Recognition of finite exceptional groups of Lie type

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

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

Abstract

Let q be a prime power and let G be an absolutely irreducible subgroup of $GL_d(F)$, where F is a finite field of the same characteristic as $\mathbb{F}_q$, the field of q elements. Assume that $G \cong G(q)$, a quasisimple group of exceptional Lie type over $\mathbb{F}_q$ which is neither a Suzuki nor a Ree group. We present a Las Vegas algorithm that constructs an isomorphism from G to the standard copy of $G(q)$. If $G \not\cong {}^3D_4(q)$ with q even, then the algorithm runs in polynomial time, subject to the existence of a discrete log oracle.

1 Introduction

Informally, a *constructive recognition algorithm* constructs an explicit isomorphism between a quasisimple group G and a 'standard' copy of G, and exploits this isomorphism to write an arbitrary element of G as a word in its defining generators. For a more formal definition, see [53, p. 192]. Such algorithms play a critical role in the 'matrix group recognition project' which aims to develop efficient algorithms for the investigation of subgroups of $\mathrm{GL}_d(F)$ where F is a finite field. We refer to the recent survey [50] for background related to this work. Such algorithms are available for classical groups; see, for example, [29, 30, 42]. Here we present constructive recognition algorithms for the finite exceptional groups of Lie type.

Let $G(q)$ denote a quasisimple exceptional group of Lie type over $\mathbb{F}_q$, a finite field of size q. Howlett, Rylands & Taylor [35] provide defining matrices for a specific faithful irreducible representation of minimal dimension of the simply connected group of type $G(q)$: we call this representation the *standard copy* of type $G(q)$.

Our principal result is the following. In the statement, $V_d(F)$ denotes the underlying vector space of dimension d over the field F.

Theorem 1 *Let q be a prime power and let G be an absolutely irreducible subgroup of $GL_d(F)$, where F is a finite field of the same characteristic as $\mathbb{F}_q$. Assume that $G \cong G(q)$, a quasisimple group of exceptional Lie type over $\mathbb{F}_q$ for $q > 2$, excluding Suzuki and Ree groups, and also ${}^3D_4(q)$ with q even. There is a Las Vegas algorithm that constructs an isomorphism from G to the standard copy of type $G(q)$ modulo*

2000 *Mathematics Subject Classification.* 20C20, 20C40.

a central subgroup, and also constructs the inverse isomorphism; it also computes the high weight of $V_d(F)$ as a G-module, up to a possible twist by a field or graph automorphism. The algorithm runs in polynomial time, subject to the existence of a discrete log oracle for extensions of $\mathbb{F}_q$ of degree at most 3.

The possible central subgroups of the standard copy of type $G(q)$ are trivial except when $G(q)$ is of type $E_6^{\epsilon}(q)$ ($\epsilon = \pm 1$) or $E_7(q)$, in which case they have order dividing $(3, q-\epsilon)$ and $(2, q-1)$ respectively.

We now discuss how the isomorphisms in the statement of the theorem are realised. Let $\hat{G}(q)$ denote the standard copy of type $G(q)$. It has a *Curtis-Steinberg-Tits* presentation, which involves only those relations which arise from certain rank 2 subgroups of $G(q)$: namely, the commutator relations among root elements corresponding to pairs of fundamental roots in the corresponding Dynkin diagram. Babai *et al.* [7, §4.2 and 6.1] reduce this presentation by running over root elements parametrised by an $\mathbb{F}_p$-basis for $\mathbb{F}_q$ (where p is the characteristic of $\mathbb{F}_q$). Those root elements of $\hat{G}(q)$ which satisfy this reduced Curtis-Steinberg-Tits presentation are the *standard generators* $\hat{\mathcal{S}}$ for $\hat{G}(q)$.

Given a group G as in the statement of the theorem, described by a generating set X, our algorithm produces a collection $\mathcal{S}$ of generators of G (as words in X) which satisfy the reduced Curtis-Steinberg-Tits presentation. These are then used to construct the required isomorphisms $\phi : G \to \hat{G}(q)/Z$ and $\psi : \hat{G}(q)/Z \to G$ (where Z is a central subgroup), as follows. Cohen, Murray & Taylor [22] developed the *generalised row and column reduction algorithm*: in polynomial time, for a given high weight representation of $G \cong G(q)$ with $G(q)$ of untwisted type, this algorithm writes an arbitrary $g \in G$ as a word $w(\mathcal{S})$ in the standard generators; this has now been extended to twisted types in [23]. Now $\phi(g) = w(\hat{\mathcal{S}})Z$, the corresponding word in the standard generators of $\hat{G}(q)$, defines the isomorphism ϕ. The inverse isomorphism ψ is defined similarly: for $\hat{g} \in \hat{G}(q)$, the algorithms of [22, 23] express $\hat{g}$ as a word $w(\hat{\mathcal{S}})$, and we set $\psi(\hat{g}Z) = w(\mathcal{S})$.

Together, the algorithms of Theorem 1 and of [22, 23] provide a solution to the *constructive membership problem* for $G = \langle X \rangle$: namely, express an arbitrary $g \in G$ as a word in X.

Our algorithms to find standard generators in G begin by constructing SL_2 subgroups of G which can be placed as nodes in the Dynkin diagram so that they pairwise generate the appropriate group of rank 2, and these are then used to label root elements and toral elements of G relative to a fixed root system. We use the root elements to compute the high weight of the given representation of G on $V_d(F)$, and then exploit the algorithms of [22, 23] to set up the isomorphisms explicitly.

To construct the SL_2 subgroups and label root elements, we use involution centralizers in G. That such centralizers can be constructed in Monte Carlo polynomial time follows in odd characteristic from [52], and in even characteristic from [43]; see Section 2.3 for further discussion.

A distinguishing feature of our work is that the resulting algorithms are practical; this desire significantly influenced our design. Our algorithms are implemented and will be publicly available in MAGMA [12].

The excluded Suzuki and Ree groups of types ${}^2B_2(q)$, ${}^2G_2(q)$, and ${}^2F_4(q)$ were studied by Bäärnhielm [2–4]. His constructive recognition algorithms apply to conjugates of the standard copy of ${}^2B_2(q)$ and ${}^2G_2(q)$, and run in polynomial time subject to the availability of a discrete log oracle. For the groups ${}^3D_4(q)$ (q even), also excluded in the theorem, we provide a practical algorithm with running time $O(q)$. We also present practical algorithms for groups defined over $\mathbb{F}_2$, the only field not covered by Theorem 1. Where feasible, our theoretical results also include $\mathbb{F}_2$.

As stated, Theorem 1 applies to absolutely irreducible representations of quasisimple groups of exceptional Lie type. The principal motivation for stating it under this assumption is our application of the algorithms of [22, 23] to realise the isomorphisms between G and $\hat{G}(q)/Z$. Using the Meataxe and associated machinery [34, Chapter 7], the result can easily be reformulated to apply, with unchanged complexity, to all matrix representations (not necessarily irreducible) in defining characteristic. For all but $E_8(q)$ in even characteristic, our algorithms to construct the SL_2 subgroups and to label the root and toral elements are black-box *provided* that the algorithms employed in Theorem 2.2 for constructive recognition of small rank classical groups are black-box. Since algorithms are available for these tasks (see, for example, [30] and its references), a version of Theorem 1 could be formulated for black-box groups. We refrain from doing so.

Kantor & Magaard [39] presented black-box Las Vegas algorithms to recognise constructively the exceptional simple groups of Lie type and rank at least 2, other than ${}^2F_4(q)$, defined over a field of known size. These have complexity depending linearly on the size of the field. Dick [28] developed a polynomial-time algorithm, a modification of that proposed by [39], for $F_4(q)$ in odd characteristic. Relying as it does on centralizers of involutions, our work differs substantially from [39].

The structure of the paper is as follows. Section 2 records a number of results which underpin our algorithm. In Section 3 we prove results on probabilistic generation for certain groups of Lie type. In Sections 4-10 we present algorithms to construct SL_2 subgroups of a group G as in Theorem 1 which correspond to the nodes in the associated Dynkin diagram. Sections 11-13 contain algorithms to label root elements and toral elements of G relative to a fixed root system; to determine the high weight of the given representation of G on $V_d(F)$; and to construct the standard generators for G. In Section 15 we present algorithms for the special case of groups defined over $\mathbb{F}_2$. In Section 16 we report on our implementation in Magma. Finally, for each group of exceptional Lie type and Lie rank at least 2, its reduced Curtis-Steinberg-Tits presentation on standard generators is listed explicitly in Appendix A.

Acknowledgements. This work was supported in part by the Marsden Fund of New Zealand via grant UOA 1323 and an International Exchange grant from the Royal Society. We thank Arjeh Cohen and Don Taylor for their work on [23], providing access to their implementation of the algorithms of [22,23], and for many helpful discussions; we thank Scott Murray for assistance on Lie algebra computations.

2 Background and preliminaries

A *Monte Carlo* algorithm is a randomised algorithm which always terminates but may return a wrong answer with probability less than any specified value. A *Las Vegas* algorithm is a randomised algorithm which never returns an incorrect answer, but may report failure with probability less than any specified value.

Our algorithms usually search for elements of G having a specified property. If $1/k$ is a lower bound for the proportion of such elements in G, then we can readily prescribe the probability of failure of the corresponding algorithm. Namely, to find such an element by random search with a probability of failure less than a given $\epsilon \in (0, 1)$ it suffices to choose (with replacement) a sample of uniformly distributed random elements in G of size at least $\lceil -\log_e(\epsilon)k\rceil$.

Babai & Szemerédi [5] 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 [53, p. 17] defined 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.

Babai [6] present a Monte Carlo algorithm to construct in polynomial time independent nearly uniformly distributed random elements of a finite group. An alternative is the *product replacement algorithm* of Celler *et al.* [21], which runs in polynomial time by a result of [51]. For a discussion of both algorithms we refer to [53, pp. 26–30].

Often it is necessary to investigate the order of $g \in \mathrm{GL}_d(\mathbb{F}_q)$, which, due to integer factorisation, cannot be determined in polynomial time. We can, however, determine its *pseudo-order*, a good multiplicative upper bound for $|g|$, and the exact power of any specified prime that divides $|g|$, using a Las Vegas algorithm with complexity $O(d^3 \log d + d^2 \log d \log q)$. Our results sometimes assume the existence of an *order oracle* but, in our applications, it always suffices to use pseudo-order. A Las Vegas algorithm with the same complexity allows us to compute large powers g^n where $0 \leq n < q^d$. We refer to [42, §2 and 10] for more details and references.

Leedham-Green & O'Brien [41] 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. Babai & Shalev [9] prove that if the normal subgroup is simple and non-abelian, then the membership algorithm runs in Monte Carlo polynomial time. A consequence is a Monte Carlo black-box algorithm to prove that a group is perfect. This algorithm is used together with the black-box polynomial-time algorithm described in [53, pp. 38-40] to construct the derived series of a group.

To construct a direct factor of a semisimple group, we use the black-box algorithm, KillFactor, of [8, Claim 5.3]; that it runs in polynomial time is a consequence of [11, Corollary 4.2].

If a matrix group acts absolutely irreducibly on its underlying vector space of dimension d, then we can determine the classical forms it preserves in $O(d^3)$ field operations (see [34, §7.5.4]). A hyperbolic basis for a vector space of dimension d with a given non-degenerate bilinear form can be constructed in $O(d^3)$ field operations (see [16] for an algorithm to perform this task).

2.1 Recognition for classical groups

Babai *et al.* [10] proved the following.

Theorem 2.1 *Given a black-box group G isomorphic to a simple group of Lie type of known characteristic, the standard name of G can be computed using a Monte*

Carlo polynomial-time algorithm.

Liebeck & O'Brien [43] present a Monte Carlo black-box polynomial-time algorithm to identify the defining characteristic. Kantor & Seress [38] give an alternative algorithm for absolutely irreducible matrix groups.

Kantor & Seress [36] developed the first black-box Las Vegas algorithms to recognise constructively classical groups; these have complexity depending linearly on the size of the field. More recently, Leedham-Green & O'Brien [42] developed algorithms for classical groups in natural representation and odd characteristic; those of Dietrich *et al.* [29] apply to even characteristic. Black-box equivalents appear in [30]. All run in time polynomial in the size of the input subject to the availability of a discrete log oracle.

Our algorithms for the labelling of root and toral elements rely on the availability of constructive recognition algorithms for the classical groups listed in the following theorem. As defined in [42], the *standard copy* of a classical group is its natural matrix representation, preserving a specified form.

Theorem 2.2 *Let q be a prime power, and let G be a subgroup of $GL_d(F)$, where F is a field of the same characteristic as $\mathbb{F}_q$. Assume that G is isomorphic to one of the following classical groups: $SL_2(q)$, $SL_3(q)$, $Sp_4(q)$, or $SU_4(q)$ in all characteristics; $SL_6(q)$, $Sp_6(q)$, $SU_6(q)$, $\Omega_8^{\pm}(q)$ or $\Omega_{12}^{+}(q)$ for even q. There is a Las Vegas algorithm that constructs an isomorphism from G to its standard copy. Subject to the existence of a discrete log oracle, the algorithm runs in polynomial time.*

This follows from [17], [18], [19], [26], [30], and [49].

2.2 Groups of Lie type

We use $SL_n^{\epsilon}(q)$ to denote $SL_n(q)$ for $\epsilon = 1$ and $SU_n(q)$ for $\epsilon = -1$; we adopt similar conventions for $D_4(q)$ and ${}^2D_4(q)$; and for $E_6(q)$ and ${}^2E_6(q)$. Dynkin diagrams for exceptional root systems are labelled as follows:

$$\begin{array}{lccccccccccccc}
E_l & & 1 & - & 3 & - & 4 & - & 5 & - & \cdots & - & l \\
 & & & & & & | & & & & & & \\
 & & & & & & 2 & & & & & &
\end{array}$$

$$F_4 \qquad 1 \; - \; 2 \; => = \; 3 \; - \; 4$$

$$G_2 \qquad 1 \; \equiv > \equiv \; 2$$

where each node i represents a simple root α_i. This is the labelling of Bourbaki [13, p. 250], except for G_2, where α_1 and α_2 are interchanged.

Let $G = G(q)$ be an exceptional group of Lie type over $\mathbb{F}_q$; we exclude Suzuki and Ree groups. The root system of $G(q)$ is described in [20, Chapter 3]; if $G(q)$ is of twisted type, then we use the twisted root system of [20, Chapter 13]. For a long root α in the root system, we denote by U_α the corresponding long root group, and a conjugate of $\langle U_{\pm\alpha} \rangle \cong SL_2(q)$ is a *long* SL_2 subgroup of $G(q)$. For a fixed isomorphism between $\langle U_{\pm\alpha} \rangle$ and $SL_2(q)$, we denote by $h_\alpha(c)$ the element of $\langle U_{\pm\alpha} \rangle$

corresponding to the matrix $\mathrm{diag}(c^{-1}, c)$; if α is a fundamental root α_i, then we may write $h_i(c)$. If $\alpha_1 \ldots, \alpha_l$ are fundamental roots and $c_1, \ldots, c_l$ are integers, then $h_{c_1 \ldots c_l}(\lambda) := h_1(\lambda^{c_1}) \cdots h_l(\lambda^{c_l})$.

An involution in a long SL_2 subgroup of $G(q)$ is a *root* involution. These involutions and their centralizers play a major role in our work. Proposition 2.3 lists the root involution centralizers; it appears in [33, 4.5] (for q odd) and [1] (for q even). A *subsystem* subgroup is one generated by root groups corresponding to roots in a closed subsystem of the root system of $G(q)$.

Proposition 2.3 *Let $G = G(q)$ be an exceptional group of Lie type over $\mathbb{F}_q$, and let t be a root involution. Let D be a subsystem subgroup of G as in the following table:*

G	$G_2(q)$	${}^3D_4(q)$	$F_4(q)$	$E_6^\epsilon(q)$	$E_7(q)$	$E_8(q)$
D	$A_1(q)$	$A_1(q^3)$	$C_3(q)$	$A_5^\epsilon(q)$	$D_6(q)$	$E_7(q)$

(i) *If q is odd, then $C_G(t)$ has a subgroup $SL_2(q)D$ of index at most 2; the factors $SL_2(q)$ and D commute (elementwise).*

(ii) *If q is even, then $C_G(t) = QD$, where Q is a normal 2-subgroup of $C_G(t)$.*

If the root system of $G(q)$ has roots of different lengths, then a *short* SL_2 subgroup is one generated by a pair of opposite short root subgroups of $G(q)$; if $G(q)$ is of untwisted type, then these are isomorphic to $SL_2(q)$, otherwise they are isomorphic to $SL_2(q^2)$, or $SL_2(q^3)$ for ${}^3D_4(q)$.

Let l be the rank of the root system of $G(q)$ and let $1, \ldots, l$ be the nodes of the Dynkin diagram. Let $K_1, \ldots, K_l$ be long (short) SL_2 subgroups of $G(q)$ which satisfy the following:

1. K_i is long (short) if and only if node i is a long (short) root;
2. if nodes i, j are not joined then K_i and K_j commute;
3. if nodes i, j are joined then $\langle K_i, K_j \rangle$ is the appropriate rank 2 group of Lie type: $A_2(q)$ or $A_2(q^2)$ if i, j are joined by a single bond; $B_2(q)$ or ${}^2A_3(q)$ if joined by a double bond; $G_2(q)$ or ${}^3D_4(q)$ if joined by a triple bond.

We call such $K_1, \ldots, K_l$ *basic* SL_2 subgroups of $G(q)$.

2.3 Centralizers of involutions

The centralizer of an involution in a black-box group having an order oracle can be constructed using an algorithm of Bray [14]; he proved the following.

Theorem 2.4 *If x is an involution in a group H, and w is an arbitrary element of H, then $[x, w]$ either has odd order $2k + 1$, in which case $w[x, w]^k$ commutes with x, or has even order $2k$, in which case both $[x, w]^k$ and $[x, w^{-1}]^k$ commute with x. If w is uniformly distributed among the elements of the group for which $[x, w]$ has odd order, then $w[x, w]^k$ is uniformly distributed among the elements of the centralizer of x.*

Thus if the odd order case occurs sufficiently often, then we can construct random elements of the involution centralizer in Monte Carlo polynomial time.

Parker & Wilson [52, Theorems 1-4] proved the following two results.

Theorem 2.5 *There is an absolute constant $c > 0$ such that if H is a finite simple group of Lie type of Lie rank r defined over a field of odd characteristic, and x is an involution in H, then the proportion of $h \in H$ such that $[x, h]$ has odd order is at least c/r.*

Theorem 2.6 *There is an absolute constant $c > 0$ such that if H is a finite simple group of Lie type of Lie rank r defined over a field of odd characteristic, and C is a conjugacy class of involutions in H, then the proportion of elements of H which power up to an element of C is at least c/r^3.*

By Theorem 2.6, an involution in a specified class of H can be constructed in polynomial time by searching for an element of even order and computing a suitable power. By Theorem 2.5, random elements of the centralizer of this involution can be constructed, and a bounded number of these generate the centralizer (see [46]).

We shall make frequent use of the following lemma, also proved by Parker & Wilson [52, Lemma 26].

Lemma 2.7 *Let H be a finite group of Lie type, T a maximal torus in H and let C be a conjugacy class of H. Assume that at least a proportion k of the regular semisimple elements of T power to a member of C. Then at least a proportion $k/|N_H(T) : T|$ of the elements of H power to an element of C.*

Liebeck & O'Brien [43] proved the following.

Theorem 2.8 *If H is a finite group of Lie type over a field of characteristic 2, and t is a root involution of H such that $C_H(t)$ is not soluble, then the proportion of $h \in H$ such that $[t, h]$ has odd order is at least $1/4$.*

Hence random elements of the centralizer of a root involution can be constructed in polynomial time, and a bounded number of these will generate the centralizer (see [43, Lemma 3.10]).

2.4 The Formula

Variations of the following lemma, sometimes known as the "Formula", have been used in algorithms for some years – see, for example, [48, Section 4.10]. A proof can be found in [29, 7.1].

Lemma 2.9 *Let $K = H \ltimes M$ where M has exponent 2. Suppose $h \in H$ has odd order and acts fixed point freely on M. If $k = am \in K$ where $a \in C_H(h)$ and $m \in M$, then $a = hk(hh^k)^{(|h|-1)/2}$.*

The lemma sometimes allows us to construct a complement to a normal 2-subgroup in a semidirect product. We apply it when $H = \langle h \rangle \times D$ for quasisimple D. Now the lemma enables us to construct random elements of H (namely, $hk(hh^k)^{(|h|-1)/2}$ for random $k \in K$). Since, by [46], D may be generated by two random elements, we can thus construct a generating set for D.

3 Probabilistic generation of certain groups

Our algorithms rely on various results on probabilistic generation; these we now present.

Proposition 3.1 *Let $G = D_4^\epsilon(q)$ with $\epsilon = \pm$ and $q > 2$ even, and let x be an element of order $q+1$ in a long SL_2 subgroup of G. For random $g \in G$, the probability that $\langle x, x^g \rangle = G$ is positive, and is at least $1 - c/q$, where c is an absolute constant.*

Proof. Let P be the probability that $\langle x, x^g \rangle = G$ for random $g \in G$. If $\langle x, x^g \rangle \neq G$, then $x, x^g \in M$ for some maximal subgroup M of G. Given a maximal subgroup M containing x, the probability that x^g lies in M is $|x^G \cap M|/|x^G|$. It is well-known (see [44, 2.5]) that

$$\frac{|x^G \cap M|}{|x^G|} = \frac{\mathrm{fix}_{G/M}(x)}{|G:M|}, \tag{1}$$

where $\mathrm{fix}_{G/M}(x)$ denotes the number of fixed points of x in the action of G on the cosets of M. Also, the number of conjugates of M containing x is $\mathrm{fix}_{G/M}(x)$. Hence, if $\mathcal{M}$ is a set of representatives of the conjugacy classes of maximal subgroups of G, then

$$1 - P \leq \sum_{M \in \mathcal{M}} \frac{\mathrm{fix}_{G/M}(x)^2}{|G:M|}. \tag{2}$$

The maximal subgroups of G are determined in [40] (for $\epsilon = +$) and are listed in [15, Tables 8.52–8.53] (for $\epsilon = -$). In Tables 1 and 2, we list those maximal subgroups M which contain a conjugate of x, together with the values of $\mathrm{fix}_{G/M}(x)$ and $|G:M|$. The notation is standard: P_i denotes a parabolic subgroup, the stabilizer of a totally singular i-space; and N_i^δ ($\delta = \pm$) is the stabilizer of a nonsingular subspace of dimension i and type δ. Note that we omit N_2^+ from the tables: if x, x^g are contained in N_2^+ then they lie in a subgroup of N_2^+ which is contained in P_1. In Table 1 we comment if a row covers 3 classes of maximal subgroups; in each case these are permuted by a triality automorphism of G.

M	$\mathrm{fix}_{G/M}(x)$	$\|G:M\|$	Comment
P_1	$(q+1)^2$	$\frac{(q^4-1)(q^3+1)}{q-1}$	3 classes of subgroups M
P_2	$3(q+1)$	$\frac{(q^6-1)(q^2+1)^2}{q-1}$	
N_1	$q(q^2-1)$	$q^3(q^4-1)$	3 classes of subgroups M
N_2^-	$\frac{1}{2}q(q-1)(q^2-q+2)$	$\frac{q^6(q^4-1)(q^3-1)}{2(q+1)}$	3 classes of subgroups M
$N_4^+.2$	$\frac{1}{4}q^3(q-1)^3$	$\frac{q^8(q^6-1)(q^2+1)^2}{4(q^2-1)}$	
$N_4^-.2$	$\frac{1}{4}q^3(q+1)(q^2-1)$	$\frac{1}{4}q^8(q^6-1)(q^2-1)$	3 classes of subgroups M

Table 1: Fixed points of x for $G = \Omega_8^+(q)$

The values of $\mathrm{fix}_{G/M}(x)$ given in the tables are calculated reasonably routinely; we give a sketch. Let G have natural module V_8. Regard x as acting on an orthogonal decomposition $V_8 = V_4 + V_4'$, where V_4, V_4' are non-degenerate subspaces of type O_4^ϵ and O_4^+ respectively; x acts trivially on V_4, and as an element in one of the $SL_2(q)$ factors of $\Omega_4^+(q) = SL_2(q) \otimes SL_2(q)$ on V_4'. For $M = P_1$ (or N_1), $\mathrm{fix}_{G/M}(x)$ is the

M	$\mathrm{fix}_{G/M}(x)$	$\lvert G:M\rvert$
P_1	q^2+1	$\frac{(q^4+1)(q^3-1)}{q-1}$
P_2	$q+1$	$\frac{(q^6-1)(q^4+1)}{q-1}$
P_3	$(q^2+1)(q+1)$	$(q^4+1)(q^3+1)(q^2+1)$
N_1	$q(q^2+1)$	$q^3(q^4+1)$
N_2^-	$\frac{1}{2}q^2(q^2+1)$	$\frac{q^6(q^4+1)(q^3+1)}{2(q+1)}$
N_4^+	$\frac{1}{2}q^3(q^2+1)(q-1)+1$	$\frac{q^8(q^6-1)(q^4+1)}{2(q^2-1)}$
$\Omega_4^-(q^2).2$	$\frac{1}{2}q^3(q^2-1)(q+1)$	$\frac{1}{2}q^8(q^6-1)(q^2-1)$
$U_3(q)$	$2(3,q+1)q^2(q^4-1)$	$(3,q+1)q^9(q^8-1)(q^3-1)$

Table 2: Fixed points of x for $G=\Omega_8^-(q)$

number of singular (or nonsingular) 1-spaces in V_4; for $M=P_2$, $\mathrm{fix}_{G/M}(x)$ is the sum of the numbers of singular 2-spaces fixed by x in V_4 and V_4'; and for $M=P_3$, the singular 3-spaces in V_8 fixed by x are spanned by one of the $q+1$ fixed 2-spaces in V_4' together with a fixed 1-space in V_4. For $M=N_2^-$, the 2-spaces of type O_2^- fixed by x either lie in V_4 or in V_4', and there are $q(q-1)$ of the latter, as can be seen using (1). Likewise, $N_4^{\pm}$-spaces in V_8 fixed by x are sums of fixed nonsingular 2-spaces in V_4 and V_4', and it is straight-forward to count these. Finally, the cases where $\epsilon=-$ and $M=\Omega_4^-(q^2).2$ or $U_3(q)$ are handled using (1). In the first case, $x^G\cap M$ is a class of elements of order $q+1$ in $\Omega_4^-(q^2)\cong L_2(q^4)$, so has size $q^4(q^4+1)$. The second case arises from the adjoint representation of $U_3(q)$, in which x acts as $\mathrm{diag}(\alpha,\alpha,\alpha^{-2})$ for some scalar α of order $q+1$ or its inverse. Hence $|x^G\cap M|=2|SU_3(q):GU_2(q)|=2q^2(q^2-q+1)$, from which $\mathrm{fix}_{G/M}(x)$ follows using (1).

The lower bound $1-c/q$ in the statement of the proposition follows from the information in the tables together with (2). These also imply that $1-P$ is less than 1 for $q\geq 8$, giving the positivity statement for these values of q. For $q=4$ we can verify computationally that G is generated by two conjugates of x. ∎

For $q=2$ the probability in the previous proposition remains positive for $\epsilon=-$, but is zero for $\epsilon=+$.

Proposition 3.2 *Let G be one of $F_4(q),E_6^\epsilon(q),E_7(q)$ or $E_8(q)$ with q even, and let x be an element of order $q+1$ in a long SL_2 subgroup of G. For random $g\in G$, the probability that $\langle x,x^g\rangle$ is a subsystem subgroup $D_4^\epsilon(q)$ (for some $\epsilon\in\{+,-\}$) is positive, and is at least $1/6-c/q$, where c is an absolute constant.*

Proof. That the probability is positive follows immediately from Proposition 3.1 (and the ensuing remark for the case $q=2$). Let $D\cong D_4^\epsilon(q)$ be a fixed subsystem subgroup of G which contains a long SL_2 subgroup containing x, and define

$$\Delta=\{D^g : g\in C_G(x)\}.$$

Observe that $|\Delta|=|C_G(x):C_G(x)\cap N_G(D)|$ since $C_G(x)$ acts transitively on Δ.

We consider first the case where $\epsilon = +$. Here $N_G(D) = D.S_3$, $DT_2.S_3$, $DA_1(q)^3.S_3$ or $DD_4(q).S_3$ according as G is of type F_4, E_6^ϵ, E_7 or E_8, where T_2 denotes a rank 2 torus (see [45, Table 5.1]). The table below gives $C_G(x)$, $C_G(x) \cap N_G(D)$ and $|\Delta|$.

G	$C_G(x)$	$C_G(x) \cap N_G(D)$	$\lvert\Delta\rvert \sim$
$F_4(q)$	$\langle x\rangle C_3(q)$	$(\langle x\rangle A_1(q)^3).S_3$	$q^{12}/6$
$E_6^\pm(q)$	$\langle x\rangle A_5^\pm(q)$	$(\langle x\rangle A_1(q)^3 T_2).S_3$	$q^{24}/6$
$E_7(q)$	$\langle x\rangle D_6(q)$	$(\langle x\rangle A_1(q)^6).S_3$	$q^{48}/6$
$E_8(q)$	$\langle x\rangle E_7(q)$	$(\langle x\rangle D_4(q) A_1(q)^3).S_3$	$q^{96}/6$

The number of pairs (x^g, E) with $x^g \in E \in \Delta$ is of the order of $|\Delta| \cdot |D : (q+1)A_1(q)^3| \sim |\Delta| q^{18}$. Given E, the proportion of conjugates $x^g \in E$ such that $\langle x, x^g\rangle = E$ is at least $1 - c/q$ by Proposition 3.1. Clearly E is the unique member of Δ containing such x^g. Hence the number of conjugates x^g such that $\langle x, x^g\rangle$ is a member of Δ is at least $(1 - c/q)|\Delta| q^{18}$. The number of conjugates of x in G is $|G : C_G(x)|$, where $C_G(x)$ is as in the above table. Hence the probability that $\langle x, x^g\rangle$ is a member of Δ is at least

$$\frac{(1 - \frac{c}{q})|\Delta| q^{18}}{|G : C_G(x)|} \geq \frac{1}{6} - \frac{c'}{q}.$$

This completes the proof for $\epsilon = +$. The proof for $\epsilon = -$ is similar. ■

Proposition 3.3 *Let $G = G_2(q)$ with $q > 2$ even; let A_1 and $\tilde{A}_1$ denote commuting $SL_2(q)$ subgroups of G generated by long and short root groups respectively; let x, y be elements of order 3 in $\tilde{A}_1, A_1$ respectively; and let t be an involution in A_1.*

(i) *$C_G(x) \cong SL_3^\epsilon(q)$ and $C_G(y) = (q - \epsilon) \times \tilde{A}_1$, where $q \equiv \epsilon \bmod 3$.*

(ii) *For random $g \in G$, the probability that $\langle x, x^g\rangle$ is a conjugate of $\tilde{A}_1$ is positive, and is at least $1 - c_1/q$ where c_1 is an absolute constant.*

(iii) *For random $g \in G$, the probability that $\langle y, y^g\rangle$ is a conjugate of A_1 is $\frac{1}{q^4(q^4+q^2+1)}$.*

(iv) *For random $g \in G$, the probability that $\langle A_1, t^g\rangle \cong SL_3(q)$ is positive, and is at least $1/2 - c_2/q$ where c_2 is an absolute constant.*

Proof. (i) If L denotes the Lie algebra of type G_2, then

$$L \downarrow A_1\tilde{A}_1 = L(A_1\tilde{A}_1) \oplus (V(1) \otimes V(3)),$$

where $V(i)$ denotes the irreducible module of high weight i (see, for example, [47, 11.12(ii)]). It follows that $C_L(x)$, $C_L(y)$ have dimensions 8 and 6 respectively, so the centralizers of x and y in the algebraic group G_2 are connected reductive subgroups of types A_2 and T_1A_1.

(ii) This is similar to the proof of Proposition 3.2. Define $\Delta = \{\tilde{A}_1^g : g \in C_G(x)\}$. Then

$$|\Delta| = |C_G(x) : C_G(x) \cap N_G(\tilde{A}_1)| = |SL_3^\epsilon(q) : A_1 \cdot (q - \epsilon)| \sim q^4.$$

The number of pairs (x^g, E) with $x^g \in E \in \Delta$ is of the order of $|\Delta| \cdot |\tilde{A}_1 : (q - \epsilon)| \sim q^6$. Arguing as in Proposition 3.1, we see that, given E, the proportion of conjugates $x^g \in E$ such that $\langle x, x^g\rangle = E$ is at least $1 - c/q$. Clearly E is the unique member of Δ containing such x^g. Hence the number of conjugates x^g such that $\langle x, x^g\rangle$ is a member of Δ is at least $(1-c/q)q^6$, so the probability that $\langle x, x^g\rangle$ is a member of Δ is at least

$$\frac{(1-\frac{c}{q})q^6}{|G:C_G(x)|} \geq 1-\frac{c'}{q}.$$

The positivity statement in (ii) follows from the fact that $\tilde{A}_1 \cong SL_2(q)$ can be generated by two conjugates of x, which can be proved using (2). Indeed, let P be the probability that $\langle x, x^g\rangle = \tilde{A}_1$ for random $g \in \tilde{A}_1$. The maximal subgroups of $\tilde{A}_1$ containing x are $N := N_{\tilde{A}_1}(\langle x\rangle) \cong D_{2(q-\epsilon)}$ ($\epsilon = \pm 1$) and conjugates of $SL_2(q_0)$ for maximal subfields $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. Observe that $\mathrm{fix}_{\tilde{A}_1/N}(x) = 1$. If $M = SL_2(q_0)$ then $x^{\tilde{A}_1} \cap M = x^M$, so

$$\mathrm{fix}_{\tilde{A}_1/M}(x) = \frac{|\tilde{A}_1 : M|\,|x^{\tilde{A}_1} \cap M|}{|x^{\tilde{A}_1}|} = \frac{|x^M|}{|x^{\tilde{A}_1}|} = \frac{q-\epsilon}{q_0-\epsilon_0},$$

where $\epsilon_0 = \pm 1$ is such that $q_0 \equiv \epsilon_0 \bmod 3$. Hence by (2)

$$1-P \leq \frac{2}{q(q+\epsilon)} + \sum_{q_0} \left(\frac{q-\epsilon}{q_0-\epsilon_0}\right)^2 \frac{q_0(q_0^2-1)}{q(q^2-1)},$$

which is less than 1.

(iii) If A_1^h is a conjugate of A_1 containing y, then $y, y^{h^{-1}} \in A_1$, so there exists $a \in A_1$ such that $y^{h^{-1}} = y^a$. Then $ah \in C_G(y)$ which is contained in $A_1\tilde{A}_1$ by (i), so $A_1^h = A_1$. In other words, the only conjugate of A_1 containing y is A_1. Thus the probability in (ii) is $|y^G \cap A_1|/|y^G|$. The conclusion follows.

(iv) This is similar to the proof of (ii). Let S be a subsystem subgroup $SL_3(q)$ containing A_1, and let $\Delta = \{S^g : g \in \tilde{A}_1\}$. Then $|\Delta| = |\tilde{A}_1 : \tilde{A}_1 \cap N_G(S)|$ which is at most $|\tilde{A}_1 : (q+1).2| \sim q^2/2$. The number of pairs (t^g, E) with $t^g \in E \in \Delta$ is of the order of $|\Delta|q^4 \sim q^6/2$, and a proportion of at least $1-c/q$ of these satisfy $\langle A_1, t^g\rangle = E$. Since $|t^G| \sim q^6$, the lower bound in the conclusion follows. The positivity statement follows from the next proposition. ■

Proposition 3.4 *Let $G = {}^3D_4(q)$ with q even, and let A be a long $SL_2(q)$ subgroup of G. Let x and t be elements of order $q+1$ and 2 in A, respectively. For random $g \in G$, the probability that $\langle x, t^g\rangle$ is a subsystem subgroup $SL_3(q)$ is positive, and is at least $1-c/q$, where c is an absolute constant.*

Proof. Let S be a subsystem $SL_3(q)$ containing A, and let $\Delta = \{S^g : g \in C_G(x)\}$. Note that $C_G(x) = \langle x\rangle SL_2(q^3)$ and $|\Delta| = |SL_2(q^3) : (q^3+1)| \sim q^6$. The number of pairs (t^g, E) with $t^g \in E \in \Delta$ is of the order of q^{10}, and also $|t^G| \sim q^{10}$. The lower bound follows as in the previous propositions.

For the positivity statement, let S be a subsystem subgroup $SL_3(q)$ containing x. The maximal subgroups of S appear in [15, Tables 8.3–8.4], from which we deduce that x lies in just two maximal subgroups P_1, P_2, stabilizers of 1- and 2-spaces, respectively. These have structure $(\mathbb{F}_q^2).(SL_2(q) \times (q-1))$, and each contains q^3-1 involutions. Since the total number of involutions in S is $(q^3-1)(q+1)$, there is an involution t such that $S = \langle x, t\rangle$, as required. ■

4 Basic SL_2 subgroups in $SL_3(q)$ and $SL_6(q)$, q odd

Recall the definition of basic SL_2 subgroups in Section 2.2. As components for our subsequent work, we require algorithms to construct two basic SL_2 subgroups in a given $SL_3(q)/Z$, and five basic SL_2 subgroups in a given $SL_6(q)/Z$; here q is odd and Z is a central subgroup.

In these and subsequent algorithms, we assume that our input group G is described by a collection of generators in $GL_d(F)$ for some field F of the same characteristic as $\mathbb{F}_q$.

4.1 Algorithm for $SL_3(q)$

Let G be isomorphic to $SL_3(q)/Z$ with q odd and Z a central subgroup. The algorithm to construct two basic SL_2 subgroups in G is the following.

1. Find an involution $t_1 \in G$ by random search.
2. Construct $C_G(t_1)$ and $K_1 = C_G(t_1)' \cong SL_2(q)$.
3. Find an involution $t_2 \in C_G(t_1)$ which does not commute with K_1, and compute $K_2 = C_G(t_2)' \cong SL_2(q)$.

Now K_1 and K_2 are the required basic SL_2 subgroups of G.

Lemma 4.1 *The algorithm is Monte Carlo, has probability greater than a positive absolute constant (independent of q) of finding the required involutions, and runs in polynomial time.*

Proof. That we can both construct the involution t_1 and its centralizer with positive probability independent of q follows from Section 2.3. Now consider the second involution t_2. There is a maximal torus T of order $(q-1)^2/|Z|$ in $C := C_G(t_1)$, and at least $1/4$ of its regular elements power into the conjugacy class in C of a suitable involution t_2. The number of non-regular elements in T is at most $3(q-1)$, and $|N_C(T) : T| = 2$. By Lemma 2.7, the proportion of elements of C which power to a suitable involution t_2 is at least $\frac{1}{2}(\frac{1}{4} - \frac{3}{q-1})$. Therefore this is a lower bound for the probability of finding t_2 and is positive for every q since t_2 exists. In Section 2 we cite polynomial-time algorithms to perform the other tasks. ∎

4.2 Algorithm for $SL_6(q)$

Let G be isomorphic to $SL_6(q)/Z$, where q is odd and Z is a central subgroup. Involutions in G have centralizers with derived groups $SL_4(q) \circ SL_2(q)$, $SL_5(q)$, $SL_3(q) \circ SL_3(q)$ or $SL_3(q^2)/Z$. In our algorithm we consider only involutions having centralizers of the first type, and we call such a centralizer "good"; we can inspect orders of random elements in the involution centralizer to determine whether the centralizer is good.

The algorithm to construct five basic SL_2 subgroups in G is the following.

1. Find an involution $t_1 \in G$ with good centralizer, so $C_G(t_1)' = SL_4(q) \circ SL_2(q)$. Use KillFactor (see Section 2) to construct the factor $K_1 \cong SL_2(q)$ of this centralizer.
2. Find an involution $t_2 \in C_G(t_1)$ with good centralizer such that $[t_2, K_1] \neq 1$. Construct K_2, the $SL_2(q)$ factor of $C_G(t_2)'$.
3. Find an involution $t_3 \in C_G(t_1, t_2)$ with good centralizer such that $t_3 t \notin Z(G)$ for all $t \in \langle t_1, t_2 \rangle$, and $[t_3, K_1] = 1$, $[t_3, K_2] \neq 1$. Construct $K_3 = C_G(t_1, t_2, t_3)' \cong SL_2(q)$.
4. Find an involution $t_4 \in C_G(t_1, t_2, t_3)$ with good centralizer such that $t_4 t \notin Z(G)$ for all $t \in \langle t_1, t_2, t_3 \rangle$, and $[t_4, K_1] = [t_4, K_2] = 1$, $[t_4, K_3] \neq 1$. Construct K_4, the $SL_2(q)$ factor in $C_G(t_4)'$.
5. Let $t_5 = t_1 t_3$ and construct K_5, the $SL_2(q)$ factor in $C_G(t_5)'$.

With respect to a suitable basis of $V_6(q)$, $\pm t_1 = (-1, -1, 1, 1, 1, 1)$, $\pm t_2 = (1, -1, -1, 1, 1, 1)$, $\pm t_3 = (1, 1, -1, -1, 1, 1)$, and $\pm t_4 = (1, 1, 1, -1, -1, 1)$. Hence $K_1, \ldots, K_5$ are the required basic SL_2 subgroups.

Lemma 4.2 *The algorithm is Monte Carlo, has probability greater than a positive absolute constant of finding the required involutions, and runs in polynomial time.*

Proof. In Steps 2, 3 and 4 we use a maximal torus of order $(q-1)^5$ and Lemma 2.7 to estimate the probabilities of finding suitable involutions t_2, t_3, t_4. We illustrate the calculation for t_2. Write $t_1 = (-1, -1, 1, 1, 1, 1)$ as above, and let T consist of the diagonal matrices $(\alpha_1, \ldots, \alpha_6)$ where $\alpha_i \in \mathbb{F}_q^*$ and $\prod \alpha_i = 1$. Let Q be the subgroup of index 2 in $\mathbb{F}_q^*$. If we take $\alpha_2 \in \mathbb{F}_q^* \setminus Q$, $\alpha_1 \in Q$ and the other α_i arbitrary, then this element of T powers to a suitable involution t_2, and the number of such elements in T is $|T|/4$, of which at most $f(q)$ are non-regular, for some polynomial $f(q)$ of degree at most 4. Also $|N_C(T) : T| = 48$, where $C = C_G(t_1)$. Hence Lemma 2.7 shows that the proportion of elements of C powering to a suitable involution t_2 is at least $1/192 - c/q$ for some absolute constant c. ■

5 Basic SL_2 subgroups in $E_6(q)$, $E_7(q)$ and $E_8(q)$, q odd

Let G be isomorphic to one of the quasisimple groups of type $G(q) = E_6(q)$, $E_7(q)$ or $E_8(q)$ with q odd. We first present algorithms to construct basic SL_2 subgroups of G and later justify them. Each algorithm starts with the construction of an involution centralizer; these are described in Proposition 2.3.

As usual, we assume that our input group G is described by a collection of generators in $GL_d(F)$ for some field F of the same characteristic as $\mathbb{F}_q$.

5.1 $E_6(q)$, q odd

Let $G(q) = E_6(q)$, q odd.

1. Find an involution $t_0 \in G$ with $C_G(t_0)$ of type $A_1 A_5$. Construct the factors $K_0 \cong SL_2(q)$ and $D \cong A_5(q)$ of $C_G(t_0)'$.

2. Find an involution $t_2 \in C_G(t_0)$ such that $C_D(t_2)' = E \cong SL_3(q) \circ SL_3(q)$. Construct the two $SL_3(q)$ factors.
3. Construct basic SL_2 subgroups K_1, K_3 in the first factor $SL_3(q)$ of E, and K_5, K_6 in the second factor. Let $Z(K_i) = \langle t_i \rangle$.
4. Construct K_4, the $SL_2(q)$ factor of $C_D(t_1, t_6)' \cong SL_2(q)^3$ which centralizes K_1K_6. Now K_1, K_3, K_4, K_5, K_6 are basic SL_2 subgroups in $D \cong SL_6(q)$.
5. The centralizer $C_G(t_2)$ is of type A_1A_5; construct K_2, the $SL_2(q)$ factor of $C_G(t_2)$.

We now have the six basic SL_2 subgroups $K_1, \ldots, K_6$ in the E_6 Dynkin diagram:

$$\begin{array}{ccccccccc} K_1 & - & K_3 & - & K_4 & - & K_5 & - & K_6 \\ & & & & | & & & & \\ & & & & K_2 & & & & \end{array}$$

5.2 $E_7(q)$, q odd

This algorithm is similar to that for E_6.

1. Find an involution $t_0 \in G$ such that $C_G(t_0)$ is of type A_1D_6, and construct the factors $K_0 \cong SL_2(q)$ and $D \cong D_6(q)$ of $C_G(t_0)'$.
2. Find an involution $t_1 \in C_G(t_0)$ such that $C_D(t_1)' = E \cong A_5(q)$ and $C_G(t_1)$ is of type A_1D_6.
3. Construct basic SL_2 subgroups K_2, K_4, K_5, K_6, K_7 in E. Let t_i be the central involution in K_i.
4. The element t_1 is a root involution; construct the factor $K_1 \cong SL_2(q)$ of $C_G(t_1)$.
5. The element $t_3 = t_0t_5t_7$ is a root involution; construct the factor $K_3 \cong SL_2(q)$ of $C_G(t_3)$.

We now have the seven basic SL_2 subgroups $K_1, \ldots, K_7$ in the E_7 Dynkin diagram:

$$\begin{array}{ccccccccccc} K_1 & - & K_3 & - & K_4 & - & K_5 & - & K_6 & - & K_7 \\ & & & & | & & & & & & \\ & & & & K_2 & & & & & & \end{array}$$

5.3 $E_8(q)$, q odd

This algorithm is similar to that for E_6 and E_7.

1. Find an involution $t_0 \in G$ with $C_G(t_0)$ of type A_1E_7, and construct the factors $K_0 \cong SL_2(q)$, $D \cong E_7(q)$ of $C_G(t_0)'$.
2. Find an involution $t_8 \in C_G(t_0)$ such that $C_D(t_8)' = E \cong E_6(q)$.
3. Construct basic SL_2 subgroups $K_1, \ldots K_6$ in E.

4. The element t_8 is a root involution; construct the factor $K_8 \cong SL_2(q)$ of $C_G(t_8)$.
5. The element $t_7 = t_0t_2t_5$ is a root involution; construct the factor $K_7 \cong SL_2(q)$ of $C_G(t_7)$.

We now have the eight basic SL_2 subgroups $K_1, \dots, K_8$ in the E_8 Dynkin diagram:

$$\begin{array}{ccccccccccccc} K_1 & - & K_3 & - & K_4 & - & K_5 & - & K_6 & - & K_7 & - & K_8 \\ & & & & | & & & & & & & & \\ & & & & K_2 & & & & & & & & \end{array}$$

5.4 Justification

Proposition 5.1 *The algorithms for $E_6(q)$, $E_7(q)$ and $E_8(q)$ for odd q described above are Monte Carlo and run in polynomial time.*

Proof. We first prove the correctness of the algorithm for $E_6(q)$. In Step 1, finding the involution t_0 and constructing its centralizer is justified by the results of Section 2.3. The factors K_0 and D of $C_G(t_0)'$ are constructed using the algorithm KillFactor, referred to in Section 2.

Now consider Step 2 of the algorithm: find an involution $t_2 \in C_G(t_0)$ with centralizer containing $SL_3(q) \circ SL_3(q)$. We show that there is a positive lower bound (independent of q) for the probability of finding such an involution. This does not follow directly from Theorem 2.6, but follows from the method of its proof in [52]. Namely, there is a maximal torus of $C_G(t_0) \cong (SL_2(q) \circ A_5(q)).2$ of order $(q^3-1)^2$, and at least 1/8 of the elements of this torus power to involutions which have the desired centralizer structure; thus Lemma 2.7 gives the required conclusion. The centralizer can be computed by Section 2.3, and the $SL_3(q)$ factors extracted using KillFactor.

Step 3 of the algorithm is justified in Section 4. In Step 4, the construction of $C_D(t_1)$, and of the centralizer of t_6 within this group, is justified using Section 2.3. Observe that if $\langle t_4 \rangle = Z(K_4)$, then $t_4 = t_1t_6t_0$.

Step 5 requires a little more argument. Recall that $E \cong SL_3(q) \circ SL_3(q)$, a central product of two $SL_3(q)$ subsystem subgroups of G. From the subsystem A_2^3 of the E_6 root system, we see that $C_G(E)$ is isomorphic to $Z(E)SL_3(q)$, so t_2 and K_0 are contained in $C := C_G(E)' \cong SL_3(q)$. Hence t_2 is a root involution and we let K_2 be the $SL_2(q)$ factor of $C_G(t_2)$.

Finally, we show that $K_1, \dots, K_6$ pairwise generate either their direct product or $SL_3(q)$ according to their positions in the Dynkin diagram. Observe that $C_G(t_2)' = K_2S$ with $S \cong SL_6(q)$, and clearly $E < S$. Hence $K_2 \leq C_G(E)' = C$. Therefore K_2 centralizes each of K_1, K_3, K_5, K_6 and $\langle K_2, K_0 \rangle = C$. Hence K_0, K_2 and K_4 are contained in $C_G(K_1K_6)' \cong SL_4(q)$. The central involutions t_0, t_2, t_4 commute: t_2 commutes with t_4 since it commutes with t_0, t_1, t_6 and $t_4 = t_1t_6t_0$. Working in $SL_4(q)$ relative to a basis diagonalizing these three involutions, we see that $\langle K_2, K_4 \rangle \cong SL_3(q)$. This justifies the algorithm for $E_6(q)$.

For $E_7(q)$ the proof is similar, with the following additional observations. In Step 2, such an involution t_1 can be found with positive probability by the usual argument using Lemma 2.7 and a maximal torus of order $(q-1)(q^6-1)$ in $C_G(t_0)$. In Step 4, observe that K_1 commutes with E and $\langle K_0, K_1\rangle = C_G(E) \cong SL_3(q)$. For Step 5 and the Dynkin diagram generation of the K_i, observe the equation between toral elements $h_0(-1) = h_{2234321}(-1) = h_3(-1)h_5(-1)h_7(-1)$ (using the notation of Section 2.2). Since $t_i = h_i(-1)$, the involution in the centre of the final $SL_2(q)$ to complete the Dynkin diagram must be $t_3 = t_0t_5t_7$.

Finally consider $E_8(q)$. To justify Step 2 we take a maximal torus of order $(q\pm 1)^2(q^6+q^3+1)$ in $C_G(t_0)$ and use Lemma 2.7 as usual. In Step 5 the equation $h_0(-1) = h_{23465432}(-1) = h_2(-1)h_5(-1)h_7(-1)$ justifies our definition $t_7 = t_0t_2t_5$, and implies that the factor $K_7 \cong SL_2(q)$ of its centralizer completes the Dynkin diagram as claimed. ■

6 Basic SL_2 subgroups in $E_6(q)$, $E_7(q)$ and $E_8(q)$, q even

In this section we assume that G is described by a collection of generators in $GL_d(F)$, and G is quasisimple and isomorphic to one of $G(q) = E_6(q)$, $E_7(q)$ or $E_8(q)$, where F and $\mathbb{F}_q$ are both finite fields of characteristic 2, and $q > 2$. We first present algorithms to construct basic SL_2 subgroups of G, and later justify them.

Throughout, ω denotes a generator for the multiplicative group of $\mathbb{F}_q$.

6.1 $E_6(q)$, q even

Assume G is isomorphic to $E_6(q)$ with q even and $q > 2$.

1. Find $y \in G$ of order $(q+1)(q^5-1)/d$ where $d = (3, q-1)$, and define $x = y^{(q^5-1)/d}$.
2. Find $g \in G$ such that $X := \langle x, x^g\rangle$ is isomorphic to $D_4^\epsilon(q)$ (where $\epsilon = \pm$).
3. Construct an isomorphism ϕ from X to the standard copy of $D_4^\epsilon(q) = \Omega(V)$, where $V = V_8(q)$.
4. Find a standard basis $e_1, e_2, e_3, f_3, f_2, f_1$ for a non-degenerate subspace of V of type O_6^+. In the $SL_3(q)$ subgroup of $X\phi$ fixing $\langle e_1, e_2, e_3\rangle$ and $\langle f_1, f_2, f_3\rangle$, write down six elements acting on $\langle e_1, e_2, e_3\rangle$ as v_i, u_i^+, u_i^- $(i = 1, 2)$, where
$$v_1 = \begin{pmatrix} \omega^{-1} & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; u_1^+ = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; u_1^- = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$v_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^{-1} & 0 \\ 0 & 0 & \omega \end{pmatrix}, \; u_2^+ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \; u_2^- = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$
Abusing notation, write also v_i, u_i^+, u_i^- for the inverse images of these elements under ϕ. Define $K_0 = \langle v_1, u_1^+, u_1^-\rangle$ and $K_2 = \langle v_2, u_2^+, u_2^-\rangle$, basic SL_2 subgroups in X.
5. Construct the involution centralizer $C_G(u_1^+)$.
6. Apply Lemma 2.9 and the ensuing remark to $N := \langle C_G(u_1^+), v_1\rangle = Q(D\times\langle v_1\rangle)$, where $D = C_G(K_0) \cong A_5(q)$ and $Q = O_2(N)$. This constructs $C_N(v_1) = (Z(Q) \times D)\langle v_1\rangle$. Construct its second derived group, D.

7. Construct an isomorphism ψ from D to the standard copy of $SL_6(q) = SL(V)$ modulo a central subgroup Z of order either 1 or $(3, q-1)$. (Here $|Z| = 3$ if and only if $3|q-1$ and $Z(G) = 1$.)

8. Consider $v_2 \in K_2$. This element acts on D. Compute $T \in GL_6(q)$ such that $(g^{v_2})\psi = (g\psi)^T$ for all $g \in D$.

9. Diagonalise T to find a basis of V with respect to which $T = (\omega I_3, \omega^{-1} I_3)$. Let this basis be $x_1, \ldots x_6$.

10. For $1 \le i \le 5$, let a_i, b_i, c_i be the inverse images under ψ of matrices fixing x_j for $j \ne i, i+1$ and such that

$$\begin{aligned} a_i\psi &: x_i \to \omega^{-1}x_i,\ x_{i+1} \to \omega x_{i+1}, \\ b_i\psi &: x_i \to x_i + x_{i+1},\ x_{i+1} \to x_{i+1}, \\ c_i\psi &: x_i \to x_i,\ x_{i+1} \to x_i + x_{i+1}. \end{aligned}$$

Define $K_1 = \langle a_1, b_1, c_1 \rangle$, and for $i = 3, \ldots, 6$, define $K_i = \langle a_{i-1}, b_{i-1}, c_{i-1} \rangle$. Then K_1, K_3, K_4, K_5, K_6 are basic SL_2 subgroups in $D \cong SL_6(q)$.

We now have the six basic SL_2 subgroups $K_1, \ldots, K_6$ in the E_6 Dynkin diagram.

6.2 $E_7(q)$, q even

Assume G is isomorphic to $E_7(q)$ with q even and $q > 2$.

1-6. These steps are as for the E_6 algorithm, with the following modifications. In Step 1, we find an element y of order $(q+1)(q^5-1)$ and define $x = y^{q^5-1}$; the basic SL_2 subgroups constructed in Step 4 are K_0 and K_1; in Step 6, we construct $D = C_G(K_0)$ which is isomorphic to $D_6(q)$.

7. Construct an isomorphism ψ from D to the standard copy of $D_6(q) = \Omega_{12}^+(q) = \Omega(V)$, where V has associated bilinear form $(\ ,\ )$.

8. Consider $v_2 \in K_1$. This element acts on D. Compute $T \in GL_{12}(q)$ such that $(g^{v_2})\psi = (g\psi)^T$ for all $g \in D$.

9. Diagonalise T to find a basis of V with respect to which $T = (\omega I_6, \omega^{-1} I_6)$. Choose a basis $e_1, \ldots, e_6$ for the ω-eigenspace, and a basis $f_1, \ldots, f_6$ for the ω^{-1}-eigenspace such that $(e_i, f_j) = \delta_{ij}$.

10. For $1 \le i \le 5$, let $a_i, b_i, c_i \in D$ be the inverse images under ψ of the matrices in $\Omega(V)$ fixing e_j, f_j for $j \ne i, i+1$ and such that

$$\begin{aligned} a_i\psi &: e_i \to \omega^{-1}e_i, e_{i+1} \to \omega e_{i+1}, f_i \to \omega f_i, f_{i+1} \to \omega^{-1} f_{i+1}, \\ b_i\psi &: e_i \to e_i + e_{i+1}, e_{i+1} \to e_{i+1}, f_i \to f_i, f_{i+1} \to f_{i+1} + f_i, \\ c_i\psi &: e_i \to e_i, e_{i+1} \to e_i + e_{i+1}, f_i \to f_i + f_{i+1}, f_{i+1} \to f_{i+1}. \end{aligned}$$

Define $K_2 = \langle a_1, b_1, c_1 \rangle$, and for $i = 4, \ldots, 7$, define $K_i = \langle a_{i-2}, b_{i-2}, c_{i-2} \rangle$. Finally, define $K_3 = \langle a_6, b_6, c_6 \rangle$, where these elements are the inverse images of the matrices fixing e_j, f_j for $j \ge 3$ and such that

$$\begin{aligned} a_6\psi &: e_1 \to \omega e_1, e_2 \to \omega e_2, f_1 \to \omega^{-1} f_1, f_2 \to \omega^{-1} f_2, \\ b_6\psi &: e_1 \to e_1 + f_2, e_2 \to e_2 + f_1, f_1 \to f_1, f_2 \to f_2, \\ c_6\psi &: e_1 \to e_1, e_2 \to e_2, f_1 \to f_1 + e_2, f_2 \to f_2 + e_1. \end{aligned}$$

Then $K_2, K_3, K_4, K_5, K_6, K_7$ are basic SL_2 subgroups in $D \cong D_6(q)$.

We now have the seven basic SL_2 subgroups $K_1, \ldots, K_7$ in the E_7 Dynkin diagram.

6.3 $E_8(q)$, q even

Assume G is isomorphic to $E_8(q)$ with q even and $q > 2$.

1-6. These steps are as for the E_6 algorithm, with the following modifications. In Step 1, we find an element y of order $(q+1)(q^7-1)$ and define $x = y^{q^7-1}$; the basic SL_2 subgroups constructed in Step 4 are K_0 and K_8; in Step 6, we construct $D = C_G(K_0)$ which is isomorphic to $E_7(q)$.

7. Using the algorithm of Section 6.2, construct basic SL_2 subgroups $K_1, \ldots, K_7$ of D; label root elements of D as in Section 11.1. Construct an isomorphism ψ from D to the standard copy of $E_7(q)$ (a group of 56×56 matrices).

8. Consider $v_2 \in K_8$. This element acts on D. Compute $T \in D\psi$ such that $(g^{v_2})\psi = (g\psi)^T$ for all $g \in D$.

9. Compute $g \in D\psi$ such that $T^g = h_{2346543}(\lambda)$ for some $\lambda \in \mathbb{F}_q$. Replace K_8 by $K_8^{g\psi^{-1}}$.

We now have the eight basic SL_2 subgroups $K_1, \ldots, K_8$ in the E_8 Dynkin diagram.

6.4 Justification

Proposition 6.1 *The algorithms for $E_6(q)$, $E_7(q)$ and $E_8(q)$ for even q described above are Monte Carlo and run in polynomial time.*

Proof. In Step 1 of each algorithm, the justification for being able to find an element y of the specified order is standard. Consider, for example, the E_6 case: in the simple group $G := E_6(q)$ there is a cyclic maximal torus T of order $t := (q+1)(q^5-1)/d$ (see [37, §2]); the number of generators of T is $\phi(t) > t/c \log\log q$ where c is an absolute constant; hence the proportion of elements of order t in G is at least $1/(c \log\log q \cdot |N_G(T) : T|)$.

Observe that y lies in a maximal torus of G contained in a subsystem subgroup of type A_1A_5, A_1D_6 or A_1E_7 (see [37, §2]). Hence the power x of y must lie in a long $SL_2(q)$ subgroup of G. By Proposition 3.2, there is a positive lower bound independent of q for the probability that, for random $g \in G$, $\langle x, x^g \rangle$ is $D_4^\epsilon(q)$, a subsystem subgroup, as required for Step 2.

In Step 3, the construction of an isomorphism $X \to D_4^\epsilon(q)$ is justified by Theorem 2.2.

In Step 5, the element u_1^+ is a root involution so the construction of the involution centralizer $C_G(u_1^+)$ is justified by Theorem 2.8 and the ensuing remark. The structure of $C_G(u_1^+)$ is given in [1]: $C_G(u_1^+) = QD$, where $D = C_G(K_0) \cong A_5(q)$, $D_6(q)$ or $E_7(q)$, and $Q \cong q^{1+20}$, q^{1+32} or q^{1+56}, when G is of type E_6, E_7, E_8 respectively. The element v_1 normalizes $C_G(u_1^+)$ (which is $C_G(U)$ where U is a root group of K_0 containing u_1^+), centralizes D, and acts fixed point freely on $Q/Z(Q)$. Lemma 2.9 and the ensuing remark gives a construction of $(Z(Q) \times D)\langle v_1 \rangle$, as claimed in Step 6.

For $E_6(q)$ (or $E_7(q)$), the isomorphism in Step 7 from D to $A_5(q)$ (or $D_6(q)$) is justified by Theorem 2.2. The remaining steps ensure that v_2 acts as $h_2(\omega)$ (or $h_1(\omega)$) on D. Hence we choose the remaining $SL_2(q)$ subgroups in D to fit in with the subgroups K_0, K_2 (or K_0, K_1) already defined. That they pairwise generate the correct groups is established as in the proof of Proposition 5.1. In Step 8, the computation of the matrix T involves solving linear equations in the entries of T of the form $TA = BT$, where $A = (g^{v_2})\psi$, $B = g\psi$ for generators g of D; such systems of equations over $\mathbb{F}_q$ can be solved in polynomial time.

For the E_6 case, in $SL_3(q) \cong \langle K_2, K_4 \rangle$, K_2 and K_4 satisfy the correct picture of being the subgroups $(X, 1)$ and $(1, X)$, for $X \in SL_2(q)$, relative to some basis of the natural module $V = V_3(q)$: indeed, we constructed K_4 so that it is stabilized by $v_2 \in K_2$, which implies that v_2 stabilizes $C_V(K_4)$; thus $C_V(K_4) \subseteq [V, K_2]$ as required. Similar remarks apply in the E_7 case to $SL_3(q) \cong \langle K_1, K_3 \rangle$.

For $E_8(q)$, Steps 7–9 are more complex. In Step 7, we construct an isomorphism ψ from D to the standard copy of $E_7(q)$, a specific group of 56×56 matrices with standard generators $\hat{\mathcal{S}}$. Specifically, we find, as in Sections 13.1 a set $\mathcal{S}$ of standard generators of D which satisfies the reduced Curtis-Steinberg-Tits presentation of $E_7(q)$. For $x \in D$, we use the algorithm of [22], applied to the action of D on an absolutely irreducible composition factor of $V_d(F) \downarrow D$, to express x as a word $w(\mathcal{S})$; now ψ is defined to send x to $w(\hat{\mathcal{S}})$. That this step can be performed in polynomial time follows from this proposition (already proved for $E_7(q)$), together with the algorithms of Section 13.1 and [22].

Since $D = C_G(v_1)'$, the element v_2 acts on D, and induces an inner automorphism. In Step 8, we use linear algebra to find $T' \in GL_{56}(q)$ such that $(g^{v_2})\psi = (g\psi)^{T'}$ for all generators g of D. Some scalar multiple, T, of T' of determinant 1 must lie in $D\psi$; we use [22] to determine T.

The centralizer of T in $D\psi$ contains the image under ψ of $C_D(K_8) = C_G(K_0, K_8) \cong E_6(q)$. It follows that T is $D\psi$-conjugate to the toral element $h := h_{2346543}(\lambda)$ for some eigenvalue λ of T on $V_{56}(q)$. We compute $g \in D\psi$ conjugating T to h as follows.

1. Map $D\psi$ to its action on the Lie algebra L of type E_7 over $\mathbb{F}_q$. Call this map ϕ.

2. In each of $C_L(T\phi)$ and $C_L(h\phi)$, compute a split Cartan subalgebra by taking the centralizer of a random semisimple element. We claim that this is a split Cartan subalgebra with probability at least $c(1 - |\Phi|/q)$, where $\Phi := \Phi(E_6)$, the E_6 root system, and c is a positive absolute constant. To prove the claim, observe that
$$C_L(h\phi) = \langle z \rangle \oplus L(E_6) = H \oplus \sum_{\alpha \in \Phi(E_6)} L_\alpha$$
where z is semisimple, H is a split Cartan subalgebra of L, and the L_α are 1-dimensional root spaces for $\alpha \in \Phi$. If $v \in H$ satisfies $\alpha(v) \neq 0$ for all α, then $C_{C_L(h\phi)}(v) = H$ – that is, v is regular semisimple in $C_L(h\phi)$. The number of such $v \in H$ is at least $|H|(1 - |\Phi|/q)$, so the total number of

regular semisimple elements in $C_L(h\phi)$ is at least this number multiplied by the number of conjugates of H under the group $C_{D\psi\phi}(h\phi) \cong E_6(q) \circ (q-1)$. For large q, the stabilizer of H in the latter group is the normalizer of a Cartan torus, of order $(q-1)^7|W(E_6)|$. It follows that the number of regular semisimple elements in $C_L(h\phi)$ is at least

$$(|E_6(q) : (q-1)^6W(E_6)|) \cdot |H|(1 - |\Phi|/q),$$

which is at least $c(1 - |\Phi|/q) \cdot |C_L(h\phi)|$. This proves the claim. That we have found a split Cartan subalgebra can be verified in polynomial time by the argument of [24, 5.2].

3. Use the polynomial-time algorithm of [25, Theorem 1] to compute Chevalley bases B_T, B_h of L with respect to the Cartan subalgebras constructed in Step 2.

4. The element g' of $GL(L)$ conjugating B_T to B_h lies in $D\psi\phi$, and conjugates $T\phi$ to an element of a Cartan torus of $D\psi\phi$ containing $h\phi$.

5. Adjust g' by a computation in the Weyl group of $E_7(q)$ to an element g'' of $D\psi\phi$ conjugating $T\phi$ to $h\phi$. Take $g = g''\phi^{-1} \in D\psi$, as required.

For convenience, we now abuse notation and write g instead of $g\psi^{-1}$. To complete the proof, we argue that replacing K_8 by K_8^g provides a set $K_1, \ldots, K_8$ of basic SL_2 subgroups. For this, we need only to check that K_8^g centralizes $K_1, \ldots, K_6$ and $\langle K_7, K_8^g\rangle \cong SL_3(q)$. First observe that $v_2^g \in N_G(D) = DK_0$, so $v_2^g = hk_0$ with $k_0 \in K_0$. Also $C_G(K_8^g) = C_G(v_2^g)' \geq C_D(h)$, and this contains $K_1, \ldots, K_6$. Finally $C_G(K_7) = C_G(h_7)'$ where $h_7 = h_{\alpha_7}(\omega)$, so $C_G(K_7, K_8^g) = C_G(h_7, hk_0)'$. We claim that this centralizer is of type $E_6(q)$. Indeed, we can label the E_8 root system so that $k_0 = h_{\alpha_0}(\mu) = h_{23465432}(\mu)$ for some $\mu \in \mathbb{F}_q$; the fact that hk_0 is conjugate to v_2 forces $\mu = \lambda^{-1}$ or λ^{-3} (recall that $h = h_{2346543}(\lambda)$). Now considering h_7 and hk_0 as elements of the subsystem subgroup A_3 corresponding to the roots $\alpha_7, \alpha_8, \alpha_0$, we see that they lie in an A_2 subsystem, and hence centralize an E_6 subsystem in E_8. This proves the claim. Hence $\langle K_7, K_8^g\rangle \leq C_G(E_6(q)) \cong SL_3(q)$. Since $\langle K_7, K_8^g\rangle$ contains $\langle h_7, hk_0\rangle$, a toral subgroup of rank 2, it follows that $\langle K_7, K_8^g\rangle \cong SL_3(q)$ as required. ∎

7 Basic SL_2 subgroups in $F_4(q)$

7.1 $F_4(q)$, q odd

Let G be isomorphic to $F_4(q)$ with q odd. We present an algorithm to construct basic SL_2 subgroups in G.

1. Find an involution $t_0 \in G$ such that $C_G(t_0) \cong (SL_2(q) \circ Sp_6(q)).2$. Construct the factors $K_0 \cong SL_2(q)$ and $D \cong Sp_6(q)$ of the centralizer.

2. Find an involution $t_1 \in C_G(t_0)$ such that $C := C_D(t_1)' \cong SL_3(q)$.

3. Construct basic SL_2 subgroups K_3, K_4 in C. Let t_i be the involution in K_i.

4. Let $t_2 = t_0t_4$, a root involution; construct K_2, the $SL_2(q)$ factor in $C_G(t_2)$.

5. Also t_1 is a root involution; construct K_1, the $SL_2(q)$ factor of its centralizer.

We now have the four basic SL_2 subgroups K_1, K_2, K_3, K_4 in the Dynkin diagram:

$$K_1 \quad - \quad K_2 \quad =>= \quad K_3 \quad - \quad K_4$$

Proposition 7.1 *The above algorithm for $F_4(q)$ for odd q is Monte Carlo and runs in polynomial time.*

Proof. Finding the involutions and centralizers in Steps 1 and 2 is justified in the usual way using Lemma 2.7 and Section 2.3. For Step 4, with respect to a suitable basis for the natural 6-dimensional module for $D \cong Sp_6(q)$, $t_3 = (-1,-1,-1,-1,1,1)$, $t_4 = (-1,-1,1,1,-1,-1)$ and $t_0 = -I$; hence $t_2 = t_0t_4$ is a root involution.

Working in D, we see that $[K_2, K_4] = 1$ and $\langle K_2, K_3\rangle \cong Sp_4(q)$. Now K_0 and t_1 lie in $C_G(C)$, which is an $SL_3(q)$ generated by long root groups in G. Arguing as in Proposition 5.1 for $E_6(q)$, we deduce that t_1 is a root involution. If K_1 is the $SL_2(q)$ factor of its centralizer, then K_1 centralizes K_3 and K_4; also $\langle K_1, K_2\rangle = C_G(C) \cong SL_3(q)$. ■

7.2 $F_4(q)$, q even

Assume G is isomorphic to $F_4(q)$, where q is even and $q > 2$. We present an algorithm to construct basic SL_2 subgroups in G. Recall that ω denotes a generator of the multiplicative group of $\mathbb{F}_q$.

1-6. These steps are as for the E_6 algorithm in Section 6.1 with the following modifications. In Step 1, we find an element y of order $(q+1)(q^3-1)$ and define $x = y^{q^3-1}$; the basic SL_2 subgroups constructed in Step 4 are K_0 and K_1; in Step 6, we construct $D = C_G(K_0)$ which is isomorphic to $Sp_6(q)$.

7. Construct an isomorphism ψ from D to the standard copy of $Sp_6(q) = Sp(V)$.

8. Consider $v_2 \in K_1$. This element acts on D. Compute $T \in GL_6(q)$ such that $(g^{v_2})\psi = (g\psi)^T$ for all $g \in D$.

9. Diagonalise T to find a basis of V with respect to which $T = (\omega I_3, \omega^{-1}I_3)$. Choose a basis e_1, e_2, e_3 for the ω-eigenspace, and a basis f_1, f_2, f_3 for the ω^{-1}-eigenspace such that $(e_i, f_j) = \delta_{ij}$.

11. Define $a_0, b_0, c_0 \in D$ to be the inverse images under ψ of the elements in $Sp(V)$ fixing e_2, e_3, f_2, f_3 and acting on e_1, f_1 as follows:

$$\begin{aligned} a_0\psi &: e_1 \to \omega^{-1}e_1,\ f_1 \to \omega f_1, \\ b_0\psi &: e_1 \to e_1 + f_1,\ f_1 \to f_1, \\ c_0\psi &: e_1 \to e_1,\ f_1 \to e_1 + f_1. \end{aligned}$$

For $i = 1, 2$ let $a_i, b_i, c_i \in D$ be the inverse images under ψ of the matrices in $Sp(V)$ fixing e_j, f_j for $j \neq i, i+1$ and such that

$$\begin{aligned} a_i\psi &: e_i \to \omega^{-1}e_i, e_{i+1} \to \omega e_{i+1}, f_i \to \omega f_i, f_{i+1} \to \omega^{-1} f_{i+1}, \\ b_i\psi &: e_i \to e_i + e_{i+1}, e_{i+1} \to e_{i+1}, f_i \to f_i, f_{i+1} \to f_{i+1} + f_i, \\ c_i\psi &: e_i \to e_i, e_{i+1} \to e_i + e_{i+1}, f_i \to f_i + f_{i+1}, f_{i+1} \to f_{i+1}. \end{aligned}$$

Define $K_2 = \langle a_0, b_0, c_0 \rangle$, and for $i = 3, 4$, define $K_i = \langle a_{i-2}, b_{i-2}, c_{i-2} \rangle$. Then K_2, K_3 and K_4 are basic SL_2 subgroups in $D \cong Sp_6(q)$.

We now have the four basic SL_2 subgroups $K_1, \dots K_4$ in the F_4 Dynkin diagram.

Proposition 7.2 *The above algorithm for $F_4(q)$ for even q is Monte Carlo and runs in polynomial time.*

The proof is similar to that of Proposition 6.1.

8 Basic SL_2 subgroups in $G_2(q)$

8.1 $G_2(q)$, q odd

Let G be isomorphic to $G_2(q)$ with q odd. We present an algorithm to construct basic SL_2 subgroups in G.

1. Find an involution $t_0 \in G$ and compute its centralizer $C_G(t_0) \cong (SL_2(q) \circ SL_2(q)).2$. Construct S_1 and S_2, the two $SL_2(q)$ factors.
2. If $q \equiv 1 \bmod 4$, then find an involution $t_1 \neq t_0$ with $t_1 \in C_G(t_0)' = S_1S_2$; if $q \equiv 3 \bmod 4$, then find an involution $t_1 \in C_G(t_0) \backslash S_1S_2$.
3. Construct the two $SL_2(q)$ factors of $C_G(t_1)$. For one of them – call it S – either
   (a) $\langle S_1, S \rangle \cong SL_3(q)$, $\langle S_2, S \rangle = G$, or
   (b) $\langle S_2, S \rangle \cong SL_3(q)$, $\langle S_1, S \rangle = G$.

Assume (a) holds; relabel as $K_0 = S_1$, $K_1 = S$, $K_2 = S_2$. Now K_1 and K_2 are basic SL_2 subgroups, and we can place K_0, K_1, and K_2 in the extended G_2 Dynkin diagram as follows:

$$K_0 \quad \cdots \quad K_1 \quad \equiv\!>\!\equiv \quad K_2$$

Proposition 8.1 *The above algorithm for $G_2(q)$ for odd q is Monte Carlo and runs in polynomial time.*

Proof. Finding the involutions and centralizers in Steps 1 and 2 is justified as usual using Lemma 2.7 and Section 2.3. We next prove the claim in Step 3. First we show that conclusion (a) or (b) in that step holds for at least one involution in $C_G(t_0)$ satisfying the condition in Step 2 on being inside or outside the derived group. Let α_1, α_2 be fundamental roots with α_1 long, and let $\alpha_0 = 2\alpha_1 + 3\alpha_2$ be the highest root. We choose notation so that, interchanging S_1 and S_2 if necessary, $S_1 = \langle U_{\pm\alpha_0} \rangle$, $S_2 = \langle U_{\pm\alpha_2} \rangle$. Let t_1 be the involution in the centre of $\langle U_{\pm\alpha_1} \rangle$. If $q \equiv 1 \bmod 4$ then $t_1 \in C_G(t_0)'$ since it equals $h_0(i)h_2(-i) \in S_1S_2$. If $q \equiv 3 \bmod 4$ then $t_1 \notin C_G(t_0)'$: indeed, Bruhat decomposition implies that if $t_1 = s_1s_2$ with $s_i \in S_i$, then s_1 is in B or $Bn_{\alpha_0}B$, and s_2 is in B or $Bn_{\alpha_2}B$. Since $t_1 = h_1(-1) \in B$, the only possibility is that $s_1, s_2 \in B$, which leads to $h_1(-1) = u_{\alpha_0}(a)u_{\alpha_2}(a')h_0(b)h_2(b')$ for some $a, a', b, b' \in \mathbb{F}_q$. This is impossible since the only involution of the form $h_0(b)h_2(b')$ is $t_0 = h_2(-1)$. When $q \equiv 1 \bmod 4$, all non-central involutions in $C_G(t_0)' = S_1S_2$ are conjugate; when $q \equiv 3 \bmod 4$, all outer involutions in $C_G(t_0) \backslash C_G(t_0)'$ are conjugate. The claim in Step 3 follows. ■

8.2 $G_2(q)$, q even

Assume G is isomorphic to $G_2(q)$, where q is even and $q > 2$. We present an algorithm to construct basic SL_2 subgroups in G. Recall that ω denotes a generator of the multiplicative group of $\mathbb{F}_q$.

1. Find $y \in G$ of order $3(q - \epsilon)$, where $\epsilon = \pm 1$ and $q \not\equiv \epsilon \bmod 3$. Define $x = y^{q-\epsilon}$, an element of order 3.
2. If, after $O(1)$ random selections, we fail to find $g \in G$ with the property that $\langle x, x^g \rangle = K_2 \cong SL_2(q)$ then go to Step 1.
3. Construct an isomorphism ϕ from K_2 to the standard copy of $SL_2(q)$. In K_2, write down
$$u = \phi^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; v = \phi^{-1}\begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}.$$
4. If $q = 4$ then compute $K_0 := C_G(K_2)$. Otherwise, construct the involution centralizer $C_G(u)$, and $N := \langle C_G(u), v \rangle$; apply Lemma 2.9 to N to construct $K_0 = C_N(v)'$, a long SL_2 subgroup centralizing K_2; now $K_0K_2 = A_1(q)\tilde{A}_1(q)$ in G.
5. Construct an isomorphism from K_0 to the standard copy of $SL_2(q)$, and hence write down an involution $t \in K_0$.
6. Find $g \in G$ such that $\langle K_0, t^g \rangle = Y \cong SL_3(q)$.
7. Construct an isomorphism ϕ from Y to $SL_3(q) = SL(V)$. Compute $\langle v_1, v_2 \rangle = [V, K_0\phi]$ and $\langle v_3 \rangle = C_V(K_0\phi)$. Construct $K_1 \cong SL_2(q)$ in Y generated by the preimages under ϕ of generators for K_1: with respect to the basis v_1, v_2, v_3, these are
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^{-1} & 0 \\ 0 & 0 & \omega \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

We now have the three $SL_2(q)$ subgroups K_0, K_1, K_2 in the extended G_2 Dynkin diagram.

Proposition 8.2 *The above algorithm for $G_2(q)$ for even q is Monte Carlo and runs in polynomial time.*

Proof. In Step 1, y lies in a maximal torus of G contained in a subsystem subgroup $A_1(q)\tilde{A}_1(q)$, where the first factor is generated by long root subgroups of G and the second by short root subgroups. Hence the element $x = y^{q-\epsilon}$ of order 3 lies in $A_1(q)$ or $\tilde{A}_1(q)$. If $x \in \tilde{A}_1(q)$ then, by Proposition 3.3(ii), there is a positive lower bound independent of q for the probability that $\langle x, x^g \rangle$ is a conjugate of $\tilde{A}_1(q)$. If $x \in A_1(q)$ then Proposition 3.3(iii) shows that the probability that $\langle x, x^g \rangle$ is a conjugate of $A_1(q)$ is very small, justifying Step 2.

Consider Step 4. The construction of $C_G(u)$ is justified as in [43, Theorem 3.9], and the structure of this involution centralizer is given by [1]: $C_G(u) = QK_0$, where Q is abelian of order q^3. If $U = C_{K_2}(u)$, then $C_G(u) = C_G(U)$ and $N_G(U) =$

$\langle C_G(U), v\rangle \cong Q(K_0 \times \langle v\rangle))$. The element v acts fixed point freely on Q for $q > 4$, so we can apply Lemma 2.9.

Finally, Proposition 3.3 justifies Step 6: for random $g \in G$, there is a positive lower bound independent of q for the probability that $\langle K_0, t^g\rangle = Y \cong SL_3(q)$. ■

9 Basic SL_2 subgroups in ${}^2E_6(q)$

9.1 ${}^2E_6(q)$, q odd

Let G be isomorphic to the quasisimple group $G(q) = {}^2E_6(q)$ with q odd.

Since $G(q)$ is a twisted group, we construct basic SL_2 subgroups and root elements relative to the twisted root system, which is of type F_4 (see [33, 2.4]). Thus we aim to find SL_2 subgroups $K_1, \dots, K_4$ forming the diagram

$$K_1 \quad - \quad K_2 \quad =>= \quad K_3 \quad - \quad K_4$$

where $K_i \cong SL_2(q)$ for $i = 1, 2$; $K_i \cong SL_2(q^2)$ for $i = 3, 4$; $\langle K_1, K_2\rangle \cong SL_3(q)$; $\langle K_2, K_3\rangle \cong SU_4(q)$; and $\langle K_3, K_4\rangle \cong SL_3(q^2)$ or $PSL_3(q^2)$.

We present an algorithm to construct basic SL_2 subgroups in G.

1. Find an involution $t_0 \in G$ such that $C_G(t_0)$ is of type $A_1\,{}^2A_5$. Construct the factors $K_0 \cong SL_2(q)$ and $D \cong {}^2A_5(q)$ of the centralizer.
2. Find an involution $t_1 \in C_G(t_0)$ such that $C := C_D(t_1)' \cong SL_3(q^2)$ or $PSL_3(q^2)$.
3. Using Section 4.1, construct basic SL_2 subgroups K_3, K_4 in C. Let t_3, t_4 be the involutions in K_3, K_4.
4. Let $t_2 = t_0t_4$, a root involution; construct K_2, the $SL_2(q)$ factor in $C_G(t_2)$.
5. Also t_1 is a root involution; construct K_1, the $SL_2(q)$ factor in $C_G(t_1)$.

We now have the four basic SL_2 subgroups $K_1, \dots, K_4$ in the Dynkin diagram.

Proposition 9.1 *The above algorithm for ${}^2E_6(q)$ for odd q is Monte Carlo and runs in polynomial time.*

The proof is similar to that of Proposition 7.1.

9.2 ${}^2E_6(q)$, q even

Assume G is isomorphic to ${}^2E_6(q)$, where q is even and $q > 2$. We present an algorithm to construct basic SL_2 subgroups in G. Recall that ω denotes a generator of the multiplicative group of $\mathbb{F}_q$.

1-6. These steps are as for the E_6 algorithm in Section 6.1, with the following modifications. In Step 1, we find an element y of order $(q^6 - 1)/(3, q + 1)$ and define $x = y^{(q^6-1)/(q+1)}$; the long SL_2 subgroups constructed in Step 4 are K_0 and K_1; in Step 6, we construct $D = C_G(K_0)$ which is isomorphic to $SU_6(q)/Z$, where Z is a central subgroup of order 1 or $(3, q + 1)$.

7. Construct an isomorphism ψ from D to the standard copy of $SU_6(q)$ modulo a central subgroup.

8. Consider $v_2 \in K_1$. This element acts on D. Compute $T \in GL_6(q^2)$ such that $(g^{v_2})\psi = (g\psi)^T$ for all $g \in D$.

9. Diagonalise T to find a basis of V with respect to which $T = (\omega I_3, \omega^{-1} I_3)$. Choose a basis e_1, e_2, e_3 for the ω-eigenspace, and a basis f_1, f_2, f_3 for the ω^{-1}-eigenspace such that $(e_i, f_j) = \delta_{ij}$.

10. Now define three basic SL_2 subgroups in D as follows. Define $a_0, b_0, c_0 \in D$ to be the inverse images under ψ of the elements in $SU(V)$ fixing e_2, e_3, f_2, f_3 and acting on e_1, f_1 as follows:

$$\begin{aligned} a_0\psi &: e_1 \to \omega^{-1}e_1,\ f_1 \to \omega f_1, \\ b_0\psi &: e_1 \to e_1 + f_1,\ f_1 \to f_1, \\ c_0\psi &: e_1 \to e_1,\ f_1 \to e_1 + f_1. \end{aligned}$$

    For $i = 1, 2$ let $a_i, b_i, c_i \in D$ be the inverse images under ψ of the matrices in $SU(V)$ fixing e_j, f_j for $j \neq i, i+1$ and such that

$$\begin{aligned} a_i\psi &: e_i \to \nu^{-1}e_i, e_{i+1} \to \nu e_{i+1}, f_i \to \bar{\nu} f_i, f_{i+1} \to \bar{\nu}^{-1} f_{i+1}, \\ b_i\psi &: e_i \to e_i + e_{i+1}, e_{i+1} \to e_{i+1}, f_i \to f_i, f_{i+1} \to f_{i+1} + f_i, \\ c_i\psi &: e_i \to e_i, e_{i+1} \to e_i + e_{i+1}, f_i \to f_i + f_{i+1}, f_{i+1} \to f_{i+1}, \end{aligned}$$

    where ν is a primitive element of $\mathbb{F}_{q^2}$ and $\bar{\nu} = \nu^q$. Define $K_2 = \langle a_0, b_0, c_0 \rangle \cong SL_2(q)$, and for $i = 3, 4$, define $K_i = \langle a_{i-2}, b_{i-2}, c_{i-2} \rangle \cong SL_2(q^2)$. Then K_2, K_3 and K_4 are basic SL_2 subgroups in D.

We now have the four basic SL_2 subgroups $K_1, \dots, K_4$ in the Dynkin diagram.

Proposition 9.2 *The above algorithm for ${}^2E_6(q)$ for even q is Monte Carlo and runs in polynomial time.*

The proof is similar to that of Proposition 6.1.

10 Basic SL_2 subgroups in ${}^3D_4(q)$

10.1 ${}^3D_4(q)$, q odd

Let G be isomorphic to ${}^3D_4(q)$ with q odd. The twisted root system is of type G_2, and we must construct basic subgroups $SL_2(q)$ and $SL_2(q^3)$.

1. Find an involution $t_0 \in G$ and compute its centralizer $C_G(t_0) \cong (SL_2(q) \circ SL_2(q^3)).2$. Construct the two SL_2 factors $K_0 \cong SL_2(q)$ and $K_2 \cong SL_2(q^3)$.

2. If $q \equiv 1 \bmod 4$, then find an involution $t_1 \neq t_0$ with $t_1 \in C_G(t_0)' = K_0K_2$; if $q \equiv 3 \bmod 4$, then find an involution $t_1 \in C_G(t_0) \backslash K_0K_2$.

3. Construct the factor $K_1 \cong SL_2(q)$ of $C_G(t_1)$.

We now have the three basic SL_2 subgroups K_0, K_1, K_2 in the extended G_2 Dynkin diagram.

Proposition 10.1 *The above algorithm for ${}^3D_4(q)$ for odd q is Monte Carlo and runs in polynomial time.*

The proof is similar to that of Proposition 8.1.

10.2 ${}^3D_4(q)$, q even

Let G be isomorphic to ${}^3D_4(q)$ with q even. This case differs from the others: our algorithm to construct basic SL_2 subgroups employs an $O(q)$ search for an involution.

1. Find an element of even order in G that powers to a root involution $t \in G$.
2. Find $y \in G$ of order $(q+1)(q^3-1)$, and let $x = y^{q^3-1}$.
3. Find $g \in G$ such that $Y := \langle x, t^g \rangle \cong SL_3(q)$.
4. Construct an isomorphism from Y to the standard copy of $SL_3(q)$, and hence write down K_0 and K_1, basic SL_2 subgroups in Y. In K_0 write down the preimages of
$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, v = \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$
where ω denotes a generator of the multiplicative group of $\mathbb{F}_q$.
5. Construct $N := \langle C_G(u), v \rangle$.
6. For $q > 2$, use Lemma 2.9 to construct $K_2 := C_N(v)'' \cong SL_2(q^3)$. For $q = 2$ construct $K_2 := C_G(K_0)$.

We now have the three basic SL_2 subgroups K_0, K_1, K_2 in the extended G_2 Dynkin diagram.

Proposition 10.2 *The above algorithm for ${}^3D_4(q)$ for even q is Monte Carlo and has complexity $O(q)$.*

Proof. By [43, Theorem 3.8], the proportion of elements of even order in G that power to a root involution is at least $1/8q$. In Step 2, y lies in a subgroup $SL_2(q) \times SL_2(q^3)$, so x lies in the $SL_2(q)$ factor. In Step 3, by Proposition 3.4, there is a positive lower bound independent of q for the probability that $Y := \langle x, t^g \rangle \cong SL_3(q)$, a subsystem group. Step 5 yields $N = \langle C_G(u), v \rangle \cong Q.(SL_2(q^3) \times \langle v \rangle)$, where $Q \cong q^{1+8}$ and v acts fixed point freely on $Q/Z(Q)$. Hence Lemma 2.9 can be applied in Step 6. Since K_2 centralizes K_0, this completes the extended Dynkin diagram. ■

11 Labelling root and toral elements

Assume that G is described by a collection of generators in $GL_d(F)$, and G is isomorphic to a quasisimple exceptional group of type $G(q)$, where F and $\mathbb{F}_q$ are finite fields of the same characteristic, and $q > 2$. Assume also that $G(q)$ is neither a Suzuki nor a Ree group. In previous sections we have shown how to construct a family of basic SL_2 subgroups K_r of G as in the Dynkin diagram. We now show how to label root and toral elements in these subgroups consistently: we define root elements $x_{\pm r}(c_i)$ and toral elements $h_r(\omega)$ in each K_r, where c_i runs over an $\mathbb{F}_p$-basis of $\mathbb{F}_q$ or an extension field, and ω is a primitive element of the field. Our labelling algorithms are largely independent of the characteristic p.

We use these root and toral elements in Section 12 to compute the high weight of the representation of G on $V = V_d(F)$ when V is irreducible, and in Section 13 to construct standard generators of G.

We summarise the result of this section.

Proposition 11.1 *Let G be a subgroup of $GL_d(F)$, where F is a finite field of the same characteristic as $\mathbb{F}_q$, and assume that $G \cong G(q)$, a quasisimple group of exceptional Lie type over $\mathbb{F}_q$ for $q > 2$, excluding Suzuki and Ree groups. Assume also that generators are given for a family of basic SL_2 subgroups of G as in the Dynkin diagram. Subject to the availability of a discrete log oracle, there is a Las Vegas polynomial-time algorithm to label root and toral elements in each of the basic SL_2 subgroups.*

The algorithm is described and justified in the remainder of this section. We make frequent use of the algorithms to construct isomorphisms to various low-dimensional classical groups given by Theorem 2.2.

11.1 Labelling $E_6(q)$, $E_7(q)$ and $E_8(q)$

Here we assume that $G \cong G(q) = E_l(q)$, $l = 6, 7$ or 8. In Sections 5 and 6, we constructed basic SL_2 subgroups $K_1, \ldots, K_l$ of G.

1. Construct an isomorphism ϕ from $\langle K_1, K_3 \rangle$ to $SL_3(q) = SL(V)$. Choose a basis v_1, v_2, v_3 of V such that $v_1 \in C_V(K_3)$, $v_2 \in [V, K_1] \cap [V, K_3]$ and $v_3 \in C_V(K_1)$. Write all matrices with respect to this basis. Define

$$x_1(c_i) = \phi^{-1}\begin{pmatrix} 1 & c_i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad x_3(c_i) = \phi^{-1}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c_i \\ 0 & 0 & 1 \end{pmatrix},$$
$$x_{-1}(c_i) = \phi^{-1}\begin{pmatrix} 1 & 0 & 0 \\ c_i & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_{-3}(c_i) = \phi^{-1}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & c_i & 1 \end{pmatrix},$$

   where c_i runs over an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, and let

$$h_1(\omega) = \phi^{-1}(\omega^{-1}, \omega, 1), \ h_3(\omega) = \phi^{-1}(1, \omega^{-1}, \omega).$$

2. Construct an isomorphism ψ from $\langle K_3, K_4 \rangle$ to $SL_3(q) = SL(V)$. Choose a basis v_1, v_2, v_3 as in Step 1. Compute λ such that $h_3(\omega) = (\lambda^{-1}, \lambda, 1)$ and define $h_4(\omega) = (1, \lambda^{-1}, \lambda)$. Compute μ_i such that

$$x_{\pm 3}(c_i)\psi = \begin{pmatrix} 1 & \mu_i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ \mu_i & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and define

$$x_{\pm 4}(c_i) = \psi^{-1}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & \mu_i\\ 0 & 0 & 1\end{pmatrix}, \psi^{-1}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & \mu_i & 1\end{pmatrix},$$

taking the plus terms to be both upper or both lower triangular, and similarly for the minus terms.

3. Repeat Step 2 in turn for $\langle K_i, K_j\rangle$ with $(i,j) = (2,4), (4,5), (5,6), \ldots, (l-1,l)$.

The justification for the above labelling is largely self-evident. In Step 2, observe that the root elements $x_{\pm 3}(c_i)\psi$ are as claimed, since the root groups generated by these elements are normalized by $h_3(\omega)$.

11.2 Labelling $F_4(q)$

Here we assume that $G \cong G(q) = F_4(q)$. In Section 7 we constructed basic SL_2 subgroups $K_1, \ldots, K_4$ of G.

1. Working in $\langle K_1, K_2\rangle \cong SL_3(q)$, label $x_{\pm 1}(c_i), x_{\pm 2}(c_i)$ and $h_1(\omega), h_2(\omega)$ as in Step 1 of Section 11.1.

2. Construct an isomorphism ψ from $\langle K_2, K_3\rangle$ to $Sp_4(q) = Sp(V)$, and let $(\ ,\ )$ be the associated symplectic form on V. Let $U = C_V(K_2\psi)$, $W = [V, K_2\psi]$ and choose $e_1, f_1 \in V$ such that $e_1 \in C_W(x_{-2}(1)\psi)$, $f_1 \in C_W(x_2(1)\psi)$ and $(e_1, f_1) = 1$. Let $X = \langle e_1^{K_3\psi}\rangle$, $Y = \langle f_1^{K_3\psi}\rangle$, so that X and Y are 2-spaces with $V = X \oplus Y$. Choose $e_2 \in U \cap X$, $f_2 \in U \cap Y$ such that $(e_2, f_2) = 1$. Write all matrices relative to the basis e_1, e_2, f_2, f_1 of V.

3. Compute λ_i, μ_i such that

$$x_2(c_i)\psi = \begin{pmatrix}1 & 0 & 0 & \lambda_i\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}, x_{-2}(c_i)\psi = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ \mu_i & 0 & 0 & 1\end{pmatrix},$$

   and define

$$x_3(c_i) = \psi^{-1}\begin{pmatrix}1 & 0 & 0 & 0\\ \lambda_i & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & -\lambda_i & 1\end{pmatrix}, x_{-3}(c_i) = \psi^{-1}\begin{pmatrix}1 & \mu_i & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & -\mu_i\\ 0 & 0 & 0 & 1\end{pmatrix}.$$

   Compute λ such that $h_2(\omega)\psi = (\lambda^{-1}, 1, 1, \lambda)$, and define $h_3(\omega) = \psi^{-1}(\lambda, \lambda^{-1}, \lambda, \lambda^{-1})$.

4. Working in $\langle K_3, K_4\rangle \cong SL_3(q)$, label $x_{\pm 4}(c_i)$ and $h_4(\omega)$ as in Step 2 of Section 11.1.

Observe that the choice of basis in Step 2 ensures that the root elements $x_{\pm 2}(c_i)\psi$, $x_{\pm 3}(c_i)\psi$ are as claimed in Step 3.

11.3 Labelling $G_2(q)$ and ${}^3D_4(q)$

Here we assume that $G \cong G(q)$ is isomorphic to either $G_2(q)$ or ${}^3D_4(q)$. In Sections 8 and 10 we constructed basic SL_2 subgroups K_0, K_1, K_2 of G, with $K_0, K_1 \cong SL_2(q)$ and $K_2 \cong SL_2(q)$ or $SL_2(q^3)$.

1. Working in $\langle K_0, K_1\rangle \cong SL_3(q)$, label $x_{\pm 0}(c_i), x_{\pm 1}(c_i)$ and $h_0(\omega), h_1(\omega)$ as in Step 1 of Section 11.1.
2. Construct an isomorphism ψ from K_2 to $SL(V) = SL_2(q)$ or $SL_2(q^3)$. Compute $T \in SL(V)$ such that $(x^{h_1(\omega)})\psi = (x\psi)^T$ for all $x \in K_2$. Choose a basis of V consisting of eigenvectors of T, and write all matrices relative to this basis.
3. Let $q = p^a$. For $q > 3$ let $\Lambda = \{\omega^{\pm p^j} : 0 \le j \le a-1\}$, a subset of $\mathbb{F}_q$ of size $2\log_p q$. For $\lambda \in \Lambda$ define $d_2(\lambda) = \psi^{-1}(\lambda^{-1}, \lambda)$. Find λ such that $h_1(\omega)^2 d_2(\lambda) \in K_0$ and define
$$h_2(\omega) = d_2(\lambda).$$
4. If $q > 4$, then $\lambda = \omega^{\epsilon p^j}$ where $\epsilon = \pm 1$. Define
$$y_+ = \psi^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ y_- = \psi^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$
Find $\delta = \pm$ such that $\langle x_1(1)^{K_2}, y_\delta^{K_1}, K_1\rangle < G$. (For the opposite δ this subgroup is G.) Now $\delta = \epsilon$, except possibly for $q = 5$ or 9. For $q = 5$ or 9, if $\delta \ne \epsilon$, then replace $h_2(\omega)$ by $h_2(-\omega)$ or $h_2(-\omega)$ (respectively), ϵ by $-\epsilon$, and j by 0 or 1 (respectively).

   If $q = 4$, find δ as for $q > 4$; compute $i \in \{1, 2\}$ such that $\lambda = \omega^i$, and choose $j \in \{0, 1\}$ such that $\delta = (-1)^{i+j+1}$. If $q = 3$, set $\delta = \epsilon = +$ and $j = 0$.
5. Let c_i $(1 \le i \le a)$ be an $\mathbb{F}_p$-basis of E where $E = \mathbb{F}_q$ (or $\mathbb{F}_{q^3}$ for ${}^3D_4(q)$), and let ν be a primitive element of E (so $\nu = \omega$ if $E = \mathbb{F}_q$). If $\delta = +$, then define $h_2(\nu) = \psi^{-1}(\nu^{-p^j}, \nu^{p^j})$ and
$$x_2(c_i) = \psi^{-1}\begin{pmatrix} 1 & c_i^{p^j} \\ 0 & 1 \end{pmatrix},\ x_{-2}(c_i) = \psi^{-1}\begin{pmatrix} 1 & 0 \\ c_i^{p^j} & 1 \end{pmatrix}.$$
If $\delta = -$, then define $h_2(\nu) = \psi^{-1}(\nu^{p^j}, \nu^{-p^j})$ and
$$x_2(c_i) = \psi^{-1}\begin{pmatrix} 1 & 0 \\ c_i^{p^j} & 1 \end{pmatrix},\ x_{-2}(c_i) = \psi^{-1}\begin{pmatrix} 1 & c_i^{p^j} \\ 0 & 1 \end{pmatrix}.$$

We now justify the above labelling. In Step 2, the computation of the matrix T involves solving linear equations of the form $TA = BT$, where $A = (x^{h_1(\omega)})\psi$, $B = x\psi$, for generators x of K_2; this system can be solved in polynomial time. In Step 3, Λ is introduced because the isomorphism ψ could change eigenvalues of elements of K_2 by a field automorphism or inversion. We define $h_2(\omega)$ as in Step 3 to ensure that $h_1(\omega)^2 h_2(\omega) = h_{2\alpha+3\beta}(\omega) \in K_0 = \langle x_{\pm 0}(c) : c \in \mathbb{F}_q\rangle$. Membership of $h_1(\omega)^2 d_2(\lambda)$ in K_0 can be decided readily: $K_0 = C_G(K_2)$, so we simply check whether the given element commutes with the generators of K_2. For q odd, $h_1(-\omega)^2 h_2(-\omega) \in K_0$;

this causes a complication only for $q = 5$ or 9: if q is not one of these values, then $-\omega \notin \Lambda$, so Step 3 defines $h_2(\omega)$ uniquely. However, if $q = 5$ or 9 then $-\omega = \omega^{-1}$ or ω^{-3} respectively, so we may need to replace $h_2(\omega)$ by $h_2(-\omega)$, ϵ by $-\epsilon$, and j by 0 or 1, as indicated in Step 4. Similar observations apply for q even: non-uniqueness occurs only for $q = 4$ when $\omega^2 = \omega^{-1}$. In Step 4, the $y_\pm$ are elements of a root group normalized by $h_1(\omega)$ (this is the reason for Step 2), hence can be taken as root elements $x_{\pm 2}(1)$. The choice of δ ensures that y_δ is $x_{+2}(1)$ rather than the negative, hence justifying the parametrization of root elements in Step 5.

11.4 Labelling ${}^2E_6(q)$

Here we assume that $G \cong G(q) = {}^2E_6(q)$. In Section 9 we constructed basic SL_2 subgroups $K_1, \ldots, K_4$ of G, with $K_1, K_2 \cong SL_2(q)$ and $K_3, K_4 \cong SL_2(q^2)$.

1. Construct an isomorphism ϕ from $\langle K_2, K_3\rangle$ to $SU_4(q) = SU(V)$, let $(\ ,\ )$ be the associated hermitian form on V, and write $\bar{\alpha} = \alpha^q$ for $\alpha \in \mathbb{F}_{q^2}$. Let $U = C_V(K_2\phi)$, $W = [V, K_2\phi]$. Write $V \downarrow K_3\phi = X \oplus Y$ with X, Y 2-spaces. Choose $e_1 \in X \cap W$, $e_2 \in X \cap U$, $f_1 \in Y \cap W$, $f_2 \in Y \cap U$ such that $(e_1, f_1) = (e_2, f_2) = \lambda$, where λ is a fixed element of $\mathbb{F}_{q^2}$ such that $\lambda + \bar{\lambda} = 0$. Write all matrices with respect to the basis e_1, e_2, f_2, f_1 of V.

2. Let c_i $(1 \le i \le a)$ be a $\mathbb{F}_p$-basis of $\mathbb{F}_q$, and extend it to a basis d_i $(1 \le i \le 2a)$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$. Let ω, ν be primitive elements of $\mathbb{F}_q, \mathbb{F}_{q^2}$, respectively. For each i, define

$$x_2(c_i) = \phi^{-1}\begin{pmatrix} 1 & 0 & 0 & c_i \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad x_{-2}(c_i) = \phi^{-1}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c_i & 0 & 0 & 1 \end{pmatrix},$$
$$x_3(d_i) = \phi^{-1}\begin{pmatrix} 1 & 0 & 0 & 0 \\ d_i & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -\bar{d}_i & 1 \end{pmatrix}, \quad x_{-3}(d_i) = \phi^{-1}\begin{pmatrix} 1 & d_i & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\bar{d}_i \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

   and set $h_2(\omega) = \phi^{-1}(\omega^{-1}, 1, 1, \omega)$, $h_3(\nu) = \phi^{-1}(\nu, \nu^{-1}, \bar{\nu}, \bar{\nu}^{-1})$.

3. Working in $\langle K_1, K_2\rangle \cong SL_3(q)$, label $x_{\pm 1}(c_i)$ and $h_1(\omega)$ as in Step 2 of Section 11.1.

4. Working in $\langle K_3, K_4\rangle \cong SL_3(q^2)$ or $PSL_3(q^2)$, label $x_{\pm 4}(d_i)$ and $h_4(\nu)$ as in Step 2 of Section 11.1.

12 Determining the high weight of a representation

Let G be an absolutely irreducible subgroup of $GL_d(F)$ that is isomorphic to a quasisimple exceptional group $G(q)$ of Lie type over $\mathbb{F}_q$, where F and $\mathbb{F}_q$ have the same characteristic. Assume also that $G(q)$ is neither a Suzuki nor a Ree group. Write $V = V_d(F)$. In this section we describe a simple algorithm to compute the high weight of the absolutely irreducible FG-module V. That is, we compute the non-negative integers n_r $(1 \le r \le l)$ such that $V = V(\lambda)$, the irreducible module of high weight $\lambda = \sum_1^l n_r \lambda_r$, where l is the rank of the corresponding simple algebraic group and λ_r are the fundamental dominant weights. Unlike previous sections, the algorithm applies for all values of q including 2.

First consider the case where $G(q)$ is of untwisted type. The algorithm is the following. Using the work of previous sections, construct the root and toral elements $x_{\pm r}(c_i)$, $h_r(\omega)$ of G. Construct the maximal unipotent subgroup U generated by all the positive root elements $x_r(c_i)$. (For $F_4(2)$ additional generators are required – see Section 15.1.) A consequence of [27, Theorem 4.3(c)] is that $C_V(U)$ is a 1-dimensional space, spanned by a *maximal* vector v. Since the $h_r(\omega)$ normalize U, they fix $C_G(U)$. Thus, for each $r \in \{1, \ldots, l\}$, there exists $n_r \in \{0, \ldots, q-1\}$ such that $\omega^{n_r} \in F$ and

$$v^{h_r(\omega)} = \omega^{n_r} v.$$

These are the required integers n_r; to compute them, use a discrete log oracle in $\mathbb{F}_q$. The only ambiguity occurs when $v^{h_r(\omega)} = v$, in which case n_r can be 0 or $q-1$. To distinguish between them, compute the spin $\langle v^{K_r} \rangle$ of v under K_r: if this is a 1-dimensional (trivial) module for K_r, then $n_r = 0$; otherwise $n_r = q-1$.

Now consider the twisted groups. For ${}^2E_6(q)$, as in Section 11.4, compute the root elements $x_{\pm r}(c_i)$, and also the toral elements $h_1(\omega), h_2(\omega)$, $h_3(\nu), h_4(\nu)$, where ω and ν are primitive elements for $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ respectively. Construct the maximal unipotent group U generated by the positive root elements $x_r(c_i)$, and compute $C_V(U) = \langle v \rangle$. Using a discrete log oracle, find $0 \leq a, b, c, d, e, f \leq q-1$ such that

$$v^{h_1(\omega)} = \omega^a v,\ v^{h_2(\omega)} = \omega^b v,\ v^{h_3(\nu)} = \nu^{c+dq} v,\ v^{h_4(\nu)} = \nu^{e+fq} v.$$

The high weight of V relative to the E_6 Dynkin diagram is

$$\begin{array}{ccccc} e & c & b & d & f \\ & & a & & \end{array}$$

Similarly, for ${}^3D_4(q)$, compute $0 \leq a, b, c, d \leq q-1$ such that

$$v^{h_1(\omega)} = \omega^a v,\ v^{h_2(\nu)} = \nu^{b+cq+dq^2} v$$

where ν is now a primitive element for $\mathbb{F}_{q^3}$. The high weight of V relative to the D_4 Dynkin diagram is *bacd*. In both twisted cases, we distinguish between the possibilities 0 and $q-1$ as in the untwisted case.

Since the labelling of the root and toral elements is only determined up to an automorphism of G, the same is true of the high weight.

We have now justified the following result.

Proposition 12.1 *Subject to the availability of a discrete log oracle, the above algorithm determines in polynomial time the high weight of the absolutely irreducible FG-module V, up to a twist by a field or graph automorphism of G.*

13 Constructing the standard generators

Assume G is described by a collection of generators in $GL_d(F)$, where F is a finite field of the same characteristic as $\mathbb{F}_q$, and G is isomorphic to an exceptional group $G(q)$ of Lie type over $\mathbb{F}_q$. Assume also that $G(q)$ is neither a Suzuki nor a Ree group.

In previous sections we showed how to construct a family of basic SL_2 subgroups K_r of G as in the Dynkin diagram, and how to label root elements $x_{\pm r}(c_i)$ and toral elements $h_r(\omega)$ in each K_r.

In this section, we use commutators among these root elements to construct additional root elements in rank 2 subsystems, guided by the Chevalley commutator relations [20, 5.2.2]. The root elements constructed in G correspond to the generators of the reduced Curtis-Steinberg-Tits presentation for $G(q)$ as in [7, §4.2 and 6.1]: namely, the standard generators of G.

We list these presentations on standard generators explicitly in Appendix A. They are used to verify the correctness of the output of the algorithms: namely, the elements $x_{\pm r}(c_i)$ and $h_r(\omega)$.

We summarise the result of this section.

Proposition 13.1 *Let G be a subgroup of $GL_d(F)$, where F is a finite field of the same characteristic as $\mathbb{F}_q$ and $q > 2$, and assume that $G \cong G(q)$, a quasisimple group of exceptional Lie type over $\mathbb{F}_q$ which is neither a Suzuki nor a Ree group. Assume also that generators are given for a family of basic SL_2 subgroups of G as in the Dynkin diagram. Subject to the availability of a discrete log oracle, there is a Las Vegas polynomial-time algorithm to construct the standard generators of G.*

The proposition is justified in the following sections.

13.1 Standard generators of $E_6(q)$, $E_7(q)$ and $E_8(q)$

These are the most straight-forward cases. Let l be the rank of $G(q)$ (so $l = 6, 7$ or 8). From Proposition 11.1 we know fundamental root elements $x_{\pm r}(c_i) \in G$ for $1 \leq r \leq l$ and c_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. For each edge r, s in the Dynkin diagram with $r < s$, define additional root elements $x_{\pm rs}(c_i)$ by

$$x_{rs}(c_i) = [x_r(c_i), x_s(1)],\ x_{-rs}(c_i) = [x_{-r}(c_i), x_{-s}(-1)].$$

The reduced Curtis-Steinberg-Tits presentation has generators $x_{\pm r}(c_i)$, $x_{\pm rs}(c_i)$ for all relevant r, s, i, the relations being the Chevalley commutator relations among these elements, together with the relations expressing that all generators have order p. This presentation defines the simply connected group $E_l(q)$. We give an explicit version in Appendix A.1.

If we require a presentation for the simple group $G/Z(G)$, then an additional relation may be needed to kill the centre. This only applies for $l = 6$ or 7, as the simply connected group $E_8(q)$ is simple. We know the toral elements $h_r(\omega) \in K_r$. If $Z(G) \neq 1$, then $q - 1$ is divisible by 3 if $G(q) = E_6(q)$; or by 2 if $G(q) = E_7(q)$; and $Z(G) = \langle z \rangle$ where

$$z = \begin{cases} h_1(\lambda^2)h_3(\lambda)h_5(\lambda^2)h_6(\lambda), & \text{if } G(q) = E_6(q) \\ h_2(-1)h_5(-1)h_7(-1), & \text{if } G(q) = E_7(q) \end{cases}$$

and λ is a cube root of unity. Each $h_r(\omega)$ can be expressed in terms of the generators $x_{\pm r}(c_i)$ using the expression

$$h_r(\omega) = n_r(\omega^{-1})n_r(1)^{-1},$$

where $n_r(c) := x_r(c)x_{-r}(-c^{-1})x_r(c)$. Hence the relation $z = 1$, where z is as above, completes a presentation of the simple group $G/Z(G)$.

13.2 Standard generators of $F_4(q)$

Suppose $G(q) = F_4(q)$. From Proposition 11.1 we know fundamental root elements $x_{\pm r}(c_i) \in G$ for $1 \le r \le 4$ and c_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_q$. We define additional root elements as follows. For $1 \le r \le 4$, let

$$n_r = x_r(1)x_{-r}(-1)x_r(1).$$

Now define

$$\begin{array}{ll} x_{12}(c_i) = x_1(c_i)^{n_2}, & x_{-12}(c_i) = x_{-1}(c_i)^{n_2}, \\ x_{23}(c_i) = x_3(-c_i)^{n_2}, & x_{-23}(c_i) = x_{-3}(-c_i)^{n_2}, \\ x_{34}(c_i) = x_3(c_i)^{n_4}, & x_{-34}(c_i) = x_{-3}(c_i)^{n_4}, \\ x_{23^2}(c_i) = x_2(c_i)^{n_3}, & x_{-23^2}(c_i) = x_{-2}(c_i)^{n_3} \end{array}$$

(where 23^2 denotes the root $\alpha_2 + 2\alpha_3$ and so on). For the definition of $x_{\pm 23^2}(c_i)$ we have used the F_4 structure constants in [31].

This defines all the root elements in rank 2 subsystems. The reduced Curtis-Steinberg-Tits presentation of G defines the simple group $G \cong F_4(q)$, since this group is simply connected. We give an explicit version in Appendix A.2.

13.3 Standard generators of ${}^2E_6(q)$

Suppose $G(q) = {}^2E_6(q)$. This is very similar to the $F_4(q)$ case, except that for short roots we define root elements over $\mathbb{F}_{q^2}$ rather than $\mathbb{F}_q$. From Proposition 11.1 we know fundamental root elements $x_{\pm r}(c_i)$ for $r = 1, 2$ and $x_{\pm s}(d_i)$ for $s = 3, 4$, where c_i and d_i run over bases for $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ over $\mathbb{F}_p$, respectively. We define additional root elements $x_{\pm 12}(c_i)$, $x_{\pm 23}(d_i)$, $x_{\pm 34}(d_i)$, $x_{\pm 23^2}(c_i)$ using exactly the same equations as in Section 13.2 for $F_4(q)$.

This defines all the root elements in rank 2 subsystems. We give an explicit version of the reduced Curtis-Steinberg-Tits presentation of the simply connected version of G in Appendix A.3. This is a variant of the presentation given in [7, §6.1]. To get a presentation for the simple group $G/Z(G)$, we add the relation $z = 1$, where $z = h_3(\lambda)h_4(\lambda^2)$; the h_r are expressed in terms of $x_{\pm r}(c)$ as in Section 13.1, and λ is a cube root of unity.

13.4 Standard generators of $G_2(q)$

Suppose $G(q) = G_2(q)$. From Proposition 11.1 we know fundamental root elements $x_{\pm r}(c_i)$ in G for $r = 1, 2$. It is convenient to change notation at this point. Let α, β be fundamental roots in the G_2 root system with α long, β short, and write $x_{\pm 1}(c_i) = x_{\pm\alpha}(c_i)$, $x_{\pm 2}(c_i) = x_{\pm\beta}(c_i)$. We define additional root elements as follows. Let

$$n_\alpha = x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1), \;\; n_\beta = x_\beta(1)x_{-\beta}(-1)x_\beta(1).$$

Now define

$$\begin{array}{ll} x_{\alpha+\beta}(c_i) = x_\beta(-c_i)^{n_\alpha}, & x_{-\alpha-\beta}(c_i) = x_{-\beta}(-c_i)^{n_\alpha}, \\ x_{\alpha+2\beta}(c_i) = x_{\alpha+\beta}(c_i)^{n_\beta}, & x_{-\alpha-2\beta}(c_i) = x_{-\alpha-\beta}(c_i)^{n_\beta}, \\ x_{\alpha+3\beta}(c_i) = x_\alpha(c_i)^{n_\beta}, & x_{-\alpha-3\beta}(c_i) = x_{-\alpha}(c_i)^{n_\beta}, \\ x_{2\alpha+3\beta}(c_i) = x_{\alpha+3\beta}(-c_i)^{n_\alpha}, & x_{-2\alpha-3\beta}(c_i) = x_{-\alpha-3\beta}(-c_i)^{n_\alpha} \end{array}$$

This defines all the root elements. The reduced Curtis-Steinberg-Tits presentation of G defines the simple group $G \cong G_2(q)$, since this group is simply connected. We give an explicit version in Appendix A.4.

13.5 Standard generators of ${}^3D_4(q)$

Suppose $G(q) = {}^3D_4(q)$. This is similar to $G_2(q)$, except that for short roots we define root elements over $\mathbb{F}_{q^3}$ rather than $\mathbb{F}_q$. From Proposition 11.1 we know root elements $x_{\pm 1}(c_i)$ for c_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, and $x_{\pm 2}(d_i)$ for d_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_{q^3}$. As for $G_2(q)$ in Section 13.4, relabel these as $x_{\pm\alpha}(c_i)$, $x_{\pm\beta}(d_i)$ respectively. We define additional root elements $x_{\pm(\alpha+\beta)}(d_i)$, $x_{\pm(\alpha+2\beta)}(d_i)$, $x_{\pm(\alpha+3\beta)}(c_i)$, $x_{\pm(2\alpha+3\beta)}(c_i)$ using exactly the same equations as in Section 13.4 for $G_2(q)$.

This defines all the root elements. The reduced Curtis-Steinberg-Tits presentation of G defines the simple group $G \cong {}^3D_4(q)$, since this group is simply connected. We give an explicit version in Appendix A.5.

14 Completion of proof of Theorem 1

Theorem 1 is an immediate consequence of the results summarised in Section 2, and of the algorithms presented and justified in Sections 5–13. Babai *et al.* [7, Corollary 4.4] prove that the reduced Curtis-Steinberg-Tits presentation for a universal Chevalley group G of rank at least 2 has length $O(\log^3 |G|)$, so evaluation of the relations takes polynomial time. That the resulting constructive recognition algorithm is Las Vegas is established by verifying that the standard generators satisfy these presentations, which are given explicitly in Appendix A.

15 Algorithms for $q = 2$

Our algorithms to construct basic SL_2 subgroups fail when $q = 2$: the critical elements v_1 and v_2 constructed in Step 4 of Section 6.1 are now both the identity; the algorithms to construct standard generators in Section 13 also fail in some cases.

Since it is desirable to have practical recognition algorithms for exceptional groups over $\mathbb{F}_2$, we now provide such. We often exploit the fact that explicit computations can be performed readily in some of their subgroups using standard machinery; for details of such, see, for example, [34, Chapter 4]. We omit $G_2(2)$ since it is isomorphic to the almost simple classical group $U_3(3).2$.

15.1 $E_6(2), F_4(2)$ and ${}^2E_6(2)$

Assume G is isomorphic to one of $E_6(2), F_4(2)$ or ${}^2E_6(2)$.

1. Apply Steps 1-4 of Sections 6.1, 7.2 and 9.2. These construct basic SL_2 subgroups K_0, K_i where $i = 2$ for $E_6(2)$ and $i = 1$ for $F_4(2)$ and ${}^2E_6(2)$. They also find a root involution $u := u_1^+ \in K_0$.

2. Construct $C_G(u) = QD$, where $D = C_G(K_0)$ and Q is a normal 2-subgroup.

3. Construct Q, the soluble radical of $C_G(u)$. Now construct D as follows. Find involutions $s \in D \backslash Q$ such that $|Q : C_Q(s)| \leq 2^{12}$. Note that $C_Q(s)$ can be computed from the action of s on the vector space $Q/Z(Q)$ over $\mathbb{F}_2$. Search for sufficient Q-conjugates of s lying in $C_G(K_0)$ to generate D.

4. Find an involution $t \in D$ such that $\langle K_i, t\rangle \cong SL_3(2)$. Compute $D \cap \langle K_i, t\rangle \cong SL_2(2)$, and call it K_j, where $j = 4$ for $G \cong E_6(2)$ and $j = 2$ otherwise.

5. Construct $T := C_D(K_i)$ which is isomorphic to $SL_3(2)^2$, $SL_3(2)$ or $SL_3(4)$ for $G \cong E_6(2)$, $F_4(2)$ or ${}^2E_6(2)$ respectively.

6. Compute $C_T(K_j)$ which is isomorphic to $SL_2(2)^2$, $SL_2(2)$ or $SL_2(4)$ respectively. Define its SL_2 factors to be K_1K_6, K_4 or K_4, respectively.

7. Search in T for the remaining basic SL_2 subgroups $K_3K_5 \cong SL_2(2)^2$, $K_3 \cong SL_2(2)$ or $K_3 \cong SL_2(4)$. We now know all the basic SL_2 subgroups in G.

8. The labelling of fundamental root elements is carried out as in Section 11.

9. The construction of the standard generators is as in Sections 13.1, 13.2 and 13.3.

15.2 $E_7(2)$

Assume $G \cong E_7(2)$.

1. Construct K_0, K_1 and $D = C_G(K_0)$ as in the previous section. Find an involution $t \in D$ such that $\langle K_1, t\rangle \cong SL_3(2)$, and compute $K_3 = D \cap \langle K_1, t\rangle$.

2. Step 5 of the previous section is too expensive to apply in $D \cong \Omega^+_{12}(2)$. Instead, we first compute $C_D(K_3) \cong SL_2(2) \times \Omega^+_8(2)$. Name the direct factors as K_2 and E respectively.

3. Compute $C_E(K_1) \cong SL_4(2)$, and construct K_5, K_6, K_7, basic SL_2 subgroups in $C_E(K_1)$.

4. In $C_D(K_6, K_7) \cong SL_4(2)$, search for the remaining basic SL_2 subgroup $K_4 \cong SL_2(2)$, satisfying $[K_1, K_4] = 1$ and $\langle K_4, K_i\rangle \cong SL_3(2)$ for $i = 2, 3, 5$.

We now know all of the basic SL_2 subgroups in G. The labelling of fundamental root elements and the construction of standard generators is unchanged from Sections 11.1 and 13.1.

15.3 $E_8(2)$

An approach modelled on the previous algorithms is too expensive to apply to $E_8(2)$. Instead, we present a different algorithm which recognises the group only in its 248-dimensional adjoint representation.

Assume that $G \leq GL_{248}(F)$, where F is a finite field of characteristic 2, and $G \cong E_8(2)$.

1. Using [32], find a basis of $V = V_{248}(F)$ with respect to which the action of G is realised over $\mathbb{F}_2$. Replace V by the $\mathbb{F}_2$-span of this basis, and F by $\mathbb{F}_2$.

2. Construct K_0 and $D = C_G(K_0) \cong E_7(2)$ as in Steps 1-3 of Section 15.1.

3. Apply the algorithm of Section 15.2 to construct basic SL_2 subgroups and root elements $x_{\pm r}(1)$ $(1 \le r \le 7)$ in D. Let $x_{\pm 0}(1)$ be two involutions generating K_0.

4. Let $\hat{G}$ be the standard copy of $E_8(2)$ in $GL_{248}(2)$, with fundamental root element generators $\hat{x}_{\pm r}(1)$ $(1 \le r \le 8)$. Let $\hat{x}_{\pm 0}(1)$ be root elements in $\hat{G}$ corresponding to the longest root α_0 in the root system.

5. Compute all matrices $g \in GL_{248}(2)$ such that $x_{\pm r}(1)^g = \hat{x}_{\pm r}(1)$ for $0 \le r \le 7$. There are precisely two such matrices. To see this, observe that $\langle x_{\pm r}(1) : 0 \le r \le 7 \rangle = DK_0$, so any two such matrices g differ by an element of $C_{GL(V)}(DK_0)$. Now $V \downarrow DK_0 = W_1 \oplus W_2 \oplus W_3$, a sum of indecomposables of dimensions 2, 112 and 134. Here W_1 and W_2 are irreducible and W_3 is uniserial with socle series having irreducible factors of dimensions $1, 132, 1$. Let M be the maximal submodule of W_3, and let $\langle s \rangle$ be the socle of M. Then $\mathrm{Hom}_{DK_0}(V, V)$ has dimension 4, with basis $1, \pi_1, \pi_2, \phi$ where π_i is the projection $V \to W_i$ and ϕ sends $w_1 + w_2 + w_3$ to 0 if $w_3 \in M$ and to s if $w_3 \notin M$. The only invertible elements of this space are 1 and $1 + \phi$. Hence, as asserted, there are exactly two such matrices g. Call them g_1, g_2.

6. For $i = 1, 2$ define $x^{(i)}_{\pm 8} = \hat{x}_{\pm 8}(1)^{g_i^{-1}}$. Decide for which value of i the group $\langle D, x^{(i)}_{\pm 8} \rangle$ is isomorphic to $E_8(2)$; the other is a "large" subgroup of $GL_{248}(2)$ containing elements of order much larger than those of $E_8(2)$. For this value of i, define $x_{\pm 8}(1) = x^{(i)}_{\pm 8}$.

We have now labelled all fundamental root elements $x_{\pm r}(1)$ $(1 \le r \le 8)$ in G. The construction of the standard generators is unchanged from Section 13.

15.4 $^3D_4(2)$

Assume $G \cong {}^3D_4(2)$. Let α, β be fundamental long and short roots in the root system, as in Section 13.4.

1. Construct subgroups $K_0, K_1 \cong SL_2(2)$ and $K_2 \cong SL_2(8)$ as in Section 10.2.

2. Construct an isomorphism from K_2 to $SL_2(8)$. In K_2, define $x_\beta(c), x_{-\beta}(c)$ (for $c \in \mathbb{F}_8$) to be the preimages of $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ respectively.

3. Let $X_{\pm\beta} = \{x_{\pm\beta}(c) : c \in \mathbb{F}_8\}$. Find $g \in K_2$ and involutions $x_\epsilon \in K_1$ $(\epsilon = \pm)$ such that each of $\langle x_\epsilon^{K_2}, X^g_{\epsilon\beta}, K_1 \rangle$ is a proper subgroup of G. Define $x_{\pm\alpha}(1) = x_\pm$ and replace $x_{\pm\beta}(c)$ by $x_{\pm\beta}(c)^g$. Now we have labelled the fundamental root elements of G.

4. Construct the remaining standard generators of G as in Section 13.5.

16 Implementation and performance

We have implemented these algorithms in MAGMA. We use the product replacement algorithm [21] to generate random elements; our implementations of [14], [17], [26], [30], and [49]; and Brooksbank's implementations of his algorithm [19] for constructive recognition of $Sp_4(q)$.

The computations reported in Table 3 were carried out using MAGMA V2.19 on a 2.8 GHz processor. We list the CPU time t_1 in seconds taken to construct standard generators in a random conjugate of the standard copy of dimension d_1 of an exceptional group of type $G(q)$; sometimes, we list t_2, the time taken to perform the same task in an irreducible representation of dimension d_2. The time is averaged over three runs.

We use Taylor's implementation of [22,23] to write an element of $G(q)$ as a word in the standard generators. As one illustration, it takes 17 seconds to write an element of $E_8(5^2)$ as a word in its standard generators.

Group	d_1	t_1	d_2	t_2
$E_6(2^3)$	27	8	78	51
$E_6(5^2)$	27	15	78	119
$E_7(2^3)$	56	35	133	158
$E_7(5^2)$	56	53	133	301
$E_8(2^3)$	248	978	–	–
$E_8(5^2)$	248	520	–	–
$F_4(2)$	26	11	246	235
$F_4(2^3)$	26	14	246	607
$F_4(5^3)$	26	30	52	248
$G_2(2^3)$	6	1	14	2
$G_2(5^3)$	7	2	14	3
${}^2E_6(2^3)$	27	99	78	790
${}^2E_6(5^2)$	27	102	78	865
${}^3D_4(2^6)$	8	15	26	122
${}^3D_4(5^3)$	8	6	28	90

Table 3: Time to construct standard generators

A Reduced Curtis-Steinberg-Tits presentations

The Curtis-Steinberg-Tits presentations are well known; the reduced versions using only an $\mathbb{F}_p$-basis of the field $\mathbb{F}_q$ (and extensions) are described in [7]. Since we know of no explicit versions listing the constants in the Chevalley relations, which we need for our work, we include such here. The constants are calculated using [20, 5.2.2] together with the $N_{\alpha\beta}$ structure constants for the G_2 and F_4 Lie algebras from [31].

In all cases, the generators are the root elements we have constructed in Section 13, namely the elements $x_r(c_i)$ for roots r in subsystems spanned by two non-orthogonal fundamental roots, and elements c_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_q$ (or an extension field). In every case, the presentation contains the following relations:

$$\begin{aligned}&x_r(c_i)^p = 1,\\&[x_r(c_i), x_s(d_i)] = 1 \text{ if } r+s \text{ is not a root.}\end{aligned}$$

For $c = \sum k_i c_i \in \mathbb{F}_q$ (or an extension field) with $k_i \in \mathbb{F}_p$, we set $x_r(c) = \prod x_r(c_i)^{k_i}$.

We present the remaining relations for each type below.

A.1 Relations for $E_6(q), E_7(q), E_8(q)$

The relations for these types are simple: for each edge rs in the Dynkin diagram with $r < s$, and for c_i, d_i in the $\mathbb{F}_p$-basis of $\mathbb{F}_q$,

$$\begin{array}{ll}
(1) & [x_r(c_i), x_s(d_i)] = x_{rs}(c_i d_i)\\
(2) & [x_{-r}(c_i), x_{-s}(d_i)] = x_{-rs}(-c_i d_i)\\
(3) & [x_r(c_i), x_{-rs}(d_i)] = x_{-s}(-c_i d_i)\\
(4) & [x_s(c_i), x_{-rs}(d_i)] = x_{-r}(c_i d_i)\\
(5) & [x_{-r}(c_i), x_{rs}(d_i)] = x_s(c_i d_i)\\
(6) & [x_{-s}(c_i), x_{rs}(d_i)] = x_r(-c_i d_i)
\end{array}$$

A.2 Relations for $F_4(q)$

For the edges 12 and 34 in the Dynkin diagram of F_4 we have the relations (1)-(4) of the previous section. The remaining relations are the following:

$$\begin{array}{ll}
(1) & [x_2(c_i), x_3(d_i)] = x_{23}(c_i d_i) x_{23^2}(c_i d_i^2)\\
(2) & [x_2(c_i), x_{-23}(d_i)] = x_{-3}(-c_i d_i) x_{-23^2}(-c_i d_i^2)\\
(3) & [x_{-2}(c_i), x_{23}(d_i)] = x_3(c_i d_i) x_{23^2}(-c_i d_i^2)\\
(4) & [x_{-2}(c_i), x_{-3}(d_i)] = x_{-23}(-c_i d_i) x_{-23^2}(c_i d_i^2)\\
(5) & [x_{23^2}(c_i), x_{-3}(d_i)] = x_{23}(c_i d_i) x_2(c_i d_i^2)\\
(6) & [x_{23^2}(c_i), x_{-23}(d_i)] = x_3(-c_i d_i) x_{-2}(-c_i d_i^2)\\
(7) & [x_{-23^2}(c_i), x_{23}(d_i)] = x_{-3}(c_i d_i) x_2(-c_i d_i^2)\\
(8) & [x_{-23^2}(c_i), x_3(d_i)] = x_{-23}(-c_i d_i) x_{-2}(c_i d_i^2)\\
(9) & [x_{23}(c_i), x_3(d_i)] = x_{23^2}(2c_i d_i)\\
(10) & [x_{-23}(c_i), x_{-3}(d_i)] = x_{-23^2}(-2c_i d_i)\\
(11) & [x_{23}(c_i), x_{-3}(d_i)] = x_2(2c_i d_i)\\
(12) & [x_3(c_i), x_{-23}(d_i)] = x_{-2}(2c_i d_i)
\end{array}$$

A.3 Relations for ${}^2E_6(q)$

Here the Dynkin diagram is F_4. For the edge 12 we have relations (1)-(4) of Section A.1 with c_i, d_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, and for edge 34 we have these relations for c_i, d_i in an $\mathbb{F}_p$-basis of $\mathbb{F}_{q^2}$. The remaining relations are (1)-(12) in Appendix A.2 with the following adjustments:

(a) in relations (1)-(8), $c_i \in \mathbb{F}_q$, $d_i \in \mathbb{F}_{q^2}$, and in (9)-(12) $c_i, d_i \in \mathbb{F}_{q^2}$;

(b) in relations (1)-(4), $c_i d_i^2$ is replaced by $c_i d_i \overline{d}_i$ (where $\overline{d}_i = d_i^q$);

(c) in relations (5)-(8), $c_i d_i$ is replaced by $c_i \overline{d}_i$, and $c_i d_i^2$ is replaced by $c_i d_i \overline{d}_i$;

(d) in relations (9)-(10), $2c_id_i$ is replaced by $c_i\overline{d}_i + \overline{c}_id_i$;

(e) in relations (11)-(12), $2c_id_i$ is replaced by $c_id_i + \overline{c}_i\overline{d}_i$.

Note that this is a variant of the presentation described in [7, 6.1].

A.4 Relations for $G_2(q)$

As in Section 13.4, we let α, β be fundamental roots in the G_2 root system, and define root elements $x_r(c_i)$ for r one of the long roots $\pm\alpha$, $\pm(\alpha+3\beta)$, $\pm(2\alpha+3\beta)$, or one of the short roots $\pm\beta$, $\pm(\alpha+\beta)$, $\pm(\alpha+2\beta)$ and c_i in a $\mathbb{F}_p$-basis of $\mathbb{F}_q$. The relations are the following:

(1) $[x_\alpha(c_i), x_\beta(d_i)] = x_{\alpha+\beta}(c_id_i)x_{\alpha+2\beta}(-c_id_i^2)x_{\alpha+3\beta}(c_id_i^3)x_{2\alpha+3\beta}(c_i^2d_i^3)$
(2) $[x_\alpha(c_i), x_{-\alpha-\beta}(d_i)] = x_{-\beta}(-c_id_i)x_{-\alpha-2\beta}(c_id_i^2)x_{-2\alpha-3\beta}(c_id_i^3)x_{-\alpha-3\beta}(-c_i^2d_i^3)$
(3) $[x_{\alpha+3\beta}(c_i), x_{-\beta}(d_i)] = x_{\alpha+2\beta}(-c_id_i)x_{\alpha+\beta}(-c_id_i^2)x_\alpha(c_id_i^3)x_{2\alpha+3\beta}(-c_i^2d_i^3)$
(4) $[x_{\alpha+3\beta}(c_i), x_{-\alpha-2\beta}(d_i)] = x_\beta(c_id_i)x_{-\alpha-\beta}(-c_id_i^2)x_{-2\alpha-3\beta}(c_id_i^3)x_{-\alpha}(c_i^2d_i^3)$
(5) $[x_{2\alpha+3\beta}(c_i), x_{-\alpha-\beta}(d_i)] = x_{\alpha+2\beta}(-c_id_i)x_\beta(-c_id_i^2)x_{-\alpha}(-c_id_i^3)x_{\alpha+3\beta}(c_i^2d_i^3)$
(6) $[x_{2\alpha+3\beta}(c_i), x_{-\alpha-2\beta}(d_i)] = x_{\alpha+\beta}(c_id_i)x_{-\beta}(c_id_i^2)x_{-\alpha-3\beta}(-c_id_i^3)x_\alpha(-c_i^2d_i^3)$
(7) $[x_{-\alpha}(c_i), x_{-\beta}(d_i)] = x_{-\alpha-\beta}(-c_id_i)x_{-\alpha-2\beta}(-c_id_i^2)x_{-\alpha-3\beta}(-c_id_i^3)x_{-2\alpha-3\beta}(c_i^2d_i^3)$
(8) $[x_{-\alpha}(c_i), x_{\alpha+\beta}(d_i)] = x_\beta(c_id_i)x_{\alpha+2\beta}(c_id_i^2)x_{2\alpha+3\beta}(-c_id_i^3)x_{\alpha+3\beta}(-c_i^2d_i^3)$
(9) $[x_{-\alpha-3\beta}(c_i), x_\beta(d_i)] = x_{-\alpha-2\beta}(c_id_i)x_{-\alpha-\beta}(c_id_i^2)x_{-\alpha}(-c_id_i^3)x_{-2\alpha-3\beta}(-c_i^2d_i^3)$
(10) $[x_{-\alpha-3\beta}(c_i), x_{\alpha+2\beta}(d_i)] = x_{-\beta}(-c_id_i)x_{\alpha+\beta}(-c_id_i^2)x_{2\alpha+3\beta}(-c_id_i^3)x_\alpha(c_i^2d_i^3)$
(11) $[x_{-2\alpha-3\beta}(c_i), x_{\alpha+\beta}(d_i)] = x_{-\alpha-2\beta}(c_id_i)x_{-\beta}(-c_id_i^2)x_\alpha(c_id_i^3)x_{-\alpha-3\beta}(c_i^2d_i^3)$
(12) $[x_{-2\alpha-3\beta}(c_i), x_{\alpha+2\beta}(d_i)] = x_{-\alpha-\beta}(-c_id_i)x_\beta(c_id_i^2)x_{\alpha+3\beta}(c_id_i^3)x_{-\alpha}(-c_i^2d_i^3)$
(13) $[x_\beta(c_i), x_{\alpha+\beta}(d_i)] = x_{\alpha+2\beta}(2c_id_i)x_{\alpha+3\beta}(-3c_i^2d_i)x_{2\alpha+3\beta}(-3c_id_i^2)$
(14) $[x_\beta(c_i), x_{-\alpha-2\beta}(d_i)] = x_{-\alpha-\beta}(-2c_id_i)x_{-\alpha}(3c_i^2d_i)x_{-2\alpha-3\beta}(3c_id_i^2)$
(15) $[x_{\alpha+\beta}(c_i), x_{-\alpha-2\beta}(d_i)] = x_{-\beta}(2c_id_i)x_\alpha(-3c_i^2d_i)x_{-\alpha-3\beta}(-3c_id_i^2)$
(16) $[x_{\alpha+2\beta}(c_i), x_{-\beta}(d_i)] = x_{\alpha+\beta}(-2c_id_i)x_{2\alpha+2\beta}(-3c_i^2d_i)x_\alpha(-3c_id_i^2)$
(17) $[x_{\alpha+2\beta}(c_i), x_{-\alpha-\beta}(d_i)] = x_\beta(2c_id_i)x_{\alpha+3\beta}(3c_i^2d_i)x_{-\alpha}(3c_id_i^2)$
(18) $[x_{-\beta}(c_i), x_{-\alpha-\beta}(d_i)] = x_{-\alpha-2\beta}(-2c_id_i)x_{-\alpha-3\beta}(-3c_i^2d_i)x_{-2\alpha-3\beta}(-3c_id_i^2)$
(19) $[x_\alpha(c_i), x_{\alpha+3\beta}(d_i)] = x_{2\alpha+3\beta}(c_id_i)$
(20) $[x_\alpha(c_i), x_{-2\alpha-3\beta}(d_i)] = x_{-\alpha-3\beta}(-c_id_i)$
(21) $[x_{\alpha+3\beta}(c_i), x_{-2\alpha-3\beta}(d_i)] = x_{-\alpha}(c_id_i)$
(22) $[x_{2\alpha+3\beta}(c_i), x_{-\alpha}(d_i)] = x_{\alpha+3\beta}(-c_id_i)$
(23) $[x_{2\alpha+3\beta}(c_i), x_{-\alpha-3\beta}(d_i)] = x_\alpha(c_id_i)$
(24) $[x_{-\alpha}(c_i), x_{-\alpha-3\beta}(d_i)] = x_{-2\alpha-3\beta}(-c_id_i)$
(25) $[x_\beta(c_i), x_{\alpha+2\beta}(d_i)] = x_{\alpha+3\beta}(3c_id_i)$
(26) $[x_\beta(c_i), x_{-\alpha-\beta}(d_i)] = x_{-\alpha}(3c_id_i)$
(27) $[x_{\alpha+\beta}(c_i), x_{\alpha+2\beta}(d_i)] = x_{2\alpha+3\beta}(3c_id_i)$
(28) $[x_{\alpha+\beta}(c_i), x_{-\beta}(d_i)] = x_\alpha(3c_id_i)$
(29) $[x_{-\beta}(c_i), x_{-\alpha-2\beta}(d_i)] = x_{-\alpha-3\beta}(-3c_id_i)$
(30) $[x_{-\alpha-\beta}(c_i), x_{-\alpha-2\beta}(d_i)] = x_{-2\alpha-3\beta}(-3c_id_i)$

A.5 Relations for ${}^3D_4(q)$

Here the Dynkin diagram is G_2. The relations are (1)-(30) in Appendix A.4 with the following adjustments:

(a) in relations (1)-(12), $c_i \in \mathbb{F}_q$, $d_i \in \mathbb{F}_{q^3}$; in (13)-(18), $c_i, d_i \in \mathbb{F}_{q^3}$; in (19)-(24), $c_i, d_i \in \mathbb{F}_q$; and in (25)-(30), $c_i, d_i \in \mathbb{F}_{q^3}$;

(b) in relations (1)-(12), $c_i d_i^2$ is replaced by $c_i \bar{d}_i \bar{\bar{d}}_i$ (where $\bar{d}_i = d_i^q$), $c_i d_i^3$ by $c_i d_i \bar{d}_i \bar{\bar{d}}_i$, and $c_i^2 d_i^3$ by $c_i^2 d_i \bar{d}_i \bar{\bar{d}}_i$;

(c) in relations (13)-(18), $2c_i d_i$ is replaced by $\bar{c}_i \bar{\bar{d}}_i + \bar{\bar{c}}_i \bar{d}_i$, $3c_i^2 d_i$ by $c_i \bar{c}_i \bar{\bar{d}}_i + \bar{c}_i \bar{\bar{c}}_i d_i + \bar{\bar{c}}_i c_i \bar{d}_i$, and $3c_i d_i^2$ by $c_i \bar{d}_i \bar{\bar{d}}_i + \bar{c}_i \bar{\bar{d}}_i d_i + \bar{\bar{c}}_i d_i \bar{d}_i$;

(d) in relations (25)-(30), $3c_i d_i$ is replaced by $c_i d_i + \bar{c}_i \bar{d}_i + \bar{\bar{c}}_i \bar{\bar{d}}_i$.

References

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

[2] H. Bäärnhielm, Algorithmic problems in twisted groups of Lie type, PhD thesis, Queen Mary, University of London, 2006.

[3] H. Bäärnhielm, Recognising the Suzuki groups in their natural representations, *J. Algebra* **300** (2006), 171–198.

[4] H. Bäärnhielm, Recognising the small Ree groups in their natural representations, *J. Algebra* (2014), to appear.

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

[6] 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.

[7] L. Babai, A.J. Goodman, W.M. Kantor, E.M. Luks and P.P. Pálfy, Short presentations for finite groups, *J. Algebra* **194** (1997), 79–112.

[8] L. Babai and R. 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.*, pp. 30–64, Cambridge, 1999, Cambridge Univ. Press.

[9] L. Babai and A. Shalev, Recognizing simplicity of black-box groups and the frequency of p-singular elements in affine groups, In *Groups and Computation* III, Ohio State Univ. Math. Res. Inst. Publ., pp. 39–62, de Gruyter, Berlin, 2001.

[10] 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.

[11] L. Babai, P. Pálfy, and J. Saxl, On the number of p-regular elements in finite simple groups, *LMS J. Comput. Math.* **12** (2009), 82–119.

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

[13] N. Bourbaki, *Groupes et Algebres de Lie* (Chapters 4,5,6), Hermann, Paris, 1968.

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

[15] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Math. Soc. Lecture Note Series **407**, Cambridge Univ. Press, 2013.

[16] P.A. Brooksbank, Constructive recognition of classical groups in their natural representation, *J. Symbolic Comput.* **35** (2003), 195–239.

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

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

[19] P.A. Brooksbank, Fast constructive recognition of black-box symplectic groups, *J. Algebra* **320** (2008), 885–909.

[20] R.W. Carter, *Simple groups of Lie type*, Wiley, 1972.

[21] 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.

[22] A.M. Cohen, S.H. Murray and D.E. Taylor, Computing in groups of Lie type, *Math. Comp.* **73** (2004), 1477–1498.

[23] A.M. Cohen and D.E. Taylor, Row reduction for twisted groups of Lie type, preprint.

[24] A.M. Cohen and S.H. Murray, An algorithm for Lang's Theorem. *J. Algebra.* **322** (2009), 675–702.

[25] A.M. Cohen and D. Roozemond, Computing Chevalley bases in small characteristics, *J. Algebra* **322** (2009), 703–721.

[26] M.D.E. Conder, C.R. Leedham-Green, and E.A. O'Brien, Constructive recognition of $\mathrm{PSL}(2, q)$, *Trans. Amer. Math. Soc.* **358** (2006), 1203–1221.

[27] C.W. Curtis. Modular representations of finite groups with split (B, N)-pairs, in *Seminar on Algebraic Groups and Related Finite Groups*, Springer Lecture Notes **131**, pp.57–95, Springer, Berlin, 1970.

[28] Ian Gregor Dick, Constructive recognition of black-box $F_4(q)$ in odd characteristic. PhD thesis, Queen Mary, University of London, 2014.

[29] H. Dietrich, C.R. Leedham-Green, F. Lübeck and E.A. O'Brien, Constructive recognition of classical groups in even characteristic, *J. Algebra* **391** (2013), 227–255.

[30] H. Dietrich, C.R. Leedham-Green and E.A. O'Brien, Effective black-box constructive recognition of classical groups, *J. Algebra* (2014), to appear.

[31] P.B. Gilkey and G.M. Seitz, Some representations of exceptional Lie algebras, Geometries and groups (Noordwijkerhout, 1986), *Geom. Dedicata* **25** (1988), no. 1-3, 407–416.

[32] S.P. Glasby, C.R. Leedham-Green and E.A. O'Brien, Writing projective representations over subfields, *J. Algebra* **295** (2006), 51–61.

[33] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups.* Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.

[34] D.F. Holt, B. Eick and E.A. O'Brien, *Handbook of computational group theory*, Chapman and Hall/CRC Press, London, 2005.

[35] R.B. Howlett, L.J. Rylands and D.E. Taylor, Matrix generators for exceptional groups of Lie type, *J. Symbolic Comput.* **31** (2001), 429–445.

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

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

[38] W.M. Kantor and Á. Seress, Large element orders and the characteristic of Lie-type simple groups, *J. Algebra* **322** (2009), 802–832.

[39] W.M. Kantor and K. Magaard, Black box exceptional groups of Lie type, *Trans. Amer. Math. Soc.* **365** (2013), 4895–4931.

[40] P.B. Kleidman, The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups, *J. Algebra* **115** (1988), 182–199.

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

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

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

[44] M.W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.* **63** (1991), 266–314.

[45] M.W. Liebeck, J. Saxl and G.M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.* **65** (1992), 297–325.

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

[47] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Math. Surveys and Monographs, Vol. 180, American Math. Soc., Providence, RI, 2012, xii+380 pp.

[48] S.A. Linton, The Art and Science of Computing in Large Groups. *Computational algebra and number theory* (Sydney, 1992), 91–109, Math. Appl. 325, Dordrecht 1995.

[49] F. Lübeck, K. Magaard and E.A. O'Brien, Constructive recognition of $\mathrm{SL}_3(q)$, *J. Algebra* **316** (2007), 619–633.

[50] E.A. O'Brien, Algorithms for matrix groups, Groups St Andrews 2009 in Bath II, London Math. Soc. Lecture Note Series **388** (2011), 297–323.

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

[52] C.W. Parker and R.A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers, *J. Algebra* **324** (2010), 885–915.

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