Finding the characteristic of a group of Lie type

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ
England

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

Abstract

We present a black-box polynomial-time Monte Carlo algorithm which, given as input a quasisimple group of Lie type, finds its characteristic.

1 Introduction

In this paper we present an algorithm which, given as input an arbitrary black-box representation of a group G of Lie type, determines its defining

Liebeck was partially supported by a Maclaurin Fellowship from the New Zealand Institute of Mathematics and its Applications. O'Brien was partially supported by the Marsden Fund of New Zealand via grant UOA412. We thank the referee for helpful comments and criticism of this work.

characteristic. Knowledge of the characteristic of G is necessary if we wish to apply the algorithms of [5] and [20], which identify the name of G and construct an isomorphism between G and its standard copy respectively.

We develop our algorithm in the general context of black-box groups. Babai & Szemerédi [7] introduced the *black-box group* model, where group elements are represented by bit-strings of uniform length. The only group operations permissible are multiplication, inversion, and checking for equality with the identity element. Seress [34, p. 17] defines a *black-box algorithm* as one which does not use specific features of the group representation, nor particulars of how group operations are performed; it can only use the operations listed above. However, a common assumption is that certain oracles are available. One such is an *order oracle* to compute the order of an element of a group.

Both permutation groups and matrix groups defined over finite fields are covered by the standard black-box model. We discuss in Section 5 how a suitable order oracle can be realised for these groups.

A *Monte Carlo* algorithm is a randomized algorithm which may return an incorrect answer to a decision question, the probability of this event being less than some specified value. A *Las Vegas* algorithm is one which never returns an incorrect answer, but may report failure with probability less than some specified value.

We present a black-box Monte Carlo algorithm which, given as input a quasisimple group G of Lie type, determines the characteristic of G. Recall

that a finite group G is quasisimple if G is perfect and $G/Z(G)$ is a non-abelian simple group.

If the elements of a black-box group G are represented by bit-strings of uniform length n, then n is the *encoding length* of G and $|G| \leq 2^n$. If G is described by a bounded list of generators, then the size of the input to a black-box algorithm is $O(n)$. If G also has Lie rank r and is defined over a field of size q, then $|G| > q^{r^2}$, so $r = O(\sqrt{n})$ and $\log q = O(n)$.

Our algorithm assumes that we can construct random elements of a finite group. Babai [2] presents a black-box Monte Carlo algorithm to construct in polynomial time nearly uniformly distributed random elements of a finite group. The product replacement algorithm of Celler *et al.* [14] also runs in polynomial time [31]. For a discussion of both algorithms, we refer the reader to [34, pp. 26-30].

Our principal result is the following.

Theorem 1.1 *There is a black-box polynomial-time Monte Carlo algorithm to determine the characteristic of a quasisimple group G of Lie type, subject to the existence of an oracle to compute the order of elements in G. If G has a black-box encoding of length n, then the characteristic can be determined by choosing a sample of size $O(n)$ of uniformly distributed random elements.*

We prove Theorem 1.1 by exhibiting the algorithm. Here is a brief outline. The algorithm proceeds by constructing centralizers of involutions in G. The structure of centralizers of involutions in groups of Lie type is well-known, and we can construct such centralizers efficiently. In particular,

few such groups have solvable involution centralisers C. Otherwise, in odd characteristic, $C^{(\infty)}$ (the last term of the derived series of C) is a commuting product of a small number (at most four) of groups of Lie type having the same characteristic as G; and in characteristic 2, $C^{(\infty)}$ has in general a non-central normal 2-subgroup. Our algorithm detects the presence or otherwise of such a normal 2-subgroup. If there is such a 2-subgroup, we conclude that the characteristic is 2, and stop; if not, the characteristic is odd and we construct an involution centralizer within a quasisimple factor of $C^{(\infty)}$, and repeat. Ultimately we obtain either a known group which we can explicitly identify, or $(P)SL_2(q)$ for q odd. We can readily deduce the latter's characteristic from knowledge of its two largest element orders.

If the quasisimple group G is given to us represented as a linear group defined over a finite field, then, as we demonstrate in Section 5, we no longer require an order oracle for G; instead we require such an oracle *only* for $(P)SL_2(q)$.

The structure of the paper is as follows. In Section 2 we discuss key concepts, and consider the context of the problem and other approaches to its solution. In Section 3 we prove the key results on groups of Lie type which underpin our algorithm and its analysis. We present the algorithm in Section 4 and consider its complexity in Section 5. Finally we report on our implementation of the algorithm, which is publicly available in Magma [8].

2 Background and motivation

We now discuss how our work contributes to the ongoing "matrix recognition" project, which seeks to develop effective well-understood algorithms for linear groups. We refer the reader to [30] for background and concepts related to this work.

Much of the focus of research activity is naturally on (quasi)simple groups. Two classes of algorithms for their study are under development:

- *non-constructive* algorithms, which name the non-abelian composition factor of a given quasisimple group;
- *constructive recognition* algorithms, which construct an explicit isomorphism between a quasisimple group G of known type and a "standard" (or natural) representation of G, and exploit this isomorphism to write an arbitrary element of G as a word in its defining generators.

Neumann & Praeger [28] present a Monte Carlo algorithm which decides whether or not a given subgroup of $GL_d(q)$ contains $SL_d(q)$. Niemeyer & Praeger [29] answer the analogous question with $SL_d(q)$ replaced by an arbitrary classical group in its natural representation. In the black-box context, Babai *et al.* [5] obtain the following result.

Theorem 2.1 ([5]) *Given a black-box group G which is isomorphic to a simple group of Lie type of known characteristic, the standard name of G can be computed using a polynomial-time Monte Carlo algorithm.*

Malle and O'Brien developed an implementation of this algorithm which is distributed with MAGMA [8]; their implementation used an "involution centralizer" approach to determine the characteristic when it is odd.

Kantor & Seress [20] prove the following.

Theorem 2.2 ([20]) *There is a Las Vegas algorithm which, when given as input a black-box quasisimple group G, where $G/Z(G)$ is isomorphic to a classical simple group C of known characteristic, produces a constructive isomorphism $G/Z(G) \longmapsto C$. The running time of the algorithm is polynomial in the size of the input and the field size.*

Brooksbank [10, 11] and Brooksbank & Kantor [12, 13] have further developed and refined this work to produce better constructive recognition algorithms for black-box classical groups.

All of this cited work *assumes* that the defining characteristic of a given group of Lie type is known. It is here that Theorem 1.1 makes an important contribution: it determines the characteristic.

A very different algorithm to determine the characteristic was developed by Kantor & Seress [21]. Here is a brief outline. Let G be a finite simple group of Lie type of characteristic p. Define a graph $\Gamma(G)$ as follows. Its vertices are those prime powers r^a ($r \neq p$ prime, $a > 0$) which occur as the order of some element of G. Two vertices having labels r^a, s^b are joined by an edge if and only if G has an element of order $\mathrm{lcm}(r^a, s^b)$. Let $\Delta(G)$ be the quotient graph subject to the equivalence relation that two vertices are equivalent if they have the same neighbours. They prove the following.

Theorem 2.3 ([21]) *Let G and H be two finite simple groups of Lie type such that $\Delta(G) \simeq \Delta(H)$. Then $G \simeq H$, with a small (explicit) list of exceptions.*

This theorem provides the theoretical underpinning for their Monte Carlo algorithm to determine the characteristic of a finite simple simple group G of Lie type. Its proof relies on testing for all prime powers q less than N, a function of the input length, whether G is a group of Lie type defined over the field of q elements. This is done by repeated invocations of the constructive recognition algorithm of Theorem 2.2. (Observe that in this application, the field size is bounded as a function of the size n of the input strings.) If this algorithm identifies the group, then the characteristic is now known. Otherwise the graph $\Delta(G)$ can be constructed, G identified, and so its characteristic determined. While polynomial-time, subject to the existence of an order oracle, the algorithm is not obviously practical: the bound N is $\max\{\lceil 5.4 \times 10^{13} \log n \rceil, \lceil 144 n^{3/2} \log n \rceil\}$ where G has black-box encoding length n.

Yet another algorithm is being developed by Seress: it aims to deduce the characteristic of a group of Lie type from its two largest element orders.

3 Key results

Let b, e be positive integers with $b > 1$. A prime r dividing $b^e - 1$ is a *primitive prime divisor* of $b^e - 1$ if r does not divide $b^i - 1$ for $1 \leq i < e$. By [37], $b^e - 1$ has a primitive prime divisor unless either $(b, e) = (2, 6)$, or

$e = 2$ and $b + 1$ is a power of 2.

For a finite group G and a prime p, let $\mu_p(G)$ and $\mu_{p'}(G)$ denote the proportions of p-singular and p-regular elements in G, respectively. (Recall that $g \in G$ is *p-singular* if its order is divisible by p, and *p-regular* if not.) If $S \subseteq G$, let $\mu_p(S)$ be the proportion of p-singular elements in S.

Let $G(q)$ denote a quasisimple group of Lie type over the field $\mathbb{F}_q$ of size $q = p^e$ (p prime). Denote by $\mathrm{rank}(G(q))$ the untwisted Lie rank of $G(q)$, that is, the Lie rank of the overlying simple algebraic group. Let q_k denote a primitive prime divisor of $p^{ek} - 1$.

We consider first the case of $L_2(q)$.

Lemma 3.1 *There is a black-box polynomial-time Monte Carlo algorithm to determine the characteristic of a quasisimple group G with $G/Z(G) \cong L_2(q)$, subject to the existence of an oracle to compute the order of elements in G. If G has a black-box encoding of length n, then the characteristic can be determined by choosing a sample of size $O(\log n)$ of uniformly distributed random elements.*

Proof. Consider first $G = SL_2(q)$. The conjugacy classes of G are well-known; see, for example, [16, p. 228]. The proportions of elements of order $q + 1, q - 1$ are each at least $1/\log\log q$. If $q = p^k$ for $k > 1$, these are the two largest orders of elements; whereas if $q = p$ there are also elements of order $2p$ and p, the proportions of which are $O(1/p)$.

Hence, with high probability, an investigation of a random sample of $O(\log n)$ elements will return either $q+1, q-1$ or $2p, p+1$ or $p+1, p$ as the

two largest orders (the latter two cases only if $q = p$ is small). In all cases we can easily deduce the value of p.

For $L_2(q)$ with q odd, again an investigation of a random sample of $O(\log n)$ elements for the two largest orders will, with high probability, return either $(q+1)/2$, $(q-1)/2$ or $p, (p+1)/2$, and again we deduce the value of p. ■

Our algorithm constructs involutions and their centralizers in $G(q)$; the next few results are important in the analysis of these tasks.

Lemma 3.2 *Let $G = G(q)$ be a quasisimple group of Lie type over $\mathbb{F}_q$.*

(i) *If q is odd, then $\mu_2(G) > 1/4$.*

(ii) *If q is even, then $\mu_2(G) > \frac{2}{5q}$.*

(iii) *If q is even, then $\mu_2(G) < \frac{3}{q-1} + \frac{2}{(q-1)^2}$.*

Proof. Part (i) follows from [19, 5.2], part (ii) from [19, 10.1], and part (iii) from [18, 1.1]. ■

Lemma 3.3 *Let $G = G(q)$ and let $r \neq p$ be a prime which divides $|G|$. Then*

(i) *$\mu_r(G) \geq \frac{1}{h}(1 - \frac{1}{r})$, where h is the Coxeter number of G;*

(ii) *if G is classical with natural module of dimension d, then $\mu_{r'}(G) > 1/2d$;*

(iii) *if G is exceptional, then $\mu_{r'}(G) > 1/15$.*

Proof. Part (i) is [19, 5.1], and parts (ii), (iii) are taken from [6]. ∎

Lemma 3.4 *Let $G = G(q)$ be quasisimple, and suppose that G contains an involution t such that $C_G(t)$ is solvable. Then one of the following holds:*

(i) *q is even, and $G/Z(G)$ is one of $L_2(q)$, $L_3^\epsilon(q)$, $Sp_4(q)$, ${}^2B_2(q)$;*

(ii) *$q = 2$ and $G/Z(G)$ is one of $L_n^\epsilon(2)$ $(n = 4, 5, 6)$, $U_n(2)$ $(n = 7, 8, 9)$, $Sp_n(2)$ $(n = 6, 8, 10)$, $\Omega_n^\epsilon(2)$ $(n = 8, 10)$, ${}^3D_4(2)$, ${}^2F_4(2)'$, $F_4(2)$, ${}^2E_6(2)$;*

(iii) *$q = 3$ and $G/Z(G)$ is one of $L_3^\epsilon(3)$, $L_4^\epsilon(3)$, $PSp_4(3)$, $\Omega_7(3)$, $P\Omega_8^+(3)$, $G_2(3)$;*

(iv) *q is odd and $G = L_2(q)$.*

Proof. For q even, the involution classes and centralizers in G are determined in [1], and the conclusion follows by inspection of these results. For q odd, the conclusion follows from [17, 4.5.1]. ∎

Lemma 3.5 *Let $G = G(q)$ with q odd, and suppose G has an involution t such that $C_G(t)$ is not solvable. Then $C_G(t)^{(\infty)}$ is a central product of at most four quasisimple groups, each of Lie type over an extension field of $\mathbb{F}_q$ of degree at most 3.*

Proof. This follows from [17, 4.5.1]. ∎

A critical component of our algorithm is the ability to construct involution centralizers in $G = G(q)$. We use an algorithm of Bray [9] to construct the centralizer $C_G(t)$ of an involution t in a black-box group G having an order oracle.

The following step produces an element of $C_G(t)$. Construct a conjugate t^g of t, where g is a random element of G. Let n be the order of the element $tt^g = [t, g]$, and let D be the dihedral group of order $2n$ generated by t and t^g. If n is odd, then D contains an element m such that $t^m = t^g$. Hence mg^{-1} is an element of $C_G(t)$.

Lemma 3.6 ([9]) *If g is uniformly distributed among the elements of G for which $[t, g]$ has odd order, say $2n + 1$, then $g[t, g]^n$ is uniformly distributed among the elements of $C_G(t)$.*

Lemma 3.7 *Let $G = G(q)$ of rank r with q odd, and let t be an involution in G.*

(i) *There is an absolute constant $c_1 > 0$ such that the proportion of $g \in G$ with $[t, g]$ of odd order is at least c_1/r.*

(ii) *Suppose that $C_G(t)^{(\infty)} \neq 1$. There is an absolute constant $c_2 > 0$ such that the proportion of pairs of elements of $C_G(t)$ which generate a subgroup containing $C_G(t)^{(\infty)}$ is at least c_2.*

Proof. Part (i) is proved in [32]. For (ii), denote by $P(H)$ the probability that a randomly chosen pair of elements of a finite group H generates

a subgroup containing $H^{(\infty)}$. It is well known that $P(H) > 0$ for every non-abelian finite simple group H; moreover, for almost simple groups H, $P(H) \to 1$ as $|H| \to \infty$, by [25, Theorem]. It follows that $P(H)$ is bounded away from 0 for almost simple groups H. Now (ii) follows easily from this fact together with Lemma 3.5. ■

Lemmas 3.6 and 3.7 show that if q is odd, then in $O(r)$ random selections we obtain, with high probability, a generating set for an involution centralizer $C_G(t)$ (or at least a subgroup between $C_G(t)^{(\infty)}$ and $C_G(t)$) in $G = G(q)$.

The situation in even characteristic is not so clear-cut. The next result will allow us to focus on a particular class of involutions for groups of even characteristic. Recall that a *long root element* of a group of Lie type is a non-identity element in the centre of a long root subgroup.

Theorem 3.8 *Let $G = G(q)$ with q even, and let $r = rank(G)$. The proportion of elements of G which have a power equal to a long root element is at least $1/(2rq)$.*

Proof. First consider the case when $G/Z(G) = L_2(q)$, $L_3^\epsilon(q)$ or ${}^2B_2(q)$. Then G has only one class of involutions, namely long root elements, and the conclusion follows from Lemma 3.2(ii); in particular $\mu_2(G) = 1/q$ for $G = L_2(q)$.

For $G = {}^2F_4(q)'$, there are two classes of involutions, and the calculation in [19, p. 177] gives lower bounds for the number of elements of G powering

into each class. Both lower bounds are at least $1/8q$.

Now assume G is not one of these groups. Let U be a long root subgroup of G, and t a long root element in U. The structure of $C_G(t)$ is well-known, and can for example be extracted from [1]. Writing $C = C_G(t)$, we have $C = QL$, where $Q = O_2(C_G(t))$ and Q, L are as in Table 1. Note that the entry in the last column of the table is only valid under the assumption that $C^{(\infty)} \neq 1$, i.e. L is non-solvable. The superscripts in the second column indicate the $\mathbb{F}_q$-dimensions of the L-composition factors in Q. We have also included an entry in the table for ${}^2F_4(q)$ for use in Theorem 3.9; the relevant information is taken from [33].

Define $\mathcal{F}$ to be the set of elements of odd order in L which act fixed point freely on the non-identity elements of Q/U. For $l \in \mathcal{F}$ the element tl has a power equal to t, and $C_Q(tl) = U$. It follows that the number of elements of G which have a power equal to t is at least $|\mathcal{F}| \cdot |Q/U|$, and hence the proportion of elements of G which have a power equal to a long root element is at least

$$\frac{|\mathcal{F}| \cdot |Q/U| \cdot |t^G|}{|G|} = \frac{|\mathcal{F}|}{q|L|}.$$

Hence, to complete the proof, it remains to show that $|\mathcal{F}|/|L| > 1/2r$. To do this, we specify in Table 2 a certain product N_L of primitive prime divisors of $|L|$.

We assert that every element of L of order divisible by N_L must lie in $\mathcal{F}$, except in the cases marked with (†) in Table 2, when this assertion requires some qualifications which will be made clear in the justification below.

Table 1: Structure of $C_G(t)$

G	Q	L	Q'	$Z(C^{(\infty)})$ (assuming $C^{(\infty)} \neq 1$)
$SL_n^\epsilon(q)\,(n \geq 4)$	$q^{1+2(n-2)}$	$SL_{n-2}^\epsilon(q).(q-\epsilon)$	U	U
$Sp_n(q)\,(n \geq 4)$	$q^{1+(n-2)}$	$Sp_{n-2}(q)$	1	U
$\Omega_{2m}^\epsilon(q)\,(m \geq 4)$	$q^{1+2(2m-4)}$	$SL_2(q) \times \Omega_{2m-4}^\epsilon(q)$	U	U
$G_2(q)\,(q > 2)$	q^{1+4}	$SL_2(q)$	U	U
${}^3D_4(q)$	q^{1+8}	$SL_2(q^3)$	U	U
${}^2F_4(q)$	$q^{1+4+1+4}$	$Sz(q)$	q^{1+4}	q
$F_4(q)$	q^{1+6+8}	$Sp_6(q)$	U	U
$E_6^\epsilon(q)$	q^{1+20}	$A_5^\epsilon(q)$	U	U
$E_7(q)$	q^{1+32}	$D_6(q)$	U	U
$E_8(q)$	q^{1+56}	$E_7(q)$	U	U

When $G = SL_n(q)$, the structure of Q/U as an $\mathbb{F}_q$-module for $L = GL_{n-2}(q)$ is $V_{n-2}(q) \oplus V_{n-2}(q)^*$, the sum of the natural module and its dual. Clearly every element of L of order divisible by q_{n-2} (if it exists) has odd order and acts fixed point freely on Q/U, and so is in $\mathcal{F}$. The only case where q_{n-2} does not exist is $(n, q) = (8, 2)$: now every element of L of order divisible by 7 and having two composition factors of dimension 3 on $V_6(2)$ is in $\mathcal{F}$.

The same argument applies when $G = Sp_n(q)$.

Table 2: Conditions on primitive prime divisors

G	N_L	conditions
$SL_n(q)\,(n \geq 4)$	q_{n-2}	$(n,q) \neq (8,2)$
	$7\,(\dagger)$	$(n,q) = (8,2)$
$SU_n(q)\,(n \geq 4)$	$q_{2(n-2)}$	n odd
	$q_{n-2}q_{(n-2)/2}$	n even, $n > 4, (n,q) \neq (8,2), (14,2)$
	$q_2\,(\dagger)$	$n = 4$
	$7, 13$	$(n,q) = (8,2), (14,2)$(resp.)
$Sp_n(q)\,(n \geq 4)$	q_{n-2}	$(n,q) \neq (8,2)$
	7	$(n,q) = (8,2)$
$\Omega^{\epsilon}_{2m}(q)\,(m \geq 4)$	$q_2\,(\dagger)$	
$G_2(q)$	q_2	$q \neq 2$
${}^3D_4(q), F_4(q), E_6^{\epsilon}(q)$	q_6q_2	$q \neq 2$
	21	$q = 2$
$E_7(q)$	q_8q_4	
$E_8(q)$	q_7 or q_{14}	

If $G = SU_n(q)$ then as an $\mathbb{F}_qL$-module, Q/U is $V_{n-2}(q^2) \oplus V_{n-2}(q^2)^*$ realised over $\mathbb{F}_q$. If n is odd the assertion is clear. If n is even, $n > 4$ and $(n,q) \neq (8,2), (14,2)$, then every element of L of order divisible by $q_{n-2}q_{(n-2)/2}$ must lie in a subgroup $GL_{(n-2)/2}(q^2)$ of L, and hence is in $\mathcal{F}$. If $n = 4$, the same is true of elements of order divisible by q_2 which have no eigenvalue 1 on the natural module. The exceptional cases $(8,2)$, $(14,2)$ are

easy.

Now suppose $G = \Omega^\epsilon_{2m}(q)$. Here $L = SL_2(q) \times \Omega^\epsilon_{2m-4}(q)$, and as an $\mathbb{F}_q L$-module, Q/U is $V_2(q) \otimes V_{2m-4}(q)$, the tensor product of the natural modules for the factors. Every element $(x, y) \in L$, where $x \in SL_2(q)$ has order divisible by q_2 and $y \in \Omega^\epsilon_{2m-4}(q)$ has odd order not divisible by q_2, is in $\mathcal{F}$.

The arguments for the remaining cases are similar. When $G = {}^3D_4(q)$, $L = SL_2(q^3)$, the $\mathbb{F}_q L$-module Q/U is $V_2 \otimes V_2^{(q)} \otimes V_2^{(q^2)}$ realised over $\mathbb{F}_q$, where $V_2 = V_2(q^3)$ is the natural L-module. When $G = F_4(q)$, Q/U has composition factors V_6 and V_8, natural and spin modules for $L = Sp_6(q)$. When $G = E_6^\epsilon(q)$, $Q/U \cong \wedge^3 V_6$, the triple wedge of the natural module V_6 for $L = A_5^\epsilon(q)$ (realised over $\mathbb{F}_q$ when $\epsilon = -$). When $G = E_7(q)$, $Q/U \cong V_{32}$, a spin module for $L = D_6(q)$. When $G = E_8(q)$, Q/U is the irreducible 56-dimensional module for $L = E_7(q)$ of high weight λ_7. In all but the last case it is clear that elements of order divisible by N_L lie in $\mathcal{F}$. In the last case, elements of $L = E_7(q)$ of order divisible by q_7 or q_{14} lie in a maximal rank subgroup $SL_8(q)$ or $SU_8(q)$, and the restriction of Q/U to these subgroups is $\wedge^2(V_8) \oplus \wedge^2(V_8)^*$. Hence these elements are in $\mathcal{F}$.

This proves our assertion. It remains to show that the proportion of elements of L of order divisible by N_L (with the restrictions indicated above in the (†) cases) is greater than $1/2r$. For the cases where L is a classical group or a product of such (i.e. all cases except for $G = E_8(q)$), this is immediate from [29, Theorem 5.7] and its proof, with obvious small modifications in

the cases where N_L is the product of more than one prime and also in the (†) cases. Finally, when $G = E_8(q)$, we need to show that the proportion of elements of $E_7(q)$ of order divisible by q_7 or q_{14} is greater than $1/16$; but this follows immediately from the main result of [6]. ■

The next theorem ensures that we can construct the centralizer of a long root element using the method of Lemma 3.6.

Theorem 3.9 *If $G = G(q)$ with q even, and t is a long root element of G such that $C_G(t)$ is not solvable, then the proportion of $g \in G$ such that $[t, g]$ has odd order is at least $1/4$.*

Proof. Assume that $G \neq {}^2F_4(q)$. Let U be a long root subgroup of G containing t, and let $S \cong SL_2(q)$ be a fundamental SL_2 in G generated by U and its opposite root group. The centralizers of S and of its elements are well-known, and can be found for example in [23, 1.2]. First, $C_G(S) = L$ where L is listed in Table 1 of Theorem 3.8. Let $x \in S$ be a non-identity element of order $q+1$ which is inverted by t, and let D be a dihedral subgroup of S of order $2(q + 1)$ containing x. Then for every $1 \neq y \in \langle x \rangle$ we have $C_G(y) = \langle x \rangle \times L$ and $N_G(\langle y \rangle) = D \times L$.

Now all involutions in D are conjugate to t, and the product of any two distinct such involutions is a non-identity element of $\langle x \rangle$. Hence the number of ordered pairs of G-conjugates of t whose product is conjugate to a non-identity power of x is at least

$$(\#\text{ of pairs in } D)\times(\#\text{ of conjugates of } \langle x \rangle) = (q+1)\cdot q\cdot|G : DL| = q|G : L|/2.$$

On the other hand, the total number of ordered pairs of conjugates of t is

$$|G : C_G(t)|^2 = |G : QL|^2,$$

where Q is as in Table 1. The proportion of pairs with product of (odd) order dividing $q+1$ is therefore at least the ratio of these two numbers, which is $q|Q|^2|L|/2|G|$. Arguing in exactly the same way with elements of order dividing $q-1$ in S, we see that the proportion of pairs of conjugates of t with product of order dividing $q-1$ is at least $(q-2)|Q|^2|L|/2|G|$. Hence the total proportion of pairs of conjugates of t having product of odd order is at least the sum of these two numbers, namely

$$\nu = \frac{(q-1)|Q|^2|L|}{|G|}.$$

The possibilities for Q and L are given by Table 1 in Theorem 3.8, and in all cases $\nu \geq 1/4$.

Finally, consider the case where $G = {}^2F_4(q)$. Note that $q > 2$ by our hypothesis that $C_G(t)$ is not solvable. Observe that the involution t lies in a Levi subgroup $S \cong Sz(q)$ of G, and $C_G(S) = T \cong Sz(q)$ (see [26]). As in the above proof, we use $x \in S$ of order $q-1$ which is inverted by t. Let $D = \langle x, t \rangle$, a dihedral group of order $2(q-1)$. For every $1 \neq y \in \langle x \rangle$ we have $C_G(y) = \langle x \rangle \times T$ and $N_G(\langle y \rangle) = D \times T$. Hence, as before, the proportion of pairs of conjugates of t with product of order dividing $q-1$ is at least

$$\frac{(q-1)(q-2)|G : DT|}{|G : C_G(t)|^2} = \frac{(q-2)q^{10}}{2(q^6+1)(q^3+1)(q^2-1)}.$$

This is greater than $1/4$, completing the proof. ∎

Lemma 3.10 *Let t be a long root element of $G = G(q)$ with q even, and suppose that $C_G(t)^{(\infty)} \neq 1$. There is an absolute constant $c > 0$ such that the proportion of pairs of elements of $C_G(t)$ which generate a subgroup containing $C_G(t)^{(\infty)}$ is at least c.*

Proof. Write $C = C_G(t) = QL$ with Q, L as in Table 1. It follows from the fact that all simple groups are 2-generator that $L^{(\infty)}$ is 2-generator, and hence so is $C^{(\infty)}$. By [25], the proportion of pairs of elements of C which, modulo Q, generate a subgroup containing $C^{(\infty)}$, tends to 1 as $|C| \to \infty$. Moreover, the proportion of such pairs which lie in some complement of Q tends to 0, and the conclusion follows. ■

We now prove a key theorem which will allow us to detect the presence of a normal 2-subgroup of an involution centralizer in characteristic 2.

Theorem 3.11 *Let $G = G(q)$ with q even, let $r = rank(G)$, and let t be a long root element of G. Assume $C_G(t)$ is non-solvable, and write $C = C_G(t)^{(\infty)}$, $Q = O_2(C)$. Then the proportion of $c \in C$ such that a power of c is an element of order 2 or 4 in $Q \backslash Z(C)$ is at least $1/2rq^3$ if $G \neq {}^2F_4(q)$, and is at least $1/2q^5$ if $G = {}^2F_4(q)$.*

Proof. Assume first that $G \neq {}^2F_4(q)$. The structure of C is given in Table 1 in the proof of Theorem 3.8. Following the notation used there, $C = QL'$, and in all cases $Q' \leq U = Z(C)$.

Let $\mathcal{J}$ be the set of $x \in L'$ of odd order such that $C_Q(x) \neq Z(C)$. Choose

$x \in \mathcal{J}$, of odd order m, say, and choose $y \in C_Q(x) \backslash Z(C)$. Define

$$S_1 = \{u \in Q : (ux)^m \in Z(C)\}, \quad S_2 = \{u \in Q : (ux)^m \notin Z(C)\}.$$

If $u \in S_1$, then $(ux)^m = z \in Z(C)$, so $(yux)^m = y^m zv$ for some $v \in Q'$, and hence $yu \in S_2$. Therefore $yS_1 \subseteq S_2$, and it follows that $|S_2| \geq \frac{1}{2}|Q|$.

Since Q has exponent dividing 4, the proportion of $c \in C$ such that a power of c is an element of order 2 or 4 in $Q \backslash Z(C)$ is at least $|\mathcal{J}|/2|L'|$. We shall show that this is at least $1/2rq^3$.

Suppose first that $G = SL_n(q)$, $L' = SL_{n-2}(q)$, so that $n \geq 4$ and $(n, q) \neq (4, 2), (4, 3)$. Here L' has a cyclic subgroup C of order $q^{n-3} - 1$, (in a subgroup $GL_{n-3}(q)$), and C has a unique subgroup C_0 of order $(q^{n-3} - 1)/(q - 1)$ (in $SL_{n-3}(q)$) fixing a nonzero vector of the natural module $V_{n-2}(q)$. Note that $N_{L'}(C) = C.(n - 3)$ if $n \geq 5$, $C.2$ if $n = 4$. Assume the primitive prime divisor q_{n-3} exists. Then every non-identity $x \in C_0$ of order divisible by q_{n-3} has centralizer C. Of course $|\mathcal{J}|$ is at least the number of L'-conjugates of such elements x, which is at least

$$|C_0|(1 - \frac{1}{q_{n-3}}) \cdot |L' : N_{L'}(C)| \geq \frac{|L'|}{2(n-3)(q-1)}(1 - \frac{1}{q_{n-3}}),$$

and hence $|\mathcal{J}|/2|L'| > 1/2rq^3$, as required. The only case where q_{n-3} does not exist is $(n, q) = (9, 2)$, in which case we apply the above argument, but count elements of order divisible by 21 rather than q_{n-3}.

Now consider $G = SU_n(q)$, $L' = SU_{n-2}(q)$. The conclusion is trivial when $n = 4$, since then $|L'| < q^3$, so assume $n \geq 5$. If n is even, we apply the argument of the previous paragraph, with C of order $q^{n-3} + 1$ (in a

subgroup $GU_{n-3}(q)$), C_0 of order $(q^{n-3}+1)/(q+1)$, counting elements x of order divisible by $q_{2(n-3)}$ (by 3 if $(n,q)=(6,2)$). If n is odd, we take a cyclic subgroup C of order $q^{n-3}-1$ (in a subgroup $GL_{(n-3)/2}(q^2)$ of $GU_{n-3}(q)$), a subgroup C_0 of order $|C|/(q+1)$, and count elements x of order divisible by a product $q_{n-3}q_{(n-3)/2}$ (with suitable modifications when $(n,q)=(9,2)$ or $(15,2)$).

When $G=Sp_{2m}(q)$, $L'=Sp_{2m-2}(q)$, the argument is slightly different. Again the conclusion is clear if $m=2$, since then $|L'|<q^3$, so assume $m\geq 3$. Take a cyclic subgroup C_0 of order $q^{m-2}+1$ in a subgroup $Sp_{2m-4}(q)$ of L' (so elements of C_0 lie in $\mathcal{J}$). Then $C_{L'}(C_0)=C_0\times Sp_2(q)$ and $N_{L'}(C_0)=(C_0\times Sp_2(q)).(m-2)$. Hence, counting conjugates of elements of C_0 of order divisible by q_{2m-4} (by 9 if $(m,q)=(5,2)$), we see that

$$\frac{|\mathcal{J}|}{|L'|}\geq\frac{1}{|Sp_2(q)|(m-2)}(1-\frac{1}{q_{2m-4}}),$$

which is at least $1/mq^3$, as required.

When $G=\Omega^\epsilon_{2m}(q)$, $L'=SL_2(q)\times\Omega^\epsilon_{2m-4}(q)$ and as an $\mathbb{F}_qL'$-module, Q/U is $V_2\otimes V_{2m-4}$, a tensor product of natural modules. If $d\in SL_2(q)$ is semisimple (of order dividing $q-\delta$, $\delta=\pm1$), then $d\in\Omega_2^\delta(q)$; so relative to a suitable basis $e_x=\mathrm{diag}(d,x)\in\Omega^\epsilon_{2m-4}(q)$ for every $x\in\Omega^{\delta\epsilon}_{2m-6}(q)$, and provided x has odd order, e_x is in $\mathcal{J}$. Counting such elements e_x yields the conclusion.

The case $G=G_2(q)$ is trivial, since here $|L'|=|SL_2(q)|<q^3$.

For $G={}^3D_4(q)$ we have $L'=SL_2(q^3)$ and an $\mathbb{F}_qL'$-module, Q/U is $V_2\otimes V_2^{(q)}\otimes V_2^{(q^2)}$ realised over $\mathbb{F}_q$, where $V_2=V_2(q^3)$ is the natural L'-

module. Take C to be a cyclic subgroup of order q^3-1 in L', and C_0 a subgroup of C of order q^2+q+1. Then $x \in C_0$ lie in $\mathcal{J}$, and if x has order divisible by q_3, then $C_{L'}(x) = C$. Now counting conjugates of such elements x gives the result in the usual way.

The case where $G = F_4(q)$, $L' = Sp_6(q)$ is handled by the argument given for $G = Sp_{2m}(q)$.

Now consider $G = E_6^\epsilon(q)$, $L' = A_5^\epsilon(q)$. Here $Q/U \cong \wedge^3 V_6$ (realised over $\mathbb{F}_q$), where V_6 is the natural L'-module. Hence L' has a subgroup $A_2^\epsilon(q)A_2^\epsilon(q)$ fixing nonzero vectors in Q/U. Now counting elements of $\mathcal{J}$ in this subgroup (for example those of order divisible by q_3 if $\epsilon = +$, by q_6 if $\epsilon = -$) yields the result.

If $G = E_7(q)$, $L' = D_6(q)$ then Q/U is a 32-dimensional spin module for L', and L' has a subgroup $A_5(q)$ fixing nonzero vectors (see [24, 2.6]). Counting elements of order divisible by q_6 (by 7 if $q = 2$) in this subgroup gives the result.

Now consider $G = E_8(q)$, $L' = E_7(q)$, so that Q/U is the 56-dimensional module for L' of high weight λ_7. Then L' has a subgroup $E = E_6(q)$, for which the restriction of Q/U is the sum of two 27-dimensional and two trivial modules. For $x \in E$ of order divisible by q_9, we have $|C_{L'}(x)| = (q^6+q^3+1)(q-1)$ (see [27]), and $|N_{L'}(C) : C| = 18$. Hence counting conjugates x in the usual way yields the conclusion.

To complete the proof, we consider the case where $G = {}^2F_4(q)$. Observe that the number of elements in Q having a power of order 2 or 4 in $Q \backslash Z(C)$

is at least $\frac{1}{2}|Q|$ (this can easily be seen using [33]). The conclusion follows, since $|Q| = |C|/|L| = |C|/|Sz(q)| > |C|/q^5$. ■

Remark In practice, in characteristic 2 our algorithm will often construct an involution which is not a long root element. Theorem 3.8 enables us to ignore such involutions in the analysis of the algorithm. However it should be possible (though not necessary for our algorithm) to use [1] to prove that the centralizers of such elements share the desirable properties of long root element centralizers established in Theorems 3.9 and 3.11.

4 The algorithm

Let G be a quasi-simple group of Lie type having a black-box encoding of length n. We now present the algorithm to find the defining characteristic p of G. In Section 5 we comment in more detail on the steps of the algorithm, where appropriate justify them, and comment on their cost.

1. Choose a sample S, of size $O(\sqrt{n})$, of random elements of G and determine the proportion of elements of even order in S. If $\mu_2(S) < 1/5$, conclude that $p = 2$ from Lemma 3.2(i) and terminate.

2. We may now assume that $\mu_2(S)$ is at least $1/5$. Hence if q is even, then $q \leq 16$ by Lemma 3.2(iii). Let $\mathcal{L}$ denote the list of groups from parts (i)-(iii) of Lemma 3.4. Let $e(H)$ denote the largest element order for $H \in \mathcal{L}$.

3. By powering elements of even order in S, obtain involutions in $G\backslash Z(G)$. If none exists, conclude that $G = SL_2(q)$ with q odd, find p using Lemma 3.1, and terminate.

4. Now we have a sample of involutions $t \in G\backslash Z(G)$. We process each t in turn as follows.

   (a) Construct first $C_G(t)$ and then $C = C_G(t)^{(\infty)}$. This is justified by Lemma 3.7 for q odd and by Theorem 3.9 and Lemma 3.10 for q even.

   (b) If $C = 1$, then by Lemma 3.4, either $G = L_2(q)$ with q odd, or $G \in \mathcal{L}$.

   If $\max\{|s| : s \in S\} \neq e(H)$ for all $H \in \mathcal{L}$, conclude that G is $L_2(q)$, find p using Lemma 3.1, and terminate.

   Otherwise, G is one of a known list of finite groups of bounded order. We construct its composition factors, so determine its characteristic, and terminate.

   (c) Otherwise $C \neq 1$.

   Among a sample of size $O(\sqrt{n})$ random elements of C, search for elements v of order 2 or 4 in $C\backslash Z(C)$. If we find such v, then set $K = \langle v^C \rangle$. Decide if K is a 2-group by investigating whether each of a sample of size $O(\sqrt{n})$ random elements of K has 2-power order. If so, conclude that $p = 2$ by Theorem 3.11, and terminate.

5. If, for all the involutions t in our sample, we fail to construct a 2-group as the normal closure of a non-central element of order 2 or 4 in the associated C, then we conclude that p is odd.

6. We may now assume that p is odd. Let $C = C_G(t)^{(\infty)}$ for some involution t from Step (4). We know by Lemma 3.5 that C is a central product of at most four groups of Lie type in characteristic p.

   Repeat the following sequence of steps until $C = 1$:

   (a) construct a quasisimple factor C_1 of C;

   (b) search for an involution $u \in C_1 \backslash Z(C_1)$;

   (c) if none is found, deduce that $C_1/Z(C_1) = L_2(q)$, find p using Lemma 3.1 and terminate;

   (d) otherwise, replace C by $C_{C_1}(u)^{(\infty)}$.

7. Conclude from Lemma 3.4 that the last non-trivial factor C_1 has central quotient isomorphic to one of the following:

   (a) $L_3^\epsilon(3)$, $L_4^\epsilon(3)$, $PSp_4(3)$, $\Omega_7(3)$, $P\Omega_8^+(3)$, $G_2(3)$;

   (b) $L_2(q)$ for q odd.

8. Let T be a sample of $O(\log n)$ random elements in C_1. If $\max\{|t| : t \in T\} \neq e(H)$ for all H having central quotient in Step (7a), then conclude $C_1/Z(C_1) = L_2(q)$, find p using Lemma 3.1, and terminate.

   Otherwise, C_1 is one of the groups listed in Step (7a). Construct its composition factors, so learning its characteristic. This determines p

since there are no isomorphisms between simple groups of Lie type in two different odd characteristics.

5 The complexity of the algorithm

We now analyze the complexity of various subtasks performed by the algorithm and verify that it completes in time polynomial in the size of the input. Recall that the input group G has a black-box encoding of length n; if G has Lie rank r and is defined over a field of size q, then $r = O(\sqrt{n})$ and $\log q = O(n)$.

Step 1. Lemma 3.2 implies that it suffices to choose a bounded sample of random elements in G. However, if G is defined over a field of characteristic 2 and size at most 16, then we must ensure that the sample of involutions considered at Step 4 contains a long root element. Hence Theorem 3.8 implies that we choose an initial sample S of size $O(\sqrt{n})$ random elements in G.

Step 3. The standard divide-and-conquer algorithm [34, p. 16] allows us to compute the mth power of an element of G in $\log_2(m)$ group multiplications.

Step 4. Recall that q is either odd or at most 16 when we construct $C_G(t)$ in Step (4a). Lemmas 3.7 and 3.10 and Theorem 3.9 imply that it suffices to choose in Step (4a) a sample of $O(\sqrt{n})$ random elements in G. Similarly Theorem 3.11 and Lemma 3.3 imply that samples of $O(\sqrt{n})$ random elements in C and K suffice in Step (4c).

Step 4a. Babai *et al.* [4] present a Monte Carlo polynomial-time algorithm to construct the derived series of a black-box group. Seress [34, pp. 38-40] describes a more practical alternative, which includes a black-box normal closure algorithm. In our application, the derived series of an involution centralizer has length at most 6.

Step 6a. The proportions of r-regular elements in $G(q)$ reported in Lemma 3.3 underpin a black-box Monte Carlo polynomial-time algorithm [3, Claim 5.3] to obtain one of the direct factors of a semisimple group. We summarize this algorithm briefly here. Let $G = H_1 \times H_2 \times \ldots \times H_k$ be semisimple. Choose a random element $g = (g_1, \ldots, g_k)$ and let $|g|$ divide m. If t is a prime dividing m, then t divides $|g_\ell|$ for some ℓ. Lemma 3.3 implies that, with probability at least $1/\sqrt{n}$, $|g_i|$ is not divisible by t for $i \neq \ell$. If so, then $g^{(m/t)} = (h_1, \ldots, h_k)$ where $h_\ell \neq 1$ and $h_i = 1$. Babai & Beals [3, Claim 5.3] prove that it suffices to consider a sample of $O(\sqrt{n})$ random elements of G to construct with high probability one direct factor. Lemma 3.5 shows that the number of such factors is at most 4.

Step 6. We recursively descend through a chain of involution centralizers. The depth of this recursion is potentially $O(\sqrt{n})$; to obtain a quasisimple factor in each case, we sample $O(\sqrt{n})$ random elements.

Steps 4b, 8. Since the list $\mathcal{L}$ arising from Lemma 3.4 is finite, the identification of individual groups on $\mathcal{L}$ has no impact on the overall complexity of the algorithm.

There are just ten coincidences between $e(H)$ for $H \in \mathcal{L}$ and $e(L_2(q))$ for

q odd, or $q \leq 16$; the largest such q is 257. Further, $e(L_2(13)) = e(SL_3(3)) = 13$, the only coincidence among groups in the lists of Step (7a) and (7b).

A case-by-case analysis shows that the proportion of elements of largest order in each group $H \in \mathcal{L}$ is at least $1/33$. Further $O = \{e(H) : H \in \mathcal{L}\}$ has cardinality 27 and maximum 273. Thus we can decide by powering if an element of G or C_1 has an order in O. If G has central quotient $L_2(q)$, then the proportion of elements of largest order is $O(\log n)$. Hence we can readily estimate the largest element order of G and C_1 in Steps (4b) and (8), respectively.

Hence, subject to the existence of a order oracle, the algorithm runs in time polynomial in the size of the input, requiring a sample of $O(n)$ uniformly distributed random elements.

5.1 The order oracle

Theorem 1.1 assumes the existence of an order oracle: it is used to determine $\mu_2(S)$ in Step (1) and is also required by Lemma 3.1.

Assume G is a black-box group. If a multiplicative upper-bound B for the order of $g \in G$ is available, and if the set of primes dividing B is known, then Babai & Beals [3, Claim 3.5] prove that $|g|$ can be determined in polynomial time. If we simply know B, then we can learn in polynomial time the *exact* power of 2 (or of any specified prime) which divides $|g|$. By repeated division by 2, we write $B = 2^m b$ where b is odd. Now we compute $h = g^b$, and determine (by powering) its order which divides 2^m. In particular, we

can deduce if g has *even order*.

In practice, black-box groups arise as permutation groups or linear groups. Since an order oracle can be readily realised for the former, we do not consider this case further.

Celler & Leedham-Green [15] provide an algorithm to compute the order of $g \in GL_d(s)$, where $s = t^k$, t prime. It first computes a multiplicative upper bound B for $|g|$. To obtain B, we determine and factorise the minimal polynomial $f(x)$ of g: let $f(x) = \prod_{i=1}^{n} f_i(x)^{m_i}$ where $\deg(f_i) = d_i$. Then take $\beta = \lceil \log_t \max m_i \rceil$ and

$$B \quad = \quad \mathrm{lcm}(s^{d_1} - 1, \ldots, s^{d_n} - 1) \times t^{\beta}. \tag{1}$$

The minimal polynomial of a $d \times d$ matrix defined over $\mathbb{F}_s$ can be computed [35] in $O(d^3 \log s)$ field operations, and factored [36, Theorem 14.14] in $O(d^2 \log s)$ field operations. If we know a factorisation of B, then the cost of the order algorithm is $O(d^3 \log s \log\log s^d)$ field operations.

Hence, if $G(q)$ is supplied as a subgroup of $GL_d(s)$, we exploit the multiplicative upper bound B from (1), and so estimate $\mu_2(S)$ in Step (1) in at most $O(d^4)$ operations, *without* an order oracle.

Hence, for linear groups, we require an order oracle *only* for groups having central quotient $L_2(q)$: in applying Lemma 3.1, we must know the *precise orders* of elements.

6 Implementation and performance

We have implemented our algorithm in MAGMA [8]. It takes as input a quasisimple group, represented either as a linear or as a permutation group.

We use the product replacement algorithm [14] to generate random elements. We use the algorithm of [15] to determine the order of a matrix, and the variation discussed in Section 5 to determine $\mu(S)$ for linear groups.

Leedham-Green & O'Brien [22] present Monte Carlo algorithms to generate random elements of the normal closure of a subgroup, and to determine membership in a normal subgroup of a black-box group having an order oracle. A consequence is a Monte Carlo algorithm to prove that a black-box group G is perfect: we prove that every generator of G is an element of its derived group. These algorithms are used with [34, pp. 38-40] to construct $C^{(\infty)}$, and with (a version of) of [3, Claim 5.3] to construct one of the direct factors of a semisimple group.

The maximum order of elements of each $H \in \mathcal{L}$ are recorded. Since q is small, the groups in $\mathcal{L}$ can be identified directly. We use (variations of) the Schreier-Sims algorithm [34, p. 64] to construct a base and strong generating set for $H \in \mathcal{L}$ and so learn its composition factors.

The computations reported in Table 3 were carried out using MAGMA V2.12 on a Pentium IV 2.8 GHz processor. The input to the algorithm is a quasisimple group of Lie type given as a subgroup of $GL_d(r^k)$. In the column entitled "Step", we identify the step in the algorithm where the defining characteristic is deduced. In the column entitled "Time", we list

the CPU time in seconds taken for this computation.

Table 3: Performance of implementation for a sample of groups

Input	d	r^k	Step	Time
$SL_{15}(2^8)$	15	2^8	(1)	0.5
$L_2(29)$	14	2^2	(4b)	0.3
$L_3(11)$	132	2^1	(6c)	15.3
$L_6(2)$	61	3^1	(4c)	5.7
$G_2(5)$	124	2^1	(6c)	6.7
$O_8^-(2)$	51	5^1	(4c)	6.4
$O_{18}^+(11^4)$	18	11^4	(6c)	7.6
$Sz(8)$	14	7^2	(4c)	0.7
$E_6(3)$	27	3^1	(8)	21.5
$E_6(5^7)$	27	5^7	(6c)	21.5
$SU_{25}(5^6)$	25	5^6	(6c)	258.9

References

[1] M. Aschbacher and G.M. Seitz, Involutions in Chevalley groups over finite fields of even order, *Nagoya Math. J.* **63** (1976), 1–91.

[2] L. Babai, Local expansion of vertex-transitive graphs and random generation in finite groups. *Theory of Computing*, (Los Angeles, 1991), pp. 164–174, Association for Computing Machinery, New York, 1991.

[3] L. Babai and R.M. Beals, A polynomial-time theory of black-box groups. I. In *Groups St. Andrews 1997 in Bath, I*, volume 260 of *London Math. Soc. Lecture Note Ser.*, pages 30–64, Cambridge, 1999. Cambridge Univ. Press.

[4] L. Babai, G. Cooperman, L. Finkelstein, E. Luks, and Á. Seress, Fast Monte Carlo algorithms for permutation groups. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991). *J. Comput. System Sci.* **50** (1995), 296–308.

[5] L. Babai, W.M. Kantor, P.P. Pálfy, and Á. Seress, Black-box recognition of finite simple groups of Lie type by statistics of element orders, *J. Group Theory* **5** (2002), 383–401.

[6] L. Babai, P. Pálfy and J. Saxl, On the number of p-regular elements in simple groups. Preprint.

[7] L. Babai and E. Szemerédi, On the complexity of matrix group problems, I. In *Proc. 25th IEEE Sympos. Foundations Comp. Sci.*, pages 229–240, 1984.

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

[9] J.N. Bray, An improved method for generating the centralizer of an involution, *Arch. Math. (Basel)* **74** (2000), 241–245.

[10] P.A. Brooksbank, A constructive recognition algorithm for the matrix group $\Omega(d, q)$. In *Groups and Computation, III (Columbus, OH, 1999)*,

volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 79–93. de Gruyter, Berlin, 2001.

[11] P.A. Brooksbank, Fast constructive recognition of black-box unitary groups, *LMS J. Comput. Math.* **6** (2003), 162–197 (electronic).

[12] P.A. Brooksbank and W.M. Kantor, On constructive recognition of a black-box PSL(d, q). In *Groups and Computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 95–111, Berlin, 2001. de Gruyter.

[13] P.A. Brooksbank and W.M. Kantor, Fast constructive recognition of black-box orthogonal groups, *J. Algebra*, **300** (2006), 256–288.

[14] F. Celler, C.R. Leedham-Green, S.H. Murray, A.C. Niemeyer and E.A. O'Brien, Generating random elements of a finite group, *Comm. Algebra* **23** (1995), 4931–4948.

[15] F. Celler and C.R. Leedham-Green, Calculating the order of an invertible matrix. In *Groups and Computation II*, volume 28 of *Amer. Math. Soc. DIMACS Series*, pages 55–60. (DIMACS, 1995), 1997.

[16] L. Dornhoff, *Group Representation Theory, Part A*, Marcel Dekker, 1971.

[17] D. Gorenstein, R. Lyons and R. Solomon, *The classification of finite simple groups*, Mathematical Surveys and Monographs, Vol. 40.3, American Mathematical Society, Providence, RI, 1998.

[18] R. Guralnick and F. Lübeck, On p-singular elements in Chevalley groups in characteristic p, in *Groups and computation, III (Columbus, OH, 1999)* (eds. W.M. Kantor and Ákos Seress), Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001, pp. 169–182.

[19] I.M. Isaacs, W.M. Kantor and N. Spaltenstein, On the probability that a group element is p-singular, *J. Algebra* **176** (1995), 139–181.

[20] W.M. Kantor and Á. Seress, Black box classical groups, *Mem. Amer. Math. Soc.* **149**, No.708 (2001), viii+168.

[21] W.M. Kantor and Á. Seress, Prime power graphs for groups of Lie type, *J. Algebra* **247** (2002), 370–434.

[22] C.R. Leedham-Green and E.A. O'Brien, Recognising tensor-induced matrix groups. *J. Algebra* **253** (2002), 14–30.

[23] M.W. Liebeck and G.M. Seitz, Subgroups generated by root elements in groups of Lie type, *Annals of Math.* **139** (1994), 293–361.

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

[25] M.W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103–113.

[26] G. Malle, The maximal subgroups of ${}^2F_4(q^2)$, *J. Algebra* **139** (1991), 52–69.

[27] K. Mizuno, The conjugate classes of Chevalley groups of type E_6, *J. Fac. Sci. Univ. Tokyo* **24** (1977), 525–563.

[28] P.M. Neumann and C.E. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc.* **65** (1992), 555–603.

[29] A.C. Niemeyer and C.E. Praeger, A recognition algorithm for classical groups over finite fields, *Proc. London Math. Soc.* **77** (1998), 117-169.

[30] E.A. O'Brien, Towards effective algorithms for linear groups. *Finite Geometries, Groups and Computation*, (Colorado), pp. 163-190. De Gruyter, Berlin, 2006.

[31] I. Pak, The product replacement algorithm is polynomial, In *41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)*, 476–485, IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

[32] Christopher W. Parker and Robert A. Wilson. Recognising simplicity of black-box groups. Preprint.

[33] D. Parrott, A characterization of the Ree groups ${}^2F_4(q)$, *J. Algebra* **27** (1973), 341–357.

[34] Á. Seress, *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[35] A. Storjohann, An $O(n^3)$ algorithm for the Frobenius normal form, In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation* (Rostock), 101–104, ACM, New York, 1998.

[36] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2002.

[37] K. Zsigmondy, Zür Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

Last revised September 2006