \mathcal{C}_{532d}) \bigm| \\
&\qquad (6a_1+5)^3 + (6a_1+5)^2 + 2(6a_1+5) + 4 = a_0\bigr\} \\
\mathcal{C}_{532f} &:= \bigl\{G \in \mathcal{C}_{532} \setminus (\mathcal{C}_{532a} \cup \mathcal{C}_{532b} \cup \mathcal{C}_{532c} \cup \mathcal{C}_{532d}) \bigm| \\
&\qquad (6a_1+5)^3 + (6a_1+5)^2 + 2(6a_1+5) + 4 \neq a_0\bigr\} \\
\mathcal{C}_{533a} &:= \{G \in \mathcal{C}_{533} \mid a_0 - 3a_1 = -1\} \\
\mathcal{C}_{533b} &:= \{G \in \mathcal{C}_{533} \mid a_0 - 3a_1 = 6\} \\
\mathcal{C}_{533c} &:= \{G \in \mathcal{C}_{533} \mid a_0 - 3a_1 > 6 \ \&\ a_1 = 10\} \\
\mathcal{C}_{533d} &:= \{G \in \mathcal{C}_{533} \mid a_0 - 3a_1 > 6 \ \&\ a_1 = 11\,193\}.
\end{aligned}$$

Proposition 3.9. *The sets $\mathcal{C}_{536}$ and $\mathcal{C}_{538}$ are empty. For $G \in \mathcal{C}$,*

(2a) *$G \in \mathcal{C}_{532a}$ if and only if either $G = E_7(7)$ or $G = \mathrm{PSL}(8k,7)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 7$.
(2b) *$G \in \mathcal{C}_{532b}$ if and only if $G = \mathrm{PSL}(4k+1,9)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 3$.
(2c) *$G \in \mathcal{C}_{532c}$ if and only if $G = \mathrm{PSL}(16k+14,9)$ for some $k \geqslant 0$. In this case,* $\mathrm{ch}(G) = 3$.
(2d) *$G \in \mathcal{C}_{532d}$ if and only if $G = \mathrm{PSL}(16k+14,q)$ for some $k \geqslant 0$ and $q \in \{25,27,29,31\}$. In this case, let q_0 be the unique positive integer such that $a_1 = q_0^3 - 2q_0^2 + 4q_0 - 8$. Then $q = q_0$ and so* $\mathrm{ch}(G) = \mathrm{ch}(q_0)$.
(2e) *$G \in \mathcal{C}_{532e}$ if and only if $G = E_6(q)$ for some composite $q \equiv 2 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(6a_1+5)$.
(2f) *$G \in \mathcal{C}_{532f}$ if and only if $G = \mathrm{PSL}(4k+3,3^e)$ for some $k \geqslant 1$ and $e \geqslant 2$. In this case,* $\mathrm{ch}(G) = 3$.
(3a) *$G \in \mathcal{C}_{533a}$ if and only if either $G = G_2(3^e)$ or $G = \mathrm{PSL}(3,3^e)$ for some $e \geqslant 2$. In this case,* $\mathrm{ch}(G) = 3$.
(3b) *$G \in \mathcal{C}_{533b}$ if and only if $G = \mathrm{PSU}(3,q)$ for some composite $q \equiv 1 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0-2)$.
(3c) *$G \in \mathcal{C}_{533c}$ if and only if $G = \mathrm{PSL}(4k+1,7)$ for some $k \geqslant 2$. In this case,* $\mathrm{ch}(G) = 7$.
(3d) *$G \in \mathcal{C}_{533d}$ if and only if $G = \mathrm{PSL}(16k+14,23)$ for some $k \geqslant 0$. In this case,* $\mathrm{ch}(G) = 23$.
(4) *$G \in \mathcal{C}_{534}$ if and only if either $G = \mathrm{PSL}(8k,5)$ for some $k \geqslant 1$ or $G = \mathrm{P}\Omega^-(10,q)$ for some $q > 13$, $q \equiv 1 \pmod 3$. In this case, if $a_1 = 3$ then $\mathrm{ch}(G) = 5$ while if $a_1 > 3$ then* $\mathrm{ch}(G) = \mathrm{ch}(\lfloor \sqrt{a_0} \rfloor)$.
(5) *$G \in \mathcal{C}_{535}$ if and only if $G = \mathrm{PSL}(16k+14,19)$ for some $k \geqslant 0$. In this case,* $\mathrm{ch}(G) = 19$.

(7) *$G \in \mathcal{C}_{537}$ if and only if $G = E_6(q)$ for some composite $q \equiv 1 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(6a_1 + 7)$.

(9) *$G \in \mathcal{C}_{539}$ if and only if $G = \mathrm{PSL}(4k+3, q)$ for some $k \geqslant 1$ and $q > 13$, $q \equiv 1 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(3a_1 + 1)$.

(10) *$G \in \mathcal{C}_{5310}$ if and only if either $G = \mathrm{PSL}(4k+3, 13)$ for some $k \geqslant 1$ or $G = \mathrm{PSL}(16k+14, 17)$ for some $k \geqslant 0$. In this case, if $a_1 = 4$ then $\mathrm{ch}(G) = 13$ and if $a_1 = 4395$ then $\mathrm{ch}(G) = 17$.*

(11) *$G \in \mathcal{C}_{5311}$ if and only if $G = \mathrm{PSL}(16k+14, 7)$ for some $k \geqslant 0$. In this case, $\mathrm{ch}(G) = 7$.*

(12) *$G \in \mathcal{C}_{5312}$ if and only if $G = \mathrm{PSL}(16k+2, q)$ for some $k \geqslant 1$ and $q > 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_1 + 1)$.

In $\mathcal{C}_{54}$, we have to deal with three doubly infinite families where $a_2 \to \infty$ as $q \to \infty$. In addition to the groups $\mathrm{PSL}(16k+14, q)$ with $a_2 = \lfloor (q+1)/17 \rfloor$ for $q \geqslant 37$, the set $\mathcal{C}_{54}$ also contains $\mathrm{PSL}(4k+1, q)$ with $a_2 = \lfloor (q-3)/4 \rfloor$ for $q \geqslant 11$ and $k \geqslant 2$, and $\mathrm{PSL}(8k, q)$ with $a_2 = \lfloor (q+1)/5 \rfloor$ for $q \geqslant 9$ and $k \geqslant 1$.

Define

$$\mathcal{C}_{54x} := \{G \in \mathcal{C}_{54} \mid a_2 = x\} \quad \text{for } x \in \{2, 3, 4, 5, 8\}$$
$$\mathcal{C}_{549} := \bigl\{G \in \mathcal{C}_{54} \bigm| a_2 \in \{6, 7\} \text{ or } a_2 \geqslant 9\bigr\}.$$

For $x \in \{2, 3, 4, 9\}$ we partition $\mathcal{C}_{54x}$ further:

$$\mathcal{C}_{542a} := \bigl\{G \in \mathcal{C}_{542} \bigm| a_1 \in \{7, 9, 11, 14\}\bigr\}$$
$$\mathcal{C}_{542b} := \{G \in \mathcal{C}_{542} \mid a_1 = 16\}$$
$$\mathcal{C}_{542c} := \bigl\{G \in \mathcal{C}_{542} \bigm| a_1 \notin \{7, 9, 11, 14, 16\} \,\&\, a_1 \equiv 0 \pmod 2\bigr\}$$
$$\mathcal{C}_{542d} := \bigl\{G \in \mathcal{C}_{542} \bigm| a_1 \notin \{7, 9, 11, 14, 16\} \,\&\, a_1 \equiv 1 \pmod 2\bigr\}$$
$$\mathcal{C}_{543a} := \{G \in \mathcal{C}_{543} \mid a_0 - 3a_1 = 5\}$$
$$\mathcal{C}_{543b} := \{G \in \mathcal{C}_{543} \mid a_0 - 3a_1 = -2\}$$
$$\mathcal{C}_{543c} := \{G \in \mathcal{C}_{543} \mid a_0 - 3a_1 > 5 \,\&\, a_1 \leqslant 20\}$$
$$\mathcal{C}_{543d} := \{G \in \mathcal{C}_{543} \mid a_0 - 3a_1 > 5 \,\&\, a_1 > 20\}$$
$$\mathcal{C}_{544a} := \bigl\{G \in \mathcal{C}_{544} \bigm| a_1 \in \{17, 21\}\bigr\}$$
$$\mathcal{C}_{544b} := \{G \in \mathcal{C}_{544} \mid a_1 = 22\}$$
$$\mathcal{C}_{544c} := \bigl\{G \in \mathcal{C}_{544} \bigm| a_1 \notin \{17, 21\} \,\&\, a_1 \equiv 1 \pmod 2\bigr\}$$
$$\mathcal{C}_{544d} := \bigl\{G \in \mathcal{C}_{544} \bigm| a_1 \neq 22 \,\&\, a_1 \equiv 0 \pmod 2\bigr\}$$
$$\mathcal{C}_{549a} := \{G \in \mathcal{C}_{549} \mid a_1 > 5a_2 + 8\}$$
$$\mathcal{C}_{549b} := \bigl\{G \in \mathcal{C}_{549} \bigm| a_1 \leqslant 5a_2 + 8 \,\&\, a_1 \equiv 0 \pmod 2\bigr\}$$
$$\mathcal{C}_{549c} := \bigl\{G \in \mathcal{C}_{549} \bigm| a_1 \leqslant 5a_2 + 8 \,\&\, a_1 \equiv 1 \pmod 2\bigr\}.$$

Proposition 3.10. *For $G \in \mathcal{C}$,*

(2a) *$G \in \mathcal{C}_{542a}$ if and only if either $G = \mathrm{PSL}(8k, q)$ for some $k \geqslant 1$ and $q \in \{9, 11, 13\}$, or $G = E_7(11)$, or $G = \mathrm{PSL}(4k+1, 11)$ for some $k \geqslant 1$. In this case, if $a_1 = 14$ then $\mathrm{ch}(G) = 11$ and otherwise $\mathrm{ch}(G) = \mathrm{ch}(a_1 + 2)$.*

(2b) *$G \in \mathcal{C}_{542b}$ if and only if either $G = \mathrm{PSL}(4k+1, 13)$ for some $k \geqslant 1$ or $G = \mathrm{PSL}(16k+14, 3)$ for some $k \geqslant 0$. In this case, if $a_0 \equiv 0 \pmod 3$ then $\mathrm{ch}(G) = 3$ and if $a_0 \equiv 1 \pmod 3$ then $\mathrm{ch}(G) = 13$.*

(2c) *$G \in \mathcal{C}_{542c}$ if and only if $G = \mathrm{P}\Omega^-(10, 3^e)$ for some $e \geqslant 3$. In this case, $\mathrm{ch}(G) = 3$.*

(2d) *$G \in \mathcal{C}_{542d}$ if and only if $G = \mathrm{PSL}(16k+14, q)$ for some $k \geqslant 0$ and $q \in \{5, 37, 41, 43, 47, 49\}$. In this case, let q_0 be the smallest integer such that $a_1 \leqslant q_0^3 - 2q_0^2 + 4q_0 - 6$. Then $q_0 = q$ and so* $\mathrm{ch}(G) = \mathrm{ch}(q_0)$.

(3a) *$G \in \mathcal{C}_{543a}$ if and only if $G = \mathrm{PSU}(3, 3^e)$ for some $e \geqslant 3$. In this case,* $\mathrm{ch}(G) = 3$.

(3b) *$G \in \mathcal{C}_{543b}$ if and only if either $G = \mathrm{PSL}(3, q)$ for some $q \geqslant 11$, $q \equiv 2 \pmod 3$ or $G = G_2(q)$ for some composite $q \equiv 2 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 + 1)$.

(3c) *$G \in \mathcal{C}_{543c}$ if and only if $G = \mathrm{PSL}(8k, 17)$ for some $k \geqslant 1$ or $G = \mathrm{PSL}(4k+1, 17)$ for some $k \geqslant 1$. In this case,* $\mathrm{ch}(G) = 17$.

(3d) *$G \in \mathcal{C}_{543d}$ if and only if $G = \mathrm{PSL}(16k+14, q)$ for some $k \geqslant 0$ and $q \in \{11, 53, 59, 61\}$. In this case, let q_0 be the smallest integer such that $a_1 \leqslant q_0^3 - 2q_0^2 + 4q_0 - 6$. Then $q_0 = q$ and so* $\mathrm{ch}(G) = \mathrm{ch}(q_0)$.

(4a) *$G \in \mathcal{C}_{544a}$ if and only if either $G = \mathrm{PSL}(8k, q)$ for some $k \geqslant 1$ and $q \in \{19, 23\}$, or $G = E_7(q)$ for some $q \in \{19, 23\}$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_1 + 2)$.

(4b) *$G \in \mathcal{C}_{544b}$ if and only if $G = \mathrm{PSL}(4k+1, 19)$ for some $k \geqslant 2$. In this case,* $\mathrm{ch}(G) = 19$.

(4c) *$G \in \mathcal{C}_{544c}$ if and only if $G = \mathrm{PSL}(16k+14, q)$ for some $k \geqslant 0$ and $q \in \{67, 71, 73, 79, 81, 83\}$. In this case, let q_0 be the smallest integer such that $a_1 \leqslant q_0^3 - 2q_0^2 + 4q_0 - 6$. Then $q_0 = q$ and so* $\mathrm{ch}(G) = \mathrm{ch}(q_0)$.

(4d) *$G \in \mathcal{C}_{544d}$ if and only if $G = \mathrm{PSL}(4k+3, q)$ for some $k \geqslant 1$ and $q \geqslant 11$, $q \equiv 2 \pmod 3$. In this case,* $\mathrm{ch}(G) = \mathrm{ch}(3a_1 - 1)$.

(5) *$G \in \mathcal{C}_{545}$ if and only if G occurs on the following list*: $\mathrm{PSL}(5, q)$ *for $q \in \{27, 29\}$*; $\mathrm{PSL}(4k+1, q)$ *for some $k \geqslant 2$ and $q \in \{23, 25\}$*; $\mathrm{PSL}(8k, q)$ *for some $k \geqslant 1$ and $q \in \{25, 27\}$*; $E_7(27)$; $\mathrm{PSL}(16k+14, q)$ *for some $k \geqslant 0$ and $q \in \{89, 97\}$; and $E_6(3^e)$ for some $e \geqslant 3$.*
In this case, if $a_1 \in \{26, 28, 30, 32\}$ then $\mathrm{ch}(G) = \mathrm{ch}(a_1 - 3)$; *if $a_1 \in \{23, 25\}$ then* $\mathrm{ch}(G) = \mathrm{ch}(a_1 + 2)$; *if $a_1 = 689\,475$ then* $\mathrm{ch}(G) = 89$; *if $a_1 = 894\,235$ then* $\mathrm{ch}(G) = 97$; *for all other values of a_1,* $\mathrm{ch}(G) = 3$.

(8) *$G \in \mathcal{C}_{548}$ if and only if G occurs on the following list*: $\mathrm{PSL}(5, q)$ *for $q \in \{41, 43\}$*; $\mathrm{PSL}(4k+1, 37)$ *for some $k \geqslant 2$*; $\mathrm{PSL}(8k, q)$ *for some $k \geqslant 1$ and $q \in \{41, 43\}$*; $E_7(43)$; $\mathrm{PSL}(16k+14, q)$ *for some $k \geqslant 0$ and $q \in \{137, 139, 149, 151\}$; and $\mathrm{P}\Omega^-(10, q)$ for some $q \geqslant 11$, $q \equiv 2 \pmod 3$.*
In this case, if $a_1 \in \{40, 44, 46\}$ then $\mathrm{ch}(G) = \mathrm{ch}(a_1 - 3)$; *if $a_1 \in \{39, 41\}$ then* $\mathrm{ch}(G) = \mathrm{ch}(a_1 + 2)$; *if $a_1 = 2\,534\,355$ then* $\mathrm{ch}(G) = 137$; *if $a_1 = 2\,647\,525$ then* $\mathrm{ch}(G) = 139$; *if $a_1 = 3\,264\,135$ then* $\mathrm{ch}(G) = 149$; *if $a_1 = 3\,397\,945$ then* $\mathrm{ch}(G) = 151$; *for all other values of a_1,* $\mathrm{ch}(G) = \mathrm{ch}(3a_1 + 2)$.

(9a) *$G \in \mathcal{C}_{549a}$ if and only if $G = \mathrm{PSL}(16k+14, q)$ for some $k \geqslant 0$ and $q \in \{13\} \cup \{q \geqslant 101 \mid q \notin \{137, 139, 149, 151\}\}$. In this case, let q_0 be the smallest integer such that $a_1 \leqslant q_0^3 - 2q_0^2 + 4q_0 - 6$. Then $q_0 = q$ and so* $\mathrm{ch}(G) = \mathrm{ch}(q_0)$.

(9b) *$G \in \mathcal{C}_{549b}$ if and only if either $G = \mathrm{PSL}(5, q)$ for some $q \in \{31, 37\} \cup \{q \mid q \geqslant 47\}$ or $G = \mathrm{PSL}(4k+1, q)$ for some $k \geqslant 2$ and $q \in \{3\} \cup \{q \geqslant 27 \mid q \neq 37\}$. In this case, if $a_1 = 8$ then $\mathrm{ch}(G) = 3$ and for other values of a_1,* $\mathrm{ch}(G) = \mathrm{ch}(a_1 - 3)$.

(9c) *$G \in \mathcal{C}_{549c}$ if and only if either $G = \mathrm{PSL}(8k, q)$ for some $k \geqslant 1$ and $q \in \{29, 31, 37\} \cup \{q \mid q \geqslant 47\}$, or $G = E_7(q)$ for some $q \in \{31\} \cup \{q \geqslant 47 \mid q \equiv 3 \pmod 4\}$, or $G = \mathrm{PSL}(4k+1, 5)$ for some $k \geqslant 2$. In this case, if $a_1 = 9$ then $\mathrm{ch}(G) = 5$ and for other values of a_1,* $\mathrm{ch}(G) = \mathrm{ch}(a_1 + 2)$.

The preceding propositions complete the proof of Theorem 1.3.

4. Proof of Theorem 1.2

In the ambiguous cases appearing in Theorem 1.3(ii), (iii), the three largest element orders m_i are listed in Table 1. For special linear groups q is composite; in all other cases q is prime. For the unitary groups in Table 1, $a(n)$ denotes the smallest odd integer $a \geqslant 3$ satisfying $(a, n-a) = 1$; we use $a(n)$ only for values of n for which $a(n) < n/2$.

Proof of Theorem 1.2. Suppose first that $G \in \mathcal{C}_{5113}$ in Lemma 3.7, corresponding to the ambiguity in Theorem 1.3(ii). If $m_1/2 \geqslant m_3$ then $G = \mathrm{PSL}(2, q)$ and $\mathrm{ch}(G) = \mathrm{ch}(2m_1 - 1)$. On the other hand, if $m_1/2 < m_3$ then $G = G_2(q)$ and $\mathrm{ch}(G) = \mathrm{ch}(m_3)$.

If $G \in \mathcal{C}_{38}$ in Lemma 3.4, corresponding to the ambiguity in Theorem 1.3(iii), then define $a := \lfloor m_1/(m_1 - m_3) \rfloor$. By straightforward checking of Table 1, we find that $a < 2m_1/3$ if and only if G is symplectic and $q > 3$; in this case, $\mathrm{ch}(G) = \mathrm{ch}((m_1 - m_2)/2)$. Also, $a < 2m_1/3$ and $m_1 - m_2 = m_2 - m_3 = 6$ if and only if G is symplectic and $q = 3$. Finally, $a \geqslant 2m_1/3$ and $m_1 - m_2 = m_2 - m_3 = 6$

Table 1
Some m_1, m_2, m_3.

G	Restrictions	m_1	m_2	m_3
PSL(2, 9)		5	4	3
PSL$(2,q)$	$9 < q \equiv 1\ (4)$	$\frac{q+1}{2}$	$\frac{q-1}{2}$	$\frac{q-1}{4}$
PSL$(2,q)$	$q \equiv 3\ (4)$	$\frac{q+1}{2}$	$\frac{q-1}{2}$	$\frac{q+1}{4}$
$G_2(q)$		q^2+q+1	q^2+q	q^2
PSU$(2k+1,q)$	$k \in \{2,4\}$	$\frac{q^{2k}+q}{(q+1,2k+1)}$	$\frac{(q^{2k}-1)}{(q+1,2k+1)}$	$\frac{q^{2k+1}+1}{(q+1)(q+1,2k+1)}$
PSU$(2k+1,q)$	$k \notin \{2,4\}$	$\frac{q^{2k}+q}{(q+1,2k+1)}$	$\frac{q^{2k}-1}{(q+1,2k+1)}$	$\frac{(q^{a'}+1)(q^{2k+1-a'}-1)}{(q+1)(q+1,2k+1)}$ $a' := a(2k+1)$
PSU(4, 3)		12	9	8
PSU(6, 5)		630	624	521
PSU$(2k,q)$	$k > 3$ $q+1 \mid 2k$ $3 \nmid 2k+1$	$q^{2k-2}+q$	$q^{2k-2}-1$	$\frac{q(q^3+1)(q^{2k-5}+1)}{q+1}$
PSU$(2k,q)$	$k > 2$ $q+1 \mid 2k$ $3 \mid 2k+1$	$q^{2k-2}+q$	$q^{2k-2}-1$	$\frac{(q^3+1)(q^{2k-4}-1)}{q+1}$
PSU$(2k,q)$	$k \in \{2,3\}$ $q+1 \nmid 2k$	$\frac{q^{2k-1}+1}{(q+1,2k)}$	$\frac{q^{2k-1}-q}{(q+1,2k)}$	$\frac{q^{2k}-1}{(q+1)(q+1,2k)}$
PSU$(2k,q)$	$k \geqslant 4$ $q+1 \nmid 2k$	$\frac{q^{2k-1}+1}{(q+1,2k)}$	$\frac{q^{2k-1}-q}{(q+1,2k)}$	$\frac{(q^{a(2k)}+1)(q^{2k-a(2k)}+1)}{(q+1)(q+1,2k)}$
PSp$(2k,3)$	$k \geqslant 4$	3^k+9	3^k+3	3^k-3
PSp$(4k,q)$	$k \geqslant 2, q > 3$	$q^{2k}+q$	$q^{2k}-q$	$\frac{q(q+1)(q^{2k-2}+1)}{2}$
PSp$(4k+2,q)$	$k \geqslant 2, q > 3$	$q^{2k+1}+q$	$q^{2k+1}-q$	$\frac{(q+1)(q^{2k}+1)}{2}$

Table 2
Exceptions in the semisimple case.

G	Restrictions	m'_1	m'_2
P$\Omega^+(8,3)$		20	14
P$\Omega^-(10,3)$		80	65
P$\Omega^-(14,3)$		820	728
P$\Omega^-(2^e+2,3)$	$e \geqslant 4$	$3^{2^{e-1}}-1$	$(3^{2^{e-2}-1}-1)(3^{2^{e-2}+1}-1)$
P$\Omega^-(2^e3+2,3)$	$e \geqslant 3$	$(3^{2^e}+1)(3^{2^{e-1}}+1)$	$3^{3\cdot 2^{e-1}}-1$
PSU(4, 3)		8	7
PSU(6, 5)		624	521

do not both hold if and only if G is unitary. In this case, $a \in \{q, q+1\}$ and so $\mathrm{ch}(G) = \mathrm{ch}(a)$ if a is odd and $\mathrm{ch}(G) = \mathrm{ch}(a-1)$ if a is even. □

5. Proof of Theorem 1.4 and a variant

We first note the following

Theorem 5.1. *With the exceptions listed in Table* 2*, the formulae for m'_1, m'_2 coincide with the appropriate line for composite q in Tables* A.1–A.7 *in Appendix* A*.*

Proof. This is contained in the proof of Theorem 2.1: that proof started with the determination of the two largest semisimple element orders in each group. □

Proof of Theorem 1.4. The proof closely follows the one in Section 3. For reasons similar to the ones discussed in Remark 3.1, we exclude the following set of groups from the general argument:

$$\begin{aligned}\mathcal{S}_0' := \big\{&\mathrm{PSL}(5,11), \mathrm{PSU}(3,7), \mathrm{PSU}(6,5), \mathrm{PSU}(6,7), \mathrm{PSU}(8,3), \mathrm{PSU}(8,7),\\ &\mathrm{PSU}(16,3), \mathrm{PSU}(16,7), \mathrm{PSp}(10,3), \mathrm{PSp}(12,3), \mathrm{PSp}(14,3), \Omega(9,3), \Omega(11,3),\\ &\Omega(13,3), \Omega(15,3), \mathrm{P\Omega}^+(10,3), \mathrm{P\Omega}^+(14,3), \mathrm{P\Omega}^+(16,3), \mathrm{P\Omega}^+(16,5), \mathrm{P\Omega}^+(16,7),\\ &\mathrm{P\Omega}^+(16,13), \mathrm{P\Omega}^+(16,19), \mathrm{P\Omega}^+(16,31), \mathrm{P\Omega}^-(8,3), \mathrm{P\Omega}^-(26,7), \mathrm{P\Omega}^-(26,11),\\ &\mathrm{P\Omega}^-(26,19), E_6(7), E_6(11), E_6(13), E_6(17), E_6(19), G_2(3), G_2(5), G_2(7)\big\}.\end{aligned}$$

Since for any fixed bound B there are only finitely many groups G with $m_1'(G) < B$, we can check that Theorem 1.4 holds for the groups in the set $\mathcal{S}_0 \cup \mathcal{S}_0'$. Namely, if $G \in \mathcal{S}_0 \cup \mathcal{S}_0'$ and $\{m_1'(G), m_2'(G)\} \neq \{8,7\}$, then there is no simple group $H \ncong G$ of Lie type with $m_1'(G) = m_1'(H)$, $m_2'(G) = m_2'(H)$, and $\mathrm{ch}(G) \neq \mathrm{ch}(H)$.

Let $\mathcal{C}' := \mathcal{S} \setminus (\mathcal{S}_0 \cup \mathcal{S}_0')$. We partition $\mathcal{C}'$ into five classes $\mathcal{C}_i'$, $1 \leqslant i \leqslant 5$, as defined near the beginning of Section 3, however using the values m_1' and m_2' instead of m_1 and m_2. For example, $\mathcal{C}_1' = \{G \in \mathcal{C}' \mid m_1' - m_2' > (m_1', m_2')^2 > 1\}$. We also compute the numbers a_i, b_i, a_2', b_2' as in Eqs. (3.1) and (3.2), but using the continued fraction decompositions of $m_1'/(m_1' - m_2')$ instead of $m_1/(m_1 - m_2)$.

For $2 \leqslant i \leqslant 5$, we partition $\mathcal{C}_i'$ exactly into the subcategories described in Section 3 (but, of course, using m_1' and m_2' instead of m_1 and m_2 in the definitions). For $\mathcal{C}_1'$, the definition of $\mathcal{C}_{1j}'$ for $1 \leqslant j \leqslant 3$ and $6 \leqslant j \leqslant 11$ is the same as in Section 3. However, we define $\mathcal{C}_{14}'$ and $\mathcal{C}_{15}'$ as

$$\begin{aligned}\mathcal{C}_{14}' &:= \big\{G \in \mathcal{C}_1' \bigm| a_0 = 6 \,\&\, a_1 \geqslant 5 \,\&\, a_2 \leqslant 5\big\}\\ \mathcal{C}_{15}' &:= \big\{G \in \mathcal{C}_1' \bigm| a_1 = 1 \,\&\, b_1 - a_0 = 3\big\}.\end{aligned}$$

The observations made in Remark 3.1 are valid for the proofs of the following Propositions 5.2–5.6 as well.

Proposition 5.2. *Let $G \in \mathcal{C}'$.*

(1) *$G \in \mathcal{C}_{11}'$ if and only if $G = \mathrm{P\Omega}^-(2^e + 2, q)$ for some $e \geqslant 5$ and $q \equiv 3 \pmod 4$. In this case, if $a_1 > 2$ then $\mathrm{ch}(G) = \mathrm{ch}(2a_1 + 3)$. If $a_1 = 2$ and $a_0 = 401$ then $\mathrm{ch}(G) = 7$ and if $a_1 = 2$ and $a_0 \neq 401$ then $\mathrm{ch}(G) = 3$.*

(2) *$G \in \mathcal{C}_{12}'$ if and only if $G = \mathrm{PSp}(6,q)$ or $G = \Omega(7,q)$ for some q. In this case, $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.*

(3) *$G \in \mathcal{C}_{13}'$ if and only if either $G = G_2(q)$ for some $q \equiv 1 \pmod 3$ or $G = \mathrm{PSp}(8k+6,3)$, $\Omega(8k+7,3)$, $\mathrm{P\Omega}^+(8k+6,3)$ for some $k \geqslant 2$. In this case, if $a_0 > 6$ then $\mathrm{ch}(G) = \mathrm{ch}(a_0 + 1)$ and if $a_0 = 6$ then $\mathrm{ch}(G) = 3$.*

(4) *$G \in \mathcal{C}_{14}'$ if and only if $G = \mathrm{PSp}(8k+2,3)$, $\mathrm{PSp}(8k+4,3)$, $\Omega(8k+3,3)$, $\Omega(8k+5,3)$, or $\mathrm{P\Omega}^+(8k+2,3)$ for some $k \geqslant 2$. In this case, $\mathrm{ch}(G) = 3$.*

(5) *$G \in \mathcal{C}_{15}'$ if and only if $G = \mathrm{P\Omega}^-(2^e 3 + 2, 3)$ for some $e \geqslant 2$. In this case, $\mathrm{ch}(G) = 3$.*

(6) *$G \in \mathcal{C}_{16}'$ if and only if $G = \mathrm{P\Omega}^+(16, 3^e)$ for some $e \geqslant 2$. In this case, $\mathrm{ch}(G) = 3$.*

(7) *$G \in \mathcal{C}_{17}'$ if and only if $G = \mathrm{P\Omega}^+(16,q)$ for some $q \equiv 1 \pmod 3$. In this case, $\mathrm{ch}(G) = \mathrm{ch}(3b_1 + 1)$.*

(8) *$G \in \mathcal{C}_{18}'$ if and only if $G = \mathrm{P\Omega}^+(16,q)$ for some $q \equiv 2 \pmod 3$. In this case, $\mathrm{ch}(G) = \mathrm{ch}(3b_1 - 1)$.*

(9) *$G \in \mathcal{C}_{19}'$ if and only if $G = \mathrm{P\Omega}^-(18,q)$ for some $q \equiv 3 \pmod 4$. In this case, $\mathrm{ch}(G) = \mathrm{ch}(b_1 - 3)$.*

(10) *$G \in \mathcal{C}_{110}'$ if and only if $G = \mathrm{P\Omega}^-(14,q)$ for some $q > 3$, $q \equiv 3 \pmod 4$. In this case, $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.*

(11) *$G \in \mathcal{C}_{111}'$ if and only if G is on the following list: $\mathrm{PSp}(2k,q)$ or $\Omega(2k+1,q)$ with $k \geqslant 5$ and $q \geqslant 5$; $\mathrm{PSp}(8k,3)$, $\Omega(8k+1,3)$ with $k \geqslant 2$; $\mathrm{PSU}(d,q)$ with $d \geqslant 8$, $d \notin \{9,15\}$ for all q; $\mathrm{P\Omega}^+(4k,q)$ with $k \geqslant 3$,* except *$k = 4$; $\mathrm{P\Omega}^+(4k+2,q)$ with $k \geqslant 2$ and $q \geqslant 5$,* except *$\mathrm{P\Omega}^+(16k+2,q)$ with $k \geqslant 2$ and $q \equiv 1 \pmod 4$; $F_4(q)$ for all q; $E_8(q)$ with $q \equiv 0, 2 \pmod 3$; and all groups $\mathrm{P\Omega}^-(2k,q)$ with $k \geqslant 8$, with two*

families of exceptions: (i) $k \in \{2^e + 1 \mid e \geqslant 4\} \cup \{2^e 7 + 1 \mid e \geqslant 1\} \cup \{13\}$ *and* $q \equiv 3 \pmod 4$; *and* (ii) $\mathrm{P}\Omega^-(2^e 3 + 2, 3)$ *with* $e \geqslant 3$.
In this case, $a_0 = q^m + 2$ *or* $a_0 = q^m + 1$ *for some* $m \geqslant 1$ *and so* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 2)$ *if* a_0 *is odd and* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$ *if* a_0 *is even.*

Proposition 5.3. *Let* $G \in \mathcal{C}'$.

(1) $G \in \mathcal{C}'_{21}$ *if and only if* $G = \mathrm{PSU}(15, q)$ *for some* q. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$.
(2) $\mathcal{C}'_{22}$ *and* $\mathcal{C}'_{26}$ *are empty.*
(3) $G \in \mathcal{C}'_{23}$ *if and only if* $G = {}^2E_6(q)$ *for some* q. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(4) $G \in \mathcal{C}'_{24}$ *if and only if either* $G = \mathrm{PSU}(7, q)$ *for some* q *or* $G = E_8(q)$ *for some* $q \equiv 1 \pmod 3$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$.
(5) $G \in \mathcal{C}'_{25}$ *if and only if either* $G = \mathrm{P}\Omega^-(2k, q)$ *for some* $k \in \{7 \cdot 2^e + 1 \mid e \geqslant 1\}$ *and* $q \equiv 3 \pmod 4$ *or* $k = 13$ *and* $q > 19$, $q \equiv 3 \pmod 4$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 2)$.

Proposition 5.4. *Let* $G \in \mathcal{C}'$.

(1) $G \in \mathcal{C}'_{31}$ *if and only if* $G = \mathrm{P}\Omega^+(8, q)$ *for some* q. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(4m_1 + 1)$.
(2) *For* $2 \leqslant i \leqslant 8$, *the sets* $\mathcal{C}'_{3i}$ *are empty.*

Proposition 5.5. *For* $G \in \mathcal{C}'$,

(1) $G \in \mathcal{C}'_{41}$ *if and only if* $G = \mathrm{PSL}(6, q)$ *for some* q. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 + 1)$.
(2) $G \in \mathcal{C}'_{42}$ *if and only if* $G = \mathrm{PSU}(6, q)$ *for some* q *or* $G = \mathrm{P}\Omega^+(16k + 2, 5)$ *for some* $k \geqslant 2$. *In this case, if* $a_0 > 7$ *then* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$ *and if* $a_0 = 7$ *then* $\mathrm{ch}(G) = 5$.
(3) $G \in \mathcal{C}'_{43}$ *if and only if* $G = \mathrm{P}\Omega^+(16k + 2, q)$ *for some* $k \geqslant 2$ *and* $q > 5$, $q \equiv 1 \pmod 4$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 2)$.
(4) $G \in \mathcal{C}'_{44}$ *if and only if* $G = {}^3D_4(q)$ *for some* q *or* $G = E_7(q)$ *for some* $q \equiv 1 \pmod 4$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0)$.
(5) $\mathcal{C}'_{45}$ *is empty.*
(6) $G \in \mathcal{C}'_{46}$ *if and only if* G *is on the following list*: $\mathrm{PSU}(d, q)$ *for some* $d \in \{5, 9\}$ *and all* q; $\mathrm{PSp}(8, q)$ *for all* q; $\Omega(9, q)$ *for all* q; $\mathrm{P}\Omega^-(2k, q)$ *for some* $k \in \{4, 6\}$ *and all* q; $\mathrm{P}\Omega^-(14, q)$ *for some* $q \equiv 1 \pmod 4$. *In this case,* $\mathrm{ch}(G) = \mathrm{ch}(a_0 - 1)$.

Proposition 5.6. *For all classes* $\mathcal{C}_{5ij\ldots}$ *considered in Propositions* 3.6, 3.8–3.10, $\mathcal{C}'_{5ij\ldots} \supseteq \mathcal{C}_{5ij\ldots} \setminus \mathcal{S}'_0$ *with one exception*:

(1) $\mathcal{C}_{511} \setminus \mathcal{C}'_{511} = \{G_2(q) \mid q \text{ prime}\}$.

Moreover, for the classes different from $\mathcal{C}'_{511}$, *the stronger condition* $\mathcal{C}'_{5ij\ldots} = \mathcal{C}_{5ij\ldots} \setminus \mathcal{S}'_0$ *holds with the following exceptions*:

(2) $\mathcal{C}'_{511} \setminus \mathcal{C}_{511} = \{\mathrm{PSL}(2, q) \mid q \text{ prime}\} \cup \{\mathrm{PSp}(4, q) \mid q \text{ prime}\}$,
(3) $\mathcal{C}'_{512} \setminus \mathcal{C}_{512} = \{\mathrm{PSU}(3, q) \mid q \equiv 2 \pmod 3 \text{ prime}\}$,
(4) $\mathcal{C}'_{521} \setminus \mathcal{C}_{521} = \{\mathrm{PSU}(4, q) \mid q \text{ prime}\}$,
(5) $\mathcal{C}'_{532e} \setminus \mathcal{C}_{532e} = \{E_6(q) \mid q \equiv 2 \pmod 3 \text{ prime}\}$,
(6) $\mathcal{C}'_{533b} \setminus \mathcal{C}_{533b} = \{\mathrm{PSU}(3, q) \mid q \equiv 1 \pmod 3 \text{ prime}\}$,
(7) $\mathcal{C}'_{537} \setminus \mathcal{C}_{537} = \{E_6(q) \mid q \equiv 1 \pmod 3 \text{ prime}\}$, *and*
(8) $\mathcal{C}'_{543b} \setminus \mathcal{C}_{543b} = \{G_2(q) \mid q \equiv 2 \pmod 3 \text{ prime}\}$.

In each of the cases (2)–(8), *the groups in* $\mathcal{C}'_{5ij\ldots} \setminus \mathcal{C}_{5ij\ldots}$ *are of the form* $X(q)$ *for a type* X *and prime* q *so that* $X(\bar{q})$ *with composite* $\bar{q}$ *is in* $\mathcal{C}_{5ij\ldots}$. *Moreover, the formulae given in Propositions* 3.6, 3.8–3.10, *for computing* $\mathrm{ch}(X(\bar{q}))$ *in* $\mathcal{C}_{5ij\ldots}$, *are also valid for prime* q.

Hence, for $G \in \mathcal{C}'_5$, $m'_1(G)$ *and* $m'_2(G)$ *determine* $\mathrm{ch}(G)$ *as described in Propositions* 3.6, 3.8–3.10.

These propositions finish the proof of Theorem 1.4. Note that, for the potential counterexamples in Theorem 1.3(ii), (iii), we have $\{m_1(G), m_2(G)\} \neq \{m'_1(G), m'_2(G)\}$, so these potential counterexamples do not arise. □

In our algorithmic application Theorem 1.5, we need a variant of Theorems 1.3 and 1.4. For, when $\{m_1(G), m_2(G)\} \neq \{m'_1(G), m'_2(G)\}$, elements of order $m'_1(G)$, $m'_2(G)$ are more frequent in G than elements of order $m_1(G)$, $m_2(G)$ [Lü]. Hence, in a computation of the characteristic based on large element orders, it is preferable to use Theorem 1.4 instead of Theorem 1.3 because a smaller sample of random element orders already contains $m'_1(G)$ and $m'_2(G)$. We will take a large enough sample of group element orders so that the quantities m'_1, m'_2 occur with high probability. Unfortunately, this does not imply that the two largest element orders we encounter are indeed m'_1 and m'_2. If our sample contains m'_1 and m'_2 then the two largest orders $m^*_1 > m^*_2$ in the sample behave as in the following definition:

Definition 5.7. Let G be a simple group of Lie type. Define $m^*_1(G) > m^*_2(G)$ to be *any* two element orders for G such that

$$m^*_2(G) \geqslant m'_2(G), \quad \text{and}$$

$$\text{if}\, m^*_2(G) < m'_1(G) \quad \text{then}\, m^*_1(G) = m'_1(G).$$

For example, if $m_i(G)$ denotes the ith largest element order in G and $m'_1(G) = m_3(G)$ and $m'_2(G) = m_5(G)$, then the possible pairs (m^*_1, m^*_2) are (m_1, m_2), (m_1, m_3), (m_2, m_3), (m_3, m_4), and (m_3, m_5).

Using the methods of Section 2, we obtained formulae for all possible pairs $(m^*_1(G), m^*_2(G))$ for all Lie-type groups G except $\mathrm{PSp}(d, 2^e)$, $\mathrm{P}\Omega^+(d, 2^e)$, and $\mathrm{P}\Omega^-(d, 2^e)$ with $d > 36$. For groups defined over prime fields, there can be many possible pairs.

Fact 5.8. *Let $\mathcal{F}^*$ be the family of simple groups G of Lie type of rank at most* 66 *and defined over a field of size at most* 10^5, except exclude $\mathrm{P}\Omega^+(d, 2^e)$, $\mathrm{P}\Omega^-(d, 2^e)$, $\mathrm{PSp}(d, 2^e)$ *for $d > 36$; also let $\mathcal{F}^*$ contain the groups* $\mathrm{PSL}(2, q)$, ${}^2B_2(q)$, *and* ${}^2G_2(q)$ *for $q < 10^{10}$.*

If $G, H \in \mathcal{F}^*$ have different defining characteristics but $m^*_1(G) = m^*_1(H)$ and $m^*_2(G) = m^*_2(H)$ for some values m^*_1, m^*_2 for these groups, then the pair $\{G, H\}$ occurs in Table 3 *or* $\{G, H\} = \{\mathrm{PSL}(2, 2p^2 + 2p + 1), G_2(p)\}$ *for some prime p.*

There are 1017 primes $p < 10^5$ for which $2p^2 + 2p + 1$ is a prime; also $2p^2 + 2p + 1$ is a proper prime power just once in this range, for $p = 3$ (compare Theorem 1.3(ii)).

Proof sketch for Fact 5.8. Just as for Fact 1.1, we verified Fact 5.8 by computer calculations. We programmed the formulae for $(m^*_1(G), m^*_2(G))$ mentioned above and evaluated them in the indicated range *with the exception of the groups* $\mathrm{PSL}(2, q)$ *for prime* $q > 10^5$. Then we collected the pairs $\{G, H\}$ with $m^*_1(G) = m^*_1(H)$ and $m^*_2(G) = m^*_2(H)$, and discarded those with $\mathrm{ch}(G) = \mathrm{ch}(H)$.

To finish the proof, we have to show that, if $m^*_1 := m^*_1(G)$, $m^*_2 := m^*_2(G)$ for $G = \mathrm{PSL}(2, q)$ with prime $q > 10^5$, then the only way to have $m^*_1 = m^*_1(H)$, $m^*_2 = m^*_2(H)$ for some group H of characteristic different from q is when $H = G_2(p)$ for a prime p satisfying $q = 2p^2 + 2p + 1$. There are two possibilities: $(m^*_1, m^*_2) = (q, (q + 1)/2)$ or $(m^*_1, m^*_2) = ((q + 1)/2, (q - 1)/2)$.

First, suppose that $(m^*_1, m^*_2) = (q, (q+1)/2)$. If a simple group H satisfies $m_1(H) < 2m'_2(H) - 1$ then $m^*_1(H) < 2m^*_2(H) - 1$ for all possible pairs $(m^*_1(H), m^*_2(H))$ and so $(m^*_1(H), m^*_2(H)) \neq (q, (q + 1)/2)$. Hence it is enough to consider groups H with $m_1(H) \geqslant 2m'_2(H) - 1$. The groups satisfying this condition are $\mathrm{PSL}(2, r)$, $\mathrm{PSp}(4, r)$, $\mathrm{PSp}(6, r)$, $\mathrm{PSp}(8, r)$ for prime r, $\mathrm{P}\Omega^+(8, r)$ for $r \geqslant 4$, and a few small examples: $\mathrm{PSL}(4, 2)$, $\mathrm{PSL}(6, 2)$, $\mathrm{PSU}(3, 3) \cong G_2(2)'$, $\mathrm{PSU}(4, 2)$, ${}^2B_2(8)$, ${}^2F_4(2)'$, ${}^3D_4(2)$. It is easy to see that in the symplectic and orthogonal families $m^*_1(H) = 2m^*_2(H) - 1$ is impossible. Some of the small examples lead to lines in Table 3, but of course only involving $\mathrm{PSL}(2, q)$ with $q < 10^5$.

Table 3
Exceptional pairs.

m_1^*	m_2^*	Groups
5	3	$\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5)$, $\mathrm{PSL}(2,9) \cong \mathrm{PSp}(4,2)'$
5	4	$\mathrm{PSL}(2,9) \cong \mathrm{PSp}(4,2)'$, $\mathrm{PSp}(4,3) \cong \mathrm{PSU}(4,2)$
6	5	$\mathrm{PSL}(2,11)$, $\mathrm{PSp}(4,3) \cong \mathrm{PSU}(4,2)$
7	3	${}^2G_2(3)' \cong \mathrm{PSL}(2,8)$, $G_2(2)' \cong \mathrm{PSU}(3,3)$
7	4	$G_2(2)' \cong \mathrm{PSU}(3,3)$, $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$
7	6	$G_2(2)' \cong \mathrm{PSU}(3,3)$, $\mathrm{PSL}(2,13)$
8	7	$G_2(2)' \cong \mathrm{PSU}(3,3)$, $\mathrm{PSU}(3,5)$, $\mathrm{PSU}(4,3)$
9	8	$\mathrm{PSL}(2,17)$, $\mathrm{PSU}(4,3)$
12	9	$\mathrm{PSp}(4,3) \cong \mathrm{PSU}(4,2)$, $\mathrm{PSU}(4,3)$
13	7	${}^2B_2(8)$, $\mathrm{PSL}(2,13)$
13	8	$G_2(3)$, ${}^2F_4(2)'$
13	12	$G_2(3)$, $\mathrm{PSL}(2,25)$, ${}^2F_4(2)'$
15	13	$\mathrm{PSp}(4,5)$, $\mathrm{PSU}(3,4)$
20	13	$\mathrm{PSL}(4,3)$, $\mathrm{PSp}(4,5)$
20	15	$\mathrm{P\Omega}^+(8,3)$, $\mathrm{PSp}(4,5)$, $\mathrm{PSp}(6,3)$
21	20	$\mathrm{PSL}(2,41)$, $\mathrm{PSp}(8,2)$, $F_4(2)$
30	20	$\mathrm{PSp}(4,5)$, $\mathrm{PSp}(6,3)$
30	24	$\mathrm{PSp}(6,3)$, $\mathrm{PSp}(8,2)$, $F_4(2)$
63	60	$\mathrm{PSU}(4,5)$, $\mathrm{PSU}(7,2)$
91	85	$\mathrm{PSL}(3,16)$, $\mathrm{PSp}(4,13)$

If $(m_1^*, m_2^*) = ((q+1)/2, (q-1)/2)$ then at least one of $m_1^*(H)$, $m_2^*(H)$ arises from a semisimple element and, by Definition 5.7, we must have $m_1'(H) \in \{m_1^*, m_2^*\}$. All groups H with $m_1'(H) < 5 \cdot 10^9$ are included in $\mathcal{F}^*$, with the exception of $\mathrm{PSp}(d, 2^e)$, $\mathrm{P\Omega}^+(d, 2^e)$, and $\mathrm{P\Omega}^-(d, 2^e)$ with $d > 36$. For groups H in $\mathcal{F}^*$ with $m_1'(H) < 5 \cdot 10^9$, we checked whether pairs $\{m_1'(H), m_1'(H) \pm 1\}$ occur among our formulae for m_i^*, and for all such pairs we computed whether they are of the form $\{(q+1)/2, (q-1)/2\}$ for some prime q. There are such pairs, listed in Table 3, and also for larger q in the case of the groups $H = G_2(p)$ with $q = 2p^2 + 2p + 1$.

The last remaining case is $\{m_1^*, m_2^*\} = \{(q+1)/2, (q-1)/2\} = \{m_1'(H),\ m_1'(H) \pm 1\}$ for some orthogonal or symplectic group H defined over $\mathrm{GF}(2^e)$ and of rank greater than 18. If $2^e > 2$ then the only possibility is $m_1^*(H) = m_1'(H)$ and $m_2^*(H) = m_2'(H)$; both of these numbers are odd, so $m_1^*(H) - m_2^*(H) = 1$ is impossible. If $2^e = 2$ and H has rank $m \geqslant 33$ then $m_1'(H) > 2^m > 5 \cdot 10^9$ and it cannot be equal to $(q \pm 1)/2$ for $q < 10^{10}$. Hence only the cases $\mathrm{PSp}(d,2)$, $\mathrm{P\Omega}^+(d,2)$, and $\mathrm{P\Omega}^-(d,2)$ remain, with $38 \leqslant d \leqslant 64$. For these groups H, we determined $m_1'(H)$ and then proved the impossibility of the pair $\{m_1^*, m_2^*\} = \{m_1'(H), m_1'(H) \pm 1\}$ using the following simple observation: in most cases, the two numbers $m_1'(H) \pm 1$ do not divide the order of H so they cannot be element orders in H. The only cases not eliminated by this trivial requirement are also easily handled as follows:

(1) $H = \mathrm{PSp}(44,2)$ or $\mathrm{P\Omega}^-(44,2)$, $m_1'(H) - 1 = 2^8(2^7 - 1)(2^8 + 1)$. In the natural representation, for an element g of this order, g^{2^8} must have invariant subspaces of dimension 14 and 16 and a fixed point space of dimension 14. However, $\mathrm{PSp}(14,2)$ has no element of order 2^8, a contradiction.

(2) $H = \mathrm{PSp}(52,2)$ or $\mathrm{P\Omega}^+(52,2)$, $m_1'(H) - 1 = 2^{11}(2^5 - 1) \cdot 2113$. Here 2113 is a $\mathrm{ppd}^{\#}(2;44)$-number, so an element of this order must have invariant subspaces of dimension 10 and 44. Since $10 + 44$ is greater than the dimension of H, we obtain a contradiction.

(3) $H = \mathrm{PSp}(56,2)$ or $\mathrm{P\Omega}^+(56,2)$, $m_1'(H) - 1 = 2^{13}(2^3 - 1) \cdot 11 \cdot 23 \cdot 37$. Here 23 is $\mathrm{ppd}^{\#}(2;11)$ and 37 is $\mathrm{ppd}^{\#}(2;36)$, $22 + 36 > \dim(H)$, a contradiction.

(4) $H = \mathrm{PSp}(62,2)$ or $\mathrm{P\Omega}^-(62,2)$, $m_1'(H) + 1 = 2^{32}$. This is not an element order in $\mathrm{PSp}(62,2)$.

(5) $H = \mathrm{PSp}(62,2)$, $m_1'(H) - 1 = 2(2^{31} - 1)$. For an element g of this order, g^2 must act irreducibly in 62 dimensions and also have fixed points, a contradiction. □

Fact 5.8 suggests the following conjecture.

Conjecture 5.9. *For any two simple groups G, H of Lie type, if $m_1^*(G) = m_1^*(H)$ and $m_2^*(G) = m_2^*(H)$ for some m_1^*, m_2^* as in Definition* 5.7*, then either* $\mathrm{ch}(G) = \mathrm{ch}(H)$*, or* $\{G, H\}$ *occurs in Table* 3*, or* $\{G, H\} = \{G_2(p), \mathrm{PSL}(2, r)\}$ *for some primes p, r satisfying $r = 2p^2 + 2p + 1$.*

It is conceivable that, for the family of groups G of odd characteristic, Conjecture 5.9 could be proved by the method of Theorem 1.3, since we have the list of possible pairs $(m_1^*(G), m_2^*(G))$. However, there are many more cases to consider than in Theorem 1.3, and the modifications required for the proof are not as straightforward as in the case of Theorem 1.4.

6. The algorithmic application

Given an absolutely irreducible $K \leqslant \mathrm{GL}(d, p^e)$ such that K modulo scalars is isomorphic to a simple group G of Lie type, we describe a Monte Carlo algorithm that *returns a list of at most* 6d *numbers including* $\mathrm{ch}(G)$. We shall prove that, with high probability, the output is correct; and that if $d \leqslant 324\,485$ then the list contains only one number. If Conjecture 5.9 is true then the output list contains only one number for all input dimensions.

We need the following number-theoretic definition and elementary lemma.

Definition 6.1. Let p_i denote the ith prime number. For a positive integer n, let $\sigma(n)$ denote the number of different prime divisors of n, let $k(n)$ be the minimum k such that $\prod_{i=1}^{k} p_i \geqslant n$, and let

$$\alpha(n) := \prod_{i=1}^{k(n)} \left(1 - \frac{1}{p_i}\right).$$

Lemma 6.2. *Let $n, m > 1$ be integers.*

(a) *If $m < n$, then the cyclic group $\mathbb{Z}_m$ contains at least $\alpha(n)m$ elements of order m.*
(b) *If $m \geqslant n$ then for any fixed prime divisor p of m, $\mathbb{Z}_m$ contains at least $\alpha(n)m$ elements of order at least n and of order divisible by p.*

Proof. Let $q_1, \ldots, q_{\sigma(m)}$ be the distinct prime divisors of m, in increasing order. Clearly, $q_i \geqslant p_i$ for all i.

First, we consider the case $\sigma(m) \leqslant k(n)$. In this case, the Euler-function is

$$\varphi(m) = m \prod_{i=1}^{\sigma(m)} \left(1 - \frac{1}{q_i}\right) \geqslant m \prod_{i=1}^{\sigma(m)} \left(1 - \frac{1}{p_i}\right) \geqslant m \prod_{i=1}^{k(n)} \left(1 - \frac{1}{p_i}\right) = m\alpha(n). \tag{6.1}$$

(a) If $m < n$ then, by the definition of $k(n)$, $\prod_{i=1}^{k(n)} p_i \geqslant n > m \geqslant \prod_{i=1}^{\sigma(m)} q_i \geqslant \prod_{i=1}^{\sigma(m)} p_i$, so $k(n) > \sigma(m)$. Hence, by (6.1), $\varphi(m) \geqslant m\alpha(n)$. Since there are $\varphi(m)$ elements in $\mathbb{Z}_m$ of order m, our claim follows.

(b) As in part (a), if $\sigma(m) \leqslant k(n)$ then there are $\varphi(m) \geqslant m\alpha(n)$ elements in $\mathbb{Z}_m$ of order m. Each of these elements has order at least n and divisible by p, so our claim is proven.

The only remaining case is that $m \geqslant n$ and $\sigma(m) > k(n)$. In this case, let Q be any set of $k(n)$ different prime divisors of m, including p, and let $r = \prod_{q \in Q} q$. Note that $r \geqslant \prod_{i=1}^{k(n)} p_i \geqslant n$. Now there are

$$m \prod_{q \in Q} \left(1 - \frac{1}{q}\right) \geqslant m \prod_{i=1}^{k(n)} \left(1 - \frac{1}{p_i}\right) = m\alpha(n)$$

elements of $\mathbb{Z}_m$ of order divisible by r, finishing the proof of the lemma. □

Proposition 6.3. *Let N be a positive integer and suppose that the set $\mathcal{P}(N)$ of primes less than N is known. Then there is a Las Vegas algorithm that, given any $g \in \mathrm{GL}(d,q)$, determines whether the order $|g|$ of g and the projective order $\|g\|$ of g are less than N. Moreover, if $|g| < N$ or $\|g\| < N$ then the algorithm computes $|g|$ and $\|g\|$, respectively.*

The running time of the algorithm is $O(\mu[d^3(\log d + \log N + \log q) + (N^2 + N\log q)d\log d\log\log d])$, where μ is the cost of a field operation in $\mathrm{GF}(q)$.

Proof. We use ideas from [LGO, Section 10]. We compute the Frobenius normal form and the minimal polynomial $h(x)$ of g by the Las Vegas algorithm of [Gi], in $O(\mu d^3 \log d)$ time. The rest of the procedure is deterministic.

First consider the computation of $|g|$. For primes $p \in \mathcal{P}(N)$, let $\mathbf{p}(p)$ denote the largest power of p that is less than N, and let $\mathbf{P} := \prod_{p\in\mathcal{P}(N)} \mathbf{p}(p)$. We compute the remainder $r(x)$ of the polynomial division of $x^{\mathbf{P}}$ by $h(x)$. By the definition of the minimal polynomial, $g^{\mathbf{P}} = 1$ if and only if $r(x) = 1$.

If $r(x) \neq 1$ then we conclude that $|g| \geqslant N$, because $|g|$ either has a prime divisor not less than N, or $|g|$ is divisible by a power p^f of some prime $p < N$ satisfying $p^f \geqslant N$. If $r(x) = 1$ then, for all primes $p \in \mathcal{P}(N)$, we compute the remainder $r_p(x)$ of the division $x^{\mathbf{P}/\mathbf{p}(p)}$ by $h(x)$. For any prime $p \in \mathcal{P}(N)$, p divides $|g|$ if and only if $r_p(x) \neq 1$.

If $r_p(x) \neq 1$ for at least $\log N$ primes p then $|g| \geqslant N$. Otherwise, for each prime p with $r_p(x) \neq 1$, we compute the p-part of $|g|$ by recursively computing the remainders of $(r_p(x))^p$, $(r_p(x))^{p^2}, \ldots$ mod $h(x)$, until we reach an exponent p^f such that $(r_p(x))^{p^f} = 1$ modulo $h(x)$.

Next, we indicate the modifications necessary to compute $\|g\|$. The projective order of g divides $\mathbf{P}$ if and only if $r(g)$, the evaluation of $r(x)$ at g, is a scalar matrix. Hence we compute $r(g)$, and if it is not a scalar matrix then $\|g\| \geqslant N$.

Similarly, we could follow the steps of the algorithm for $|g|$ and substitute the checks of whether $r_p(x)^{p^i} = 1$ for some $i \geqslant 0$ by checking whether $r_p(g)^{p^i}$ is a scalar matrix. Instead, we speed up the algorithm as follows.

If $r(g)$ is a scalar matrix then we write $q-1$ in the form $q-1 = q_1q_2$, where all prime divisors of q_1 are less than N and all prime divisors of q_2 are at least N. (This decomposition of $q-1$ can be computed by dividing $q-1$ by primes $p \in \mathcal{P}(N)$ as long as possible.) Then, for $p \in \mathcal{P}(N)$, we define $\mathbf{q}(p)$ as the product of $\mathbf{p}(p)$ and the p-part of q_1, and define $\mathbf{Q} := \prod_{p\in\mathcal{P}(N)} \mathbf{q}(p)$. Note that $\mathbf{q}(p) \neq \mathbf{p}(p)$ can occur for at most $\log q$ primes.

For $p \in \mathcal{P}(N)$, we compute the remainder $s_p(x)$ of the division $x^{\mathbf{Q}/\mathbf{q}(p)}$ by $h(x)$. If there are at least $\log N + \log q$ primes p with $s_p(x) \neq 1$, then $\|g\| \geqslant N$, since at least $\log N$ of these primes must divide $\|g\|$. If there are fewer than $\log N + \log q$ primes p with $s_p(x) \neq 1$, then for these primes we recursively compute the remainders of $(s_p(x))^p$, $(s_p(x))^{p^2}, \ldots$ mod $h(x)$, until we reach an exponent p^f such that $(s_p(x))^{p^f}$, evaluated at g, is a scalar matrix. This power p^f is the p-part of $\|g\|$.

Finally, we estimate the time requirement of the algorithm. The polynomial $h(x)$ is of degree at most d. Hence, for any n, the remainder of the division of x^n by $h(x)$ can be computed by $O(\log n)$ multiplications and divisions of polynomials of degree less than $2d$, by repeated squaring and computing the remainder of x^{2^i} for $i \leqslant \lceil \log n \rceil$. The cost of division and multiplication of polynomials of degree at most $2d$ is $O(\mu d \log d \log\log d)$ [vzG, Sections 8.3, 9.1]. Thus, since $\mathbf{P} < N^N$ and $\mathbf{Q} < N^N q$, the polynomials $r(x), r_p(x), s_p(x)$ can be computed at a cost of $O(\mu(N\log N + \log q)d\log d\log\log d)$ each. Also, since $|\mathcal{P}(N)| = O(N/\log N)$, the total cost of the computation of $r(x), r_p(x), s_p(x)$ is $O(\mu(N^2 + N\log q)d\log d\log\log d)$.

The computations of $(r_p(x))^{p^i}$ and $(s_p(x))^{p^i}$ are performed for a *total* of at most $\log N + \log q$ values of the pair (p,i), because every time such a computation is performed, we add a factor p either to $\|g\|$ or to the part of $|g|$ occurring in q_1. As soon as the product of primes included in $\|g\|$ reaches N, we can stop the computation. Similarly, the evaluations $(r_p(g))^{p^i}$ and $(s_p(g))^{p^i}$ are performed for at most $\log N + \log q$ pairs (p,i). Each evaluation requires $O(d)$ matrix multiplications but, performing the multiplications with the sparse matrix Frobenius form of g, the cost of each multiplication is only $O(\mu d^2)$. Hence the total cost of the evaluations of $(r_p(g))^{p^i}$ and $(s_p(g))^{p^i}$ is $O(\mu(\log N + \log q)d^3)$. □

Remark 6.4. An algorithm for computing the order and projective order of a matrix is described in [CLG]. The claimed running time is similar to the timing of Proposition 6.3; however, the timing analysis of the "Bounded order algorithm" on page 55 of [CLG] should involve an extra factor d. Hence, using [CLG] would increase the timing of Proposition 6.3 by a factor N and hence the timing of Theorem 1.5 by a factor d, increases that we prefer to avoid. Therefore, it seems that the more delicate procedure and analysis of Proposition 6.3 are necessary for our results.

Let $\mathcal{L}$ denote the set of formulae for possible triples $(H, m_1^*(H), m_2^*(H))$ for the following groups H: all special linear, unitary, and exceptional groups; all symplectic and orthogonal groups in odd characteristic; and all symplectic and orthogonal groups of characteristic 2 and rank at most 18 (see Definition 5.7 and the two paragraphs following that definition). Recall that $\|g\|$ denotes the projective order of a matrix g, and that K is an absolutely irreducible matrix group such that K modulo scalars is isomorphic to a simple group G of Lie type.

Algorithm FIND_CHAR.
Input: $K \leqslant \mathrm{GL}(d, p^e)$, $\mathcal{L}$ as above and an error bound $\varepsilon > 0$.
Output: A list of possibilities for $\mathrm{ch}(G)$.

```
(1)  $L := \emptyset$, **output** $:= \emptyset$
     /* in $L$ we collect random element orders and in **output** we collect possibilities for $\mathrm{ch}(G)$ or for
     the pair $(\mathrm{ch}(G), G)$ */
(2)  repeat up to $\lceil 32\log^2(3d)\log(2/\varepsilon)/\alpha(3d)\rceil$ times
     $g :=$ (pseudo)random element of $K$
     if $\|g\| \geqslant 3d$ then return **output** $:= \{p\}$
     else place $\|g\|$ in $L$
(3)  $m_1^*, m_2^*, m_3^* :=$ three largest elements in $L$
(4)  use $\mathcal{L}$ to determine all $H$ with $m_1^* = m_1^*(H)$, $m_2^* = m_2^*(H)$ and place the pair $(\mathrm{ch}(H), H)$ in **output**
(5)  if $d \geqslant 324\,485$ then place the number 2 in **output**
(6)  /* handle ambiguous cases */
(6a) if **output** contains $(q, \mathrm{PSL}(2, q))$ and $(p, G_2(p))$ with $q = 2p^2 + 2p + 1$ then $m_3^* :=$ third largest
     element of $L$
     if $m_3^* \geqslant p^2 - 1$ then delete $(q, \mathrm{PSL}(2, q))$ from **output**
     else delete $(p, G_2(p))$ from **output**
(6b) if $(m_1^*, m_2^*) \in \{(5,3), (5,4), (7,4), (15,13), (30,20), (30,24), (63,60), (91,85)\}$ then choose the
     unique group $G$ from Table 3 with $m_1^* = m_1(G)$ and $m_2^* = m_2(G)$
(6c) if $(m_1^*, m_2^*) \in \{(12,9), (13,7), (13,12)\}$ then use $m_3^*$ to choose one of the groups described in
     Fact 1.1
(7)  return the numbers for $\mathrm{ch}(G)$ collected in **output**
```

Theorem 6.5. *With probability at least* $1 - \varepsilon$, *the output of* FIND_CHAR *contains* $\mathrm{ch}(G)$. *If* $d < 324\,485$ *then* $\mathrm{ch}(G)$ *is the only number in the output.*

Proof. First we prove that, if the algorithm terminates in Step (2), then the output is correct. Estimates for *the minimal dimension* $\delta(G)$ *of cross-characteristic representations* were given in [LS] and [SZ]; we use the tables from [Ti], which also record later improvements to the Landazuri–Seitz–Zalesskii bounds. Comparing the values $m_1(G)$ from Appendix A with $\delta(G)$ from [Ti], we see that all Lie-type simple groups satisfy $m_1(G) < 3\delta(G)$. Therefore, if we encounter some $g \in K$ with $|g| \geqslant 3d$, then indeed $\mathrm{ch}(G) = p$.

Claim. *If G is* not *orthogonal or symplectic of characteristic* 2 *and rank greater than* 18 *then, with probability at least* $1 - \varepsilon$, *the following holds. If* $m_1'(G) \geqslant 3d$, *then L contains a projective order at least* $3d$ *and if* $m_1'(G) < 3d$ *then L contains* $m_1'(G)$ *and* $m_2'(G)$ (*see Theorem* 1.4 *for the definition of* m_1' *and* m_2').

Proof of claim.

Classical groups. First, consider $G = X(\mathbf{d}, \mathbf{q})$, where X denotes any of the classical types PSL, PSp, PSU, $\mathrm{P}\Omega^{\varepsilon}$ and $\mathbf{d}$, $\mathbf{q}$ denote the (unknown) dimension and field size for G. We distinguish three cases.

Case 1. $\mathbf{d} \geqslant 7$ *and* $\mathbf{q}^{\mathbf{d}} \geqslant 81d^4$. Let $\mathbf{d}/2 < e \leqslant \mathbf{d} - 2$ and moreover let e be even in the symplectic and orthogonal cases, and let e be odd in the unitary case. We shall estimate the proportion of elements of G of order at least $3d$ and acting irreducibly on an e-dimensional nondegenerate subspace in the natural representation of G.

Standard arguments (see, e.g., [NiP, Section 5]) show that G contains at least $|G|/(2e\ \mathbf{c})$ cyclic subgroups $\mathbb{Z}_{\mathbf{c}}$, where $\mathbf{c} = \mathbf{q}^e - 1$ if G is special linear, $\mathbf{c} = \mathbf{q}^e + 1$ if G is unitary, and $\mathbf{c} = \mathbf{q}^{e/2} + 1$ if G is orthogonal or symplectic. Note that $\mathbf{c} \geqslant \mathbf{q}^{e/2} \geqslant \mathbf{q}^{\mathbf{d}/4} \geqslant 3d$ in all types of groups and for all e under consideration. By Lemma 6.2(b), each of these subgroups contains at least $\mathbf{c}\alpha(3d)$ elements of order at least $3d$. Moreover, if we choose the prime p in Lemma 6.2(b) to be a $\mathrm{ppd}^{\#}(\mathbf{q}; e)$-number in the nonunitary cases and a $\mathrm{ppd}^{\#}(\mathbf{q}; 2e)$-number in the unitary case then the sets of elements considered in different subgroups $\mathbb{Z}_{\mathbf{c}}$ are pairwise disjoint.

Define $f(\mathbf{d}) = \sum_e (1/(2e))$, where the summation runs over odd e satisfying $\mathbf{d}/2 < e \leqslant \mathbf{d} - 2$. For even $\mathbf{d}$ define $g(\mathbf{d}) = \sum_e (1/(2e))$ where the summation runs over even e satisfying $\mathbf{d}/2 < e \leqslant \mathbf{d} - 2$. By the estimates in the previous paragraph, G contains at least $|G|\alpha(3d)f(\mathbf{d})$ elements of order at least $3d$ in the unitary case and at least $|G|\alpha(3d)g(\mathbf{d})$ elements of order at least $3d$ in the other cases.

We claim that $f(\mathbf{d}), g(\mathbf{d}) \geqslant 1/12$ *for all* $\mathbf{d} \geqslant 7$. Indeed, it is clear that

$$\lim_{\mathbf{d}\to\infty} f(\mathbf{d}) = \lim_{\mathbf{d}\to\infty} g(\mathbf{d}) = \frac{1}{4} \lim_{\mathbf{d}\to\infty} \sum_{k=\lceil \mathbf{d}/2 \rceil}^{\mathbf{d}} \frac{1}{k} = \frac{\ln 2}{4} > 1/12.$$

Moreover, if we restrict the values of $\mathbf{d}$ to any of the four residue classes modulo 4 then, using the definitions of the functions, it is easy to see that the restrictions of $f(\mathbf{d})$ and $g(\mathbf{d})$ are monotone. Hence, it is enough to perform the easy check that $f(\mathbf{d}), g(\mathbf{d}) \geqslant 1/12$ for the four smallest possible values of $\mathbf{d} \geqslant 7$. We showed that the probability that a random element of G has order at least $3d$ is at least $\alpha(3d)/12$, implying that the probability that the sample L does *not* contain such a large order is at most

$$\left(1 - \frac{\alpha(3d)}{12}\right)^{|L|} \leqslant \left(1 - \frac{\alpha(3d)}{12}\right)^{\frac{32 \log^2(3d) \log(2/\varepsilon)}{\alpha(3d)}} < \varepsilon/2.$$

Case 2. $\mathbf{d} \geqslant 7$ *and* $\mathbf{q}^{\mathbf{d}} < 81d^4$. In this case, we claim that G contains at least $|G|/(2m'_i\ \mathbf{d}^2)$ cyclic subgroups of order m'_i, for $i = 1, 2$. If the elements of order m'_i come from tori that are direct products of at most two cyclic groups of order $\mathbf{q}^j \pm 1$ for some j, say for j_1, j_2 with $j_1 + j_2 = \mathbf{d}$ or $j_1 + j_2 = \lfloor \mathbf{d}/2 \rfloor$ (depending on the type of G; cf. Section 2), then the number of tori is at least $|G|/(m'_i \cdot 2j_1 \cdot 2j_2) \geqslant |G|/(m'_i\ \mathbf{d}^2)$. If the elements of order m'_i come from tori that are direct products of three cyclic groups and one of those is of order $\mathbf{q} + 1$ then the number of tori is at least $|G|/(2m'_i\ \mathbf{d}^2)$. These two subcases cover all instances when $\mathrm{ch}(G)$ is odd, or $\mathrm{ch}(G) = 2$ and G is special linear or unitary. Finally, if $\mathrm{ch}(G) = 2$ and G is symplectic or orthogonal of rank at most 18 then there are a few instances where the m'_i come from tori that are the products of four cyclic groups of order $\mathbf{q}^j \pm 1$ but the estimate $|G|/(2m'_i\ \mathbf{d}^2)$ is valid for these groups as well. Note that in Case 2 we have $2\mathbf{d}^2 < 32 \log^2(3d)$.

By Lemma 6.2(b), if $m'_1(G) \geqslant 3d$ then G contains at least $|G|\alpha(3d)/(2\mathbf{d}^2)$ elements of projective order at least $3d$ and so, with probability at least $1 - \varepsilon/2$, L contains a projective element order of at least $3d$. On the other hand, if $m'_1(G) < 3d$ then, by Lemma 6.2(a), L contains m'_i with probability at least $1 - \varepsilon/2$ for $i = 1, 2$, so L contains both m'_1 and m'_2 with probability at least $1 - \varepsilon$.

Case 3. $\mathbf{d} \leqslant 6$. In this case, $2\mathbf{d}^2 \leqslant 72 < 32\log^2(3d)$ and, as in Case 2, either L contains an element of order at least $3d$ or L contains both m'_1 and m'_2 with high probability.

Exceptional groups. Next, consider the case of exceptional groups G. In this case, as above, there are at least $|G|/(64m'_i)$ cyclic subgroups of order $m'_i = m'_i(G)$ for $i = 1, 2$ and, as in Cases 2 and 3 above, with probability at least $1 - \varepsilon$, either the list L contains an element of order at least $3d$ or L contains both m'_1 and m'_2. That finishes the proof of the claim. □

To finish the proof of the theorem, we have to show that if L contains both $m'_1(G)$ and $m'_2(G)$, and if $m'_1(G) < 3d$, then the output of the algorithm is correct with high probability. In this case, the values m^*_1, m^*_2 defined in Step (3) are one of the possible pairs $m^*_1(G)$ and $m^*_2(G)$ (cf. Definition 5.7), so they occur in the formulae in $\mathcal{L}$ unless G is orthogonal or symplectic of characteristic 2 and rank greater than 18. In the latter groups, $m'_1(G) \geqslant 973\,455$ so, since $m'_1(G) < 3d$, they can occur only if $d \geqslant 973\,455/3 = 324\,485$, and then Step (5) adds the number 2 as possible characteristic to the output list. For all other G, Step (4) adds $\mathrm{ch}(G)$ to the output list so, in any case, the output contains $\mathrm{ch}(G)$.

Our last task is to prove that *if $d \leqslant 324\,485$ then the output contains only one number*. We claim that the family $\mathcal{F}^*$ defined in Fact 5.8 contains all groups G with $m'_1(G) < 973\,455$. Indeed, suppose that $G = X(\mathbf{d}, \mathbf{q}) \notin \mathcal{F}^*$. The number 973 455 was chosen so that if $\mathbf{q}$ is even then $m'_1(G) > 973\,455$. If $\mathbf{q}$ is odd and G has Lie-rank at least 2, or $G = \mathrm{PSU}(3, \mathbf{q})$ then $\mathbf{q} > 10^5$ and Tables A.1–A.7 give $m'_1(G) > 973\,455$. Finally, if $\mathbf{q}$ is odd and G is rank 1 different from $\mathrm{PSU}(3, \mathbf{q})$ then $\mathbf{q} > 10^{10}$ and again $m'_1(G) > 973\,455$. Thus, if Step (4) created an output list containing more than one pair $(\mathrm{ch}(G), G)$, then these pairs occur either in Table 3 or they are of the form $(q, \mathrm{PSL}(2, q))$ and $(p, G_2(p))$. The groups G occurring in Table 3 are so small that, with probability at least $1 - \varepsilon$, the element orders $m_1(G)$ and $m_2(G)$ occur in our sample L. This means that a pair (m^*_1, m^*_2) from Table 3 can occur only if $m^*_1 = m_1(G)$ and $m^*_2 = m_2(G)$ for some group, and all of these possibilities are listed in Steps (6b) and (6c). For the pairs listed in Step (6b), there is a unique group with $m^*_1 = m_1(G)$ and $m^*_2 = m_2(G)$. Step (6c) handles the three pairs (m^*_1, m^*_2) for which there are two groups H, G of different characteristic with $m^*_1 = m_1(G) = m_1(H)$ and $m^*_2 = m_2(G) = m_2(H)$. Finally, if the input group modulo scalars is $G = G_2(p)$ then $m'_2(G) = p^2 - 1$ occurs in L, so that Step (6a) eliminates this type of ambiguity. □

Completion of the proof of Theorem 1.5. Since $n/\varphi(n) = O(\log\log n)$ for all n (see [MSC, §II.8]) and $1/\alpha(3d) = n/\varphi(n)$ for $n = \prod_{i=1}^{k(3d)} p_i$, we have $1/\alpha(3d) = O(\log\log d)$. Hence the number of random element selections is $O(\log^2 d \log\log d)$, as claimed in Theorem 1.5.

Applying Proposition 6.3 with $N = 3d$, we obtain that the computation of each projective order can be performed in $O(\mu d^3(\log d \log\log d + \log q))$ time.

The time requirement of Step (4) is negligible, because in the formulae in $\mathcal{L}$ the element orders grow exponentially with the rank of the groups. Hence, in the pairs in $\mathcal{L}$ to be compared to (m^*_1, m^*_2), the rank is bounded by $\log d$ and the number of pairs is a nearly linear, $O(d \log^c d)$, function of d.

Finally, we prove that the output contains fewer than $6d$ numbers. For every pair $(m^*_1(G), m^*_2(G))$ in $\mathcal{L}$ we have $m^*_1(G) \geqslant m'_1(G) \geqslant (\mathbf{q} + 1)/2$ (recall that $\mathbf{q}$ is the size of the field of definition of G). Hence, if the algorithm encounters no projective order greater than $3d$ then, with high probability, $3d \geqslant m^*_1 = m^*_1(G) \geqslant (\mathbf{q} + 1)/2$ and $\mathrm{ch}(G) \leqslant \mathbf{q} < 6d$. Therefore, the output is either $\{p\}$ (if no projective order greater than $3d$ is encountered) or a subset of the primes less than $6d$ (and hence has length quite a bit less than $6d$), as required in Theorem 1.5. □

Remark 6.6. *We claim that, in fact,* it is possible to modify our Algorithm Find_Char so that the output length is at most two for any d. We have already noted that, if Algorithm Find_Char encounters an element of projective order at least $3d$, then $\mathrm{ch}(G) = p$; and if all elements of the sample have projective order less than $3d$ then, with high probability, the size $\mathbf{q}$ of the field of the definition of G satisfies $\mathbf{q} < 6d$.

If $\mathbf{m}$ is the Lie-rank of G, then $\mathbf{m} \leqslant d$. Examining the values $m_i(G)$, $i = 1, 2, 3$, in Tables A.1–A.7 and Table 1 if $\mathrm{ch}(G)$ is odd, and using the same probability estimates as in the proof of Theorem 6.5, we find: $m_i(G)$ is attained among the element orders of G with frequency at least $\Omega(1/\mathbf{m}^2)$ if $m_i(G)$

Table 4
Sample running times.

K	d	p^e	Output	Time
$\mathrm{SL}(15, 2^8)$	15	2^8	2	< 0.01
$\mathrm{SL}(2, 29)$	14	2^2	$\mathrm{PSL}(2, 29)$	0.1
$\mathrm{SL}(2, 29)$	29	29	$\mathrm{PSL}(2, 29)$	0.2
$\mathrm{SL}(3, 11)$	132	2	$\mathrm{PSL}(3, 11), G_2(11)$	1.5
$\mathrm{SL}(6, 2)$	61	3	$\mathrm{PSL}(6, 2)$	0.5
$G_2(5)$	124	2	$G_2(5)$	0.9
$\mathrm{P}\Omega^-(8, 2)$	51	5	$F_4(2), \mathrm{P}\Omega^-(8, 2), \mathrm{PSp}(8, 2)$	0.4
$\mathrm{P}\Omega^+(18, 11^4)$	18	11^4	11	< 0.01
$Sz(8)$	14	7^2	$Sz(8)$	0.1
$Sz(8)$	195	5	$Sz(8)$	1.9
$E_6(3)$	27	3	3	< 0.01
$E_6(5^7)$	27	5^7	5	0.7
$\mathrm{SU}(25, 5^6)$	25	5^6	5	0.8
$\mathrm{Sp}(4, 7)$	175	2	$\mathrm{PSp}(4, 7)$	2.0
$\mathrm{SL}(30, 3^2)$	900	3^2	3	0.1

occurs for semisimple elements, and at least $\Omega(1/(\mathbf{qm}))$ if $m_i(G)$ occurs for nonsemisimple elements. (Recall that for functions $a(n), b(n)$, we say that $a(n)$ is $\Omega(b(n))$ if for large enough n, $a(n) > c\ b(n)$ for some positive constant c.) If Algorithm FIND_CHAR finds only projective orders less than $3d$ then both of these lower bounds are $\Omega(1/d^2)$ and, with the *selection of an additional* $\Omega(d^2 \log(1/\varepsilon))$ *random group elements in* Step (2), L will contain $m_1(G), m_2(G)$ (and $m_3(G)$ if $m_1(G) = m_1(H), m_2(G) = m_2(H)$ for some group H occurring in Table 1). Hence, by Theorem 1.2, the triple (m_1^*, m_2^*, m_3^*) computed in Step (3) uniquely determines $\mathrm{ch}(G)$ if $\mathrm{ch}(G)$ is odd. However, since we cannot exclude the case $\mathrm{ch}(G) = 2$, we also return the number 2, increasing the output length to two. If no group H in Tables A.1–A.7 satisfies $m_1^* = m_1(H)$ and $m_2^* = m_2(H)$, then the only number in the output is 2. This proves our claim.

This modified algorithm runs in $O(\xi d^2 + \mu d^5(\log d \log\log d + \log p^e))$ time, hence still in polynomial time.

Implementation. The algorithm has been implemented in *GAP*, and since 2006 has been part of the package `recog` [NS]. The implemented version works for input dimensions up to 5000.

Standard *GAP* functions are used for random element generation and order computation, based on [CLMNO,CLG]. Since we overestimated the number of random element selections with the bound $\lceil 32\log^2(3d)\log(2/\varepsilon)/\alpha(3d)\rceil$, in the implementation we use the following stopping criterion. If the value of (m_1^*, m_2^*, m_3^*) last changed at the computation of the order of the mth random group element then we stop after the generation of $2m + 50$ random elements.

Another useful heuristic is to start by computing the orbit of a random vector under the product of the given generators. This step seems to recognize groups with $\mathrm{ch}(G) = p$, and for these groups we can even avoid the initialization of the pseudorandom element generator and any potentially expensive projective order computations.

As a speedup of Step (4), we pre-computed and stored all of the triples $(m_1^*(H), m_2^*(H), H)$ with $m_1^*(H) \leqslant 15\,000$.

The computations reported in Table 4 were carried out using *GAP* Version 4.4.12 on an Intel Dual-Core 3.0 GHz processor. The input is a quasisimple group $K \leqslant \mathrm{GL}(d, p^e)$. The output is either $\mathrm{ch}(K/Z(K))$, or a list of candidate groups for $K/Z(K)$ all of the same characteristic. The reported running times are in seconds. The sample of groups includes all of the examples considered in [LO].

Acknowledgments

We are indebted to László Seress for the proof of Lemma 3.7, and to Frank Lübeck, Bob Guralnick and the referees for their helpful suggestions. The second author is grateful to the Mathematics

Department at the University of Auckland, Lehrstuhl D für Mathematik at the RWTH Aachen, and the School of Mathematics at the University of Western Australia, where parts of this research were carried out.

Appendix A

In Table A.2 for unitary groups, $a(n)$ denotes the smallest odd integer $a \geqslant 3$ satisfying $(a, n-a) = 1$. Note that we use $a(n)$ only for values of n for which $a(n) < n/2$.

Table A.1
$\mathrm{PSL}(d, q)$.

G	Restrictions	m_1	m_2
$\mathrm{PSL}(2, q)$	$q > 3$ prime	q	$\frac{q+1}{2}$
$\mathrm{PSL}(2, q)$	q composite	$\frac{q+1}{2}$	$\frac{q-1}{2}$
$\mathrm{PSL}(2k+1, q)$	$k \geqslant 1$	$\frac{q^{2k+1}-1}{(q-1)(q-1,2k+1)}$	$\frac{(q^{k+1}-1)(q^k-1)}{(q-1)(q-1,2k+1)}$
$\mathrm{PSL}(4k+2, q)$	$k \geqslant 1$	$\frac{q^{4k+2}-1}{(q-1)(q-1,4k+2)}$	$\frac{(q^{2k+3}-1)(q^{2k-1}-1)}{(q-1)(q-1,4k+2)}$
$\mathrm{PSL}(4k, q)$	$k \geqslant 1$	$\frac{q^{4k}-1}{(q-1)(q-1,4k)}$	$\frac{(q^{2k+1}-1)(q^{2k-1}-1)}{(q-1)(q-1,4k)}$

Table A.2
$\mathrm{PSU}(d, q)$.

G	Restrictions	m_1	m_2
$\mathrm{PSU}(2k+1, q)$	$k \geqslant 1$, q prime	$\frac{q^{2k}+q}{(q+1,2k+1)}$	$\frac{q^{2k}-1}{(q+1,2k+1)}$
$\mathrm{PSU}(2k+1, q)$	$k \in \{1, 2, 4\}$, q composite	$\frac{q^{2k}-1}{(q+1,2k+1)}$	$\frac{q^{2k+1}+1}{(q+1)(q+1,2k+1)}$
$\mathrm{PSU}(2k+1, q)$	$k \notin \{1, 2, 4\}$, q composite	$\frac{q^{2k}-1}{(q+1,2k+1)}$	$\frac{(q^{a'}+1)(q^{2k+1-a'}-1)}{(q+1)(q+1,2k+1)}$ $a' := a(2k+1)$
$\mathrm{PSU}(4, 3)$		12	9
$\mathrm{PSU}(2k, q)$	$k > 2$, q prime $q+1 \mid 2k$	$q^{2k-2} + q$	$q^{2k-2} - 1$
$\mathrm{PSU}(2k, q)$	$k \geqslant 2$, q prime $q+1 \nmid 2k$	$\frac{q^{2k-1}+1}{(q+1,2k)}$	$\frac{q^{2k-1}-q}{(q+1,2k)}$
$\mathrm{PSU}(2k, q)$	$k \in \{2, 3\}$, q composite	$\frac{q^{2k-1}+1}{(q+1,2k)}$	$\frac{q^{2k}-1}{(q+1)(q+1,2k)}$
$\mathrm{PSU}(10, 9)$		43 046 720	38 742 049
$\mathrm{PSU}(2k, q)$	$k \geqslant 6$, q composite $q+1 \mid 2k$	$q^{2k-2} - 1$	$\frac{(q^{a'}+1)(q^{2k-1-a'}-1)}{q+1}$ $a' := a(2k-1)$
$\mathrm{PSU}(2k, q)$	$k \geqslant 4$, q composite $q+1 \nmid 2k$	$\frac{q^{2k-1}+1}{(q+1,2k)}$	$\frac{(q^{a(2k)}+1)(q^{2k-a(2k)}+1)}{(q+1)(q+1,2k)}$

Table A.3
$\mathrm{PSp}(d, q)$.

G	Restrictions	m_1	m_2
$\mathrm{PSp}(4, 3)$		12	9
$\mathrm{PSp}(2k, 3)$	$k \geqslant 3$	$3^k + 9$	$3^k + 3$
$\mathrm{PSp}(2k, q)$	$k \geqslant 2$, $q > 3$ prime	$q^k + q$	$q^k - q$
$\mathrm{PSp}(4, q)$	q composite	$\frac{q^2+1}{2}$	$\frac{q^2-1}{2}$
$\mathrm{PSp}(6, q)$	q composite	$\frac{(q^2+1)(q+1)}{2}$	$\frac{q^3+1}{2}$
$\mathrm{PSp}(8, q)$	q composite	$\frac{(q^3-1)(q+1)}{2}$	$\frac{q^4+1}{2}$
$\mathrm{PSp}(4k+2, q)$	$k \geqslant 2$, q composite	$\frac{(q^{2k}+1)(q+1)}{2}$	$\frac{(q^{2k-1}+1)(q^2+1)}{2}$

(continued on next page)

Table A.3 (*continued*)

G	Restrictions	m_1	m_2
$\mathrm{PSp}(8k+4,q)$	$k \geqslant 1$, q composite	$\frac{(q^{4k+1}-1)(q+1)}{2}$	$\frac{(q^{4k}+1)(q^2+1)}{2}$
$\mathrm{PSp}(8k,q)$	$k \geqslant 2$, q composite	$\frac{(q^{4k-1}-1)(q+1)}{2}$	$\frac{(q^{4k-2}-1)(q^2+1)}{2}$

Table A.4
$\Omega(2m+1,q)$.

G	Restrictions	m_1	m_2
$\Omega(7,3)$		20	18
$\Omega(2k+1,3)$	$k \geqslant 4$	$2(3^{k-1}+9)$	$2(3^{k-1}+1)$
$\Omega(7,q)$	$q > 3$ prime	$\frac{(q^2+1)(q+1)}{2}$	$\frac{q(q^2+1)}{2}$
$\Omega(4k+3,q)$	$k \geqslant 2$, $q > 3$ prime	$\frac{(q^{2k}+1)(q+1)}{2}$	$\frac{q(q+1)(q^{2k-1}-1)}{2}$
$\Omega(4k+1,q)$	$k \geqslant 2$, $q > 3$ prime	$\frac{q(q+1)(q^{2k-2}+1)}{2}$	$\frac{(q^{2k-1}-1)(q+1)}{2}$
$\Omega(2k+1,q)$	$k \geqslant 3$, q composite	$m_1(\mathrm{PSp}(2k,q))$	$m_2(\mathrm{PSp}(2k,q))$

Table A.5
$\mathrm{P}\Omega^+(2m,q)$.

G	Restrictions	m_1	m_2
$\mathrm{P}\Omega^+(8,3)$		20	18
$\mathrm{P}\Omega^+(8,q)$	$q \geqslant 5$	$\frac{q^4-1}{4}$	$\frac{q^4-1}{8}$
$\mathrm{P}\Omega^+(2k,q)$	$k \in \{5,7,9\}$ q prime	$\frac{(q^{k-1}+1)(q+1)}{(q-1,4)}$	$\frac{q(q+1)(q^{k-2}-1)}{(q-1,4)}$
$\mathrm{P}\Omega^+(2k,q)$	$k \in \{5,7,9\}$ q composite	$\frac{(q^{k-1}+1)(q+1)}{(q-1,4)}$	$\frac{(q^2+1)(q^{k-2}+1)}{(q-1,4)}$
$\mathrm{P}\Omega^+(12,q)$		$\frac{(q+1)(q^2+1)(q^3-1)}{4}$	$\frac{(q^4+1)(q^2+1)}{4}$
$\mathrm{P}\Omega^+(4k+2,q)$	$k \geqslant 5$, q prime	$\frac{(q^{2k}+1)(q+1)}{(q-1,4)}$	$\frac{q(q+1)(q^{2k-1}-1)}{(q-1,4)}$
$\mathrm{P}\Omega^+(4k+2,q)$	$k \geqslant 5$ $q \equiv 1\ (4)$ composite	$\frac{(q^{2k}+1)(q+1)}{4}$	$\frac{(q^2+1)(q^4+1)(q^{2k-5}-1)}{4}$
$\mathrm{P}\Omega^+(4k+2,q)$	$k \geqslant 5$ $q \equiv 3\ (4)$ composite	$\frac{(q^{2k}+1)(q+1)}{2}$	$\frac{(q^2+1)(q^{2k-1}+1)}{2}$
$\mathrm{P}\Omega^+(16k+4,q)$	$k \geqslant 1$	$\frac{(q+1)(q^2+1)(q^{8k-1}-1)}{4}$	$\frac{(q+1)(q^4+1)(q^{8k-3}-1)}{4}$
$\mathrm{P}\Omega^+(16k+12,q)$	$k \geqslant 1$, q prime	$\frac{(q+1)(q^2+1)(q^{8k+3}-1)}{4}$	$\frac{q(q+1)(q^4+1)(q^{8k}+1)}{4}$
$\mathrm{P}\Omega^+(16k+12,q)$	$k \geqslant 1$, q composite	$\frac{(q+1)(q^2+1)(q^{8k+3}-1)}{4}$	$\frac{(q+1)(q^4+1)(q^{8k+1}-1)}{4}$
$\mathrm{P}\Omega^+(8k,q)$	$k \geqslant 2$, q prime	$\frac{q(q+1)(q^2+1)(q^{4k-4}+1)}{4}$	$\frac{(q+1)(q^2+1)(q^{4k-3}-1)}{4}$
$\mathrm{P}\Omega^+(8k,q)$	$k \geqslant 2$, q composite	$\frac{(q+1)(q^2+1)(q^{4k-3}-1)}{4}$	$\frac{(q+1)(q^4+1)(q^{4k-5}-1)}{4}$

Table A.6

G	Restrictions	m_1	m_2
$\mathrm{P}\Omega^-(10,3)$		$\frac{3(3+1)(3^3+1)}{4}$	$\frac{(3^4-1)(3+1)}{4}$
$\mathrm{P}\Omega^-(10,q)$	$q > 3$	$\frac{(q^2+1)(q^3-1)}{(q+1,4)}$	$\frac{q^5+1}{(q+1,4)}$
$\mathrm{P}\Omega^-(14,q)$	$q \equiv 1\ (4)$	$\frac{(q^2+1)(q^5-1)}{2}$	$\frac{q^7+1}{2}$
$\mathrm{P}\Omega^-(14,q)$	$q \equiv 3\ (4)$ prime	$\frac{(q+1)(q^2+1)(q^4+1)}{4}$	$\frac{q(q+1)(q^2+1)(q^3-1)}{4}$
$\mathrm{P}\Omega^-(14,q)$	$q \equiv 3\ (4)$ composite	$\frac{(q+1)(q^2+1)(q^4+1)}{4}$	$\frac{(q^2+1)(q^5-1)}{4}$
$\mathrm{P}\Omega^-(4k+2,q)$	$k \geqslant 4$, $q \equiv 1\ (4)$	$\frac{(q^2+1)(q^{2k-1}-1)}{2}$	$\frac{(q^4+1)(q^{2k-3}-1)}{2}$
$\mathrm{P}\Omega^-(8k+6,q)$	$k \geqslant 2$, $q \equiv 3\ (4)$ prime	$\frac{(q+1)(q^2+1)(q^{4k}+1)}{4}$	$\frac{q(q+1)(q^2+1)(q^{4k-1}-1)}{4}$

Table A.6 (*continued*)

G	Restrictions	m_1	m_2
$\mathrm{P\Omega}^-(8k+6,q)$	$k \geqslant 2$, $q \equiv 3$ (4) composite	$\frac{(q+1)(q^2+1)(q^{4k}+1)}{4}$	$\frac{(q+1)(q^4+1)(q^{4k-2}+1)}{4}$
$\mathrm{P\Omega}^-(16k+10,q)$	$k \geqslant 1$, $q \equiv 3$ (4) prime	$\frac{q(q+1)(q^2+1)(q^{8k+1}-1)}{4}$	$\frac{(q+1)(q^4+1)(q^{8k}+1)}{4}$
$\mathrm{P\Omega}^-(16k+10,q)$	$k \geqslant 2$, $q \equiv 3$ (4) composite	$\frac{(q+1)(q^4+1)(q^{8k}+1)}{4}$	$\frac{(q+1)(q^8+1)(q^{8k-4}+1)}{4}$
$\mathrm{P\Omega}^-(18,3)$		$\frac{3(3+1)(3^2+1)(3^5-1)}{4}$	$\frac{3(3+1)(3^7+1)}{4}$
$\mathrm{P\Omega}^-(16k+2,q) \neq \mathrm{P\Omega}^-(18,3)$	$k \geqslant 1$, $q \equiv 3$ (4) prime	$\frac{q(q+1)(q^2+1)(q^{8k-3}-1)}{4}$	$\frac{q(q+1)(q^4+1)(q^{8k-5}-1)}{4}$
$\mathrm{P\Omega}^-(18,q)$	$q \equiv 3$ (4) composite	$\frac{(q^2+1)(q^3+1)(q^4+1)}{4}$	$\frac{(q^2+1)(q^7-1)}{4}$
$\mathrm{P\Omega}^-(2^e+2,q)$	$e \geqslant 5$, $q \equiv 3$ (4) composite	$\frac{(q^2+1)(q^3+1)(q^{2^{e-1}-4}+1)}{4}$	$\frac{(q^2+1)(q^4+1)(q^{2^{e-1}-5}+1)}{4}$
$\mathrm{P\Omega}^-(2^e3+2,q)$	$e \geqslant 3$, $q \equiv 3$ (4) composite	$\frac{(q+1)(q^{2^{e-1}}+1)(q^{2^e}+1)}{4}$	$\frac{(q^2+1)(q^3+1)(q^{3\cdot 2^{e-1}-4}+1)}{4}$
$\mathrm{P\Omega}^-(2^ea+2,q)$	$e \geqslant 3$, $a \geqslant 5$ odd	$\frac{(q+1)(q^{2^{e-1}}+1)(q^{a'}+1)}{4}$	$\frac{(q+1)(q^{2^e}+1)(q^{a''}+1)}{4}$
	$q \equiv 3$ (4) composite	$a' := 2^{e-1}(a-1)$	$a'' := 2^{e-1}(a-2)$
$\mathrm{P\Omega}^-(4k,q)$	$k \geqslant 2$, q prime	$\frac{q(q+1)(q^{2k-2}+1)}{2}$	$\frac{(q+1)(q^{2k-1}-1)}{2}$
$\mathrm{P\Omega}^-(4k,q)$	$k \in \{2,3\}$, q composite	$\frac{(q+1)(q^{2k-1}-1)}{2}$	$\frac{q^{2k}+1}{2}$
$\mathrm{P\Omega}^-(8k,q)$	$k \geqslant 2$, q composite	$\frac{(q+1)(q^{4k-1}-1)}{2}$	$\frac{(q^2+1)(q^{4k-2}-1)}{2}$
$\mathrm{P\Omega}^-(8k+4,q)$	$k \geqslant 2$, q composite	$\frac{(q+1)(q^{4k+1}-1)}{2}$	$\frac{(q^3+1)(q^{4k-1}-1)}{2}$

Table A.7
Exceptional groups.

G	Restrictions	m_1	m_2
${}^2G_2(3)'$		9	7
${}^2G_2(3^k)$	$k = 2e+1, e \geqslant 1$	$3^{2e+1}+3^{e+1}+1$	$3^{2e+1}-1$
$G_2(q)$	q prime	q^2+q+1	q^2+q
$G_2(q)$	q composite	q^2+q+1	q^2-1
${}^3D_4(q)$	q prime	$(q^3-1)(q+1)$	$q(q^3+1)$
${}^3D_4(q)$	q composite	$(q^3-1)(q+1)$	q^4-q^2+1
$F_4(q)$	q prime	$q(q+1)(q^2+1)$	$(q^3-1)(q+1)$
$F_4(q)$	q composite	$(q^3-1)(q+1)$	q^4+1
$E_6(q)$	q prime	$\frac{q(q^6-1)}{(q-1)(3,q-1)}$	$\frac{(q+1)(q^5-1)}{(3,q-1)}$
$E_6(q)$	q composite	$\frac{(q+1)(q^5-1)}{(3,q-1)}$	$\frac{(q^2+q+1)(q^4-q^2+1)}{(3,q-1)}$
${}^2E_6(q)$	q prime	$\frac{(q+1)(q^2+1)(q^3-1)}{(3,q+1)}$	$\frac{q(q^5+1)}{(3,q+1)}$
${}^2E_6(q)$	q composite	$\frac{(q+1)(q^2+1)(q^3-1)}{(3,q+1)}$	$\frac{q^6-1}{(3,q+1)}$
$E_7(q)$	$q \equiv 1 \pmod 4$ prime	$\frac{(q^2+q+1)(q^5-1)}{2}$	$\frac{q(q+1)(q^2+1)(q^3-1)}{2}$
$E_7(q)$	$q \equiv 1 \pmod 4$ composite	$\frac{(q^2+q+1)(q^5-1)}{2}$	$\frac{(q+1)(q^6-q^3+1)}{2}$
$E_7(q)$	$q \equiv 3 \pmod 4$	$\frac{(q+1)(q^2+1)(q^4+1)}{2}$	$\frac{(q^2+q+1)(q^5-1)}{2}$
$E_8(q)$	$q \equiv 7 \pmod{12}$ prime	$(q+1)(q^2+q+1)(q^5-1)$	$q(q+1)(q^2+1)(q^4+1)$
$E_8(q)$	$q \equiv 7 \pmod{12}$ composite	$(q+1)(q^2+q+1)(q^5-1)$	$(q+1)(q^2+1)(q^5-1)$
$E_8(q)$	$q \equiv 1 \pmod{12}$ $q \equiv 0, 2 \pmod 3$	$(q+1)(q^2+q+1)(q^5-1)$	$(q^2+q+1)(q^6+q^3+1)$

References

[BB] László Babai, Robert Beals, A polynomial-time theory of black box groups. I, in: Groups St. Andrews 1997 in Bath, I, in: London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 30–64.

[BKPS] László Babai, William M. Kantor, Péter P. Pálfy, Ákos Seress, Black-box recognition of finite simple groups of Lie type by statistics of element orders, J. Group Theory 5 (2002) 383–401.

[BLGNPS] Robert Beals, C.R. Leedham-Green, Alice Niemeyer, Cheryl E. Praeger, Ákos Seress, A black-box group algorithm for recognizing finite symmetric and alternating groups, I, Trans. Amer. Math. Soc. 355 (2003) 2097–2113.

[Ca] Roger W. Carter, Finite Groups of Lie Type. Conjugacy Classes and Complex Characters, John Wiley & Sons, Inc., New York, 1985.

[CLG] Frank Celler, C.R. Leedham-Green, Calculating the order of an invertible matrix, in: Groups and Computation, II, New Brunswick, NJ, 1995, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 55–60.

[CLMNO] Frank Celler, C.R. Leedham-Green, Scott Murray, Alice Niemeyer, E.A. O'Brien, Generating random elements of a finite group, Comm. Algebra 23 (1995) 4931–4948.

[GAP4] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4, http://www.gap-system.org, 2005.

[Gi] Mark Giesbrecht, Nearly optimal algorithms for canonical matrix forms, PhD thesis, University of Toronto, 1993.

[H] Sergei Haller, Computing Galois cohomology and forms of linear algebraic groups, PhD thesis, Eindhoven Univ. Techn., 2005.

[KM] William M. Kantor, Kay Magaard, Black box exceptional groups of Lie type, in preparation.

[KS1] William M. Kantor, Ákos Seress, Black box classical groups, Mem. Amer. Math. Soc. 149 (708) (2001), viii+168 pages.

[KS2] William M. Kantor, Ákos Seress, Prime power graphs for groups of Lie type, J. Algebra 247 (2002) 370–434.

[LS] Vicente Landazuri, Gary M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra 32 (1974) 418–443.

[LG] C.R. Leedham-Green, The computational matrix group project, in: Groups and Computation, III, Columbus, OH, 1999, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 229–247.

[LGO] C.R. Leedham-Green, E.A. O'Brien, Constructive recognition of classical groups in odd characteristic, J. Algebra 322 (2009) 833–881.

[LO] Martin W. Liebeck, E.A. O'Brien, Finding the characteristic of a group of Lie type, J. Lond. Math. Soc. 75 (2007) 741–754.

[LiS] Martin W. Liebeck, Gary M. Seitz, Unipotent and nilpotent classes in simple algebraic groups and Lie algebras, preprint.

[Lü] Frank Lübeck, Finding p'-elements in finite groups of Lie type, in: Groups and Computation, III, Columbus, OH, 1999, in: Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 249–255.

[MSC] M.S. Mitrinović, J. Sándor, B. Crstici, Handbook of Number Theory, Math. Appl., vol. 351, Kluwer Academic Publishers, 1996.

[NS] Max Neunhöffer, Ákos Seress, A data structure for a uniform approach to computations with finite groups, in: Proc. International Symposium on Symbolic and Algebraic Computation, ISSAC '06, 2006, pp. 254–261.

[NiP] Alice Niemeyer, Cheryl E. Praeger, A recognition algorithm for classical groups over finite fields, Proc. London Math. Soc. 77 (1998) 117–169.

[O'B] E.A. O'Brien, Towards effective algorithms for linear groups, in: Finite Geometries, Groups, and Computation, de Gruyter, Berlin, 2006, pp. 163–190.

[SZ] Gary M. Seitz, Alexander E. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups. II, J. Algebra 158 (1) (1993) 233–243.

[Se] Ákos Seress, A unified approach to computations with permutation and matrix groups, in: Proc. of the International Congress of Mathematicians, Madrid, Spain, European Math. Soc., 2006, pp. 245–258.

[Ti] Pham Huu Tiep, Low dimensional representations of finite quasisimple groups, in: Groups, Combinatorics and Geometry, Durham, 2001, World Sci. Publishing, River Edge, NJ, 2003, pp. 277–294.

[vzG] Joachim von zur Gathen, Jürgen Gerhard, Modern Computer Algebra, Cambridge Univ. Press, Cambridge, 2003.