

## BLACK BOX EXCEPTIONAL GROUPS OF LIE TYPE

W. M. KANTOR AND K. MAGAARD

ABSTRACT. If a black box group is known to be isomorphic to an exceptional simple group of Lie type of (twisted) rank  $> 1$ , other than any  ${}^2F_4(q)$ , over a field of known size, a Las Vegas algorithm is given to produce a constructive isomorphism. In view of its timing, this algorithm yields an upgrade of all known nearly linear time Monte Carlo permutation group algorithms to Las Vegas algorithms when the input group has no composition factor isomorphic to any group  ${}^2F_4(q)$  or  ${}^2G_2(q)$ .

### 1. INTRODUCTION

In a number of algorithmic settings it is essential to take a permutation group or matrix group that is known (probably) to be simple and to produce an explicit isomorphism with an explicitly defined simple group, such as a group of matrices ([LG, KS1, Ka3] contain background on this and many related questions). This has been accomplished for the much more general setting of black box classical groups in [KS1, Br1, Br2, Br3, BrK1, BrK2, LMO] (starting with the groups  $\mathrm{PSL}(d, 2)$  in [CFL]). Black box alternating groups are dealt with in [BLNPS]. In this paper we consider this identification question for black box exceptional groups of Lie type. Note that the *name* of the group can be found quickly using Monte Carlo algorithms in suitable settings [BKPS, KS3, KS4, LO].

The elements of a black box group  $G$  are assumed to be encoded by 0-1 strings of uniform length, and  $G$  is specified as  $G = \langle \mathcal{S} \rangle$  for some set  $\mathcal{S}$  of elements of  $G$ . Our main result is as follows (where  $\epsilon$  is 1 in general, and 3 for  ${}^3D_4(q)$ ):

**Theorem 1.1.** *There is a Las Vegas algorithm which, when given a black box group  $G = \langle \mathcal{S} \rangle$  isomorphic to a perfect central extension of a simple exceptional group of Lie type of (twisted) rank  $> 1$  and given field size  $q$ , other than any  ${}^2F_4(q)$ , finds the following:*

- (i) *The name of the simple group of Lie type to which  $G/Z(G)$  is isomorphic and*
- (ii) *A new set  $\mathcal{S}^*$  generating  $G$ , a generating set  $\hat{\mathcal{S}}$  of the universal cover  $\hat{G}$  of the simple group in (i) and an epimorphism  $\Psi: \hat{G} \rightarrow G$ , specified by the requirement that  $\hat{\mathcal{S}}\Psi = \mathcal{S}^*$ .*

---

Received by the editors November 1, 2009 and, in revised form, November 6, 2009 and December 13, 2011.

2010 *Mathematics Subject Classification.* Primary 20D06, 20G40; Secondary 20B40, 20G41, 20P05, 68Q25.

This research was supported in part by NSF grants DMS 9731421, DMS 0242983 and DMS 0753640, and NSA grant MDA-9049810020.

©2013 American Mathematical Society  
Reverts to public domain 28 years from publication

Moreover, the data structures underlying (ii) yield algorithms for each of the following:

- (iii) Given  $g \in G$ , find  $\hat{g} \in \hat{G}$  such that  $g = \hat{g}\Psi$ , and a straight-line program of length<sup>1</sup>  $O(\log q)$  from  $\mathcal{S}^*$  to  $g$  and
- (iv) Given  $\hat{g} \in \hat{G}$ , find  $\hat{g}\Psi$  and a straight-line program of length  $O(\log q)$  from  $\hat{\mathcal{S}}$  to  $\hat{g}$ .

In addition, the following all hold.

- (v)  $\mathcal{S}^*$  has size  $O(\log q)$  and contains a generating set for  $G$  consisting of root elements.
- (vi) The algorithm for (ii) is an  $O(\xi q^\epsilon \log q + \mu q^\epsilon \log^2 q)$ -time Las Vegas algorithm succeeding with probability  $> 1/2$ , where  $\mu$  is an upper bound on the time required for each group operation in  $G$  and  $\xi \geq \mu$  is an upper bound on the time requirement per element for the construction of independent, (nearly) uniformly distributed random elements of  $G$ .

In additional  $O(|\mathcal{S}| \log |\mathcal{S}| (\xi q^\epsilon \log q + \mu q^\epsilon \log^2 q))$  time it can be verified that  $G$  is indeed isomorphic to a perfect central extension of the exceptional group in (i).

- (vii) The algorithm for (iii) is Las Vegas, running in  $O(\xi q^\epsilon \log q + \mu q^\epsilon \log^2 q)$  time and succeeding with probability  $> 1/2$ , while the algorithm for (iv) is deterministic and runs in  $O(\mu \log q)$  time.
- (viii) The center of  $G$  can be found in  $O(\mu \log q)$  time.

Parts (ii)–(iv) are the requirements for a *constructive epimorphism*  $\Psi: \hat{G} \rightarrow G$ . The verification at the end of (vi) is omitted in some references, since  $G$  is assumed to be an epimorphic image of a specific group  $\hat{G}$  which, in turn, is isomorphic to (a central extension of) an explicitly constructed subgroup  $G_0$  of  $G$  (cf. Proposition 2.33). In practice, it is hard to imagine that this test would be omitted since it appears to be the only way to guarantee that the group  $G$  behaves as hypothesized. We note that, in (iv),  $\hat{g} \in \hat{G}$  might be given in standard Bruhat normal form but alternatively might merely be given as an automorphism of the associated Lie algebra (cf. Remark 2.40). It is also worth remarking that we use  $\epsilon = 1$  for groups of type  ${}^2E_6(q)$ , since that is the case for its Levi factor  $SU(6, q)$  (Theorem 1.3).

The above algorithms do not run in polynomial time: the timing in (vi) and (vii) have factors  $q$ . At present there are no polynomial-time algorithms for the type of problem considered here, neither in the black box setting nor even in the matrix group one. This was already evident for classical groups in [KS1] and, even earlier, in [CLG]. A standard way around this obstacle involves a lovely idea in [CoLG] (used in [BrK1, BrK2, Br2, Br3, LMO]): *use suitable oracles*. The preceding references assume the availability of an oracle that constructively recognizes subgroups  $SL(2, q)$ . This was motivated by [CoLG], which deals with matrix groups and assumes the availability of a *Discrete Log oracle* for  $\mathbb{F}_q^*$ . In this matrix group setting, [CoLG, CoLGO] provide a constructive Las Vegas algorithm for a group isomorphic to a nontrivial homomorphic image of  $SL(2, q)$  in any irreducible representation in characteristic dividing  $q$ , running in time that is polynomial in the input length, assuming the availability of a Discrete Log oracle. In effect, this idea replaces annoying factors  $q$  by an oracle. This is discussed further in Section 4, Remarks 4–6, making it clear that this will not be the last paper on this type of problem!

<sup>1</sup>All logarithms are to the base 2.

A rough outline of the proof of the theorem is given in Section 1.2. The first part resembles [KS1]: we find a long root element and then build a subgroup  $SL(3, q)$  and also a subgroup  $Spin_{\bar{8}}(q)$  when the Lie rank is more than 2. We then use pieces of these groups to obtain the centralizer of a subgroup  $SL(2, q)$  generated by long root groups. However, there is no module to aim for that is as nice as in the classical case. Hence, instead we proceed directly to obtain all of the root groups corresponding to a root system, and then verify the standard commutator relations that define these groups: the corresponding presentation guarantees the Las Vegas nature of our algorithm.

Our proofs are divided into two parts, with rank  $> 2$  and rank 2 in Sections 2 and 3, respectively. Section 4 contains remarks concerning improvements or variations on the theorem and the algorithms.

In view of [KS2] (and [BrB]), we obtain the following immediate but significant consequence of the above theorem:

**Corollary 1.2.** *Given a permutation group  $G \leq S_n$  with no composition factor isomorphic to any group  ${}^2F_4(q)$  or  ${}^2G_2(q)$ , all known nearly linear time Monte Carlo algorithms dealing with  $G$  can be upgraded to Las Vegas algorithms.*

The stated algorithms find  $|G|$  and a composition series of  $G$ , among many other things (cf. [Ser]). In fact, it can be shown that the groups  ${}^2G_2(q)$  do not need to be excluded here; see Section 4, Remark 7.

**1.1. Background.** For background on groups of Lie type we refer to [Ca1, GLS]. For background on required aspects of black box groups, in particular for discussions of the parameters  $\xi$  and  $\mu$  in the theorem, see [KS1, 2.2.2]. Thus, we assume that  $\xi \geq \mu|\mathcal{S}|$  and  $\mu \geq N$  if  $N$  is the string length of the elements of our black box group  $G$ . Moreover,  $N \geq \log |G| > C \log q$  for some constant  $C$ , since we are dealing with exceptional groups of Lie type over  $\mathbb{F}_q$ .

We note that, as in [KS1, 2.2.4], we presuppose the availability of independent (nearly) uniformly distributed random elements of  $G$ , a major result in [Bab] (compare [CLMNO, Dix]).

*Straight-line programs* from  $\mathcal{S}$  to elements of  $G = \langle \mathcal{S} \rangle$  are also defined and discussed in [KS1, 2.2.5]. For use in [KS2] (or in Corollary 1.2), part (iii) of the theorem needs the stated straight-line program, not just the preimage  $\hat{g}$ .

In general the symbol  $\text{ppd}^{\#}(p; n)$  stands for some integer divisible by a prime  $r$  (a *primitive prime divisor*) such that  $r|p^n - 1$  but  $r \nmid p^i - 1$  for  $1 \leq i < n$  (cf. [Zs]). The exceptions to this definition are:  $\text{ppd}^{\#}(p; 1)$  with  $p > 5$  a Fermat prime, where we require divisibility by 4;  $\text{ppd}^{\#}(p; 2)$  with  $p$  a Mersenne prime, where we require divisibility by 4; and  $\text{ppd}^{\#}(2; 6)$ , where we require divisibility by 21. It is easy to test this property of an integer for a single  $\text{ppd}^{\#}(p; n)$  requirement ([NP, p. 578], [KS1, Lemma 2.7]), and hence also for a product  $\text{ppd}^{\#}(p; n_1) \cdots \text{ppd}^{\#}(p; n_k)$  of a bounded number of them (where  $n_1 < \cdots < n_k$ ). In those references, the time requirement for such tests is far smaller than other aspects of our algorithms, and hence will be ignored.

*Notation.* We always write  $q = p^e$ , where  $p$  is the characteristic of  $G$ .

We will usually have available a field  $\mathbb{F} = \mathbb{F}_q$  obtained from subgroups of  $G$ , and also an extension field  $\mathbb{F}'$  of  $\mathbb{F}$  of degree 1, 2 or 3. We choose an  $\mathbb{F}_p$ -basis  $\{f_1, \dots\}$  of  $\mathbb{F}'$  such that  $f_1 = 1$  and  $\{f_1, \dots, f_e\}$  is a basis of  $\mathbb{F}$ .

In view of the discussion in [KS1, Sec. 2.3], we will always assume that *field operations can be carried out in constant time*.

**1.2. Outline.** A very rough summary of our approach to Theorem 1.1(ii),(vi) is as follows (with many details suppressed or ignored).

- Use random group elements and primitive prime divisors to find  $\tau \in G$  of special order, in particular such that some power  $z = \tau^l$  is a long root element (cf. Sections 2.2, 2.5, 3.2). (In types  $E_7$  and  $E_8$  we need two such elements  $\tau$  of different specific orders.)
- Find three conjugates of  $z$  that generate a subgroup  $S = \mathrm{SL}(3, q)$  (cf. Sections 2.3, 2.7, 3.2), together with a subgroup  $R \cong \mathrm{SL}(2, q)$  of  $S$  also generated by conjugates of  $z$ . Much of the algorithm depends heavily on  $\mathrm{SL}(2, q)$  and  $\mathrm{SL}(3, q)$  subgroups.
- For rank  $> 2$  use  $S$  and a conjugate of  $z$  to construct a  $G$ -conjugate of  $R$  lying in  $L = C_G(R)$  (cf. Section 2.8); this  $\mathrm{SL}(2, q)$  and variants of the element(s)  $\tau$  are used to generate  $L$  (cf. Section 2.9). If the rank is 2, then  $C_S(R)$  and  $\tau$  generate  $L$  (which this time is an  $\mathrm{SL}(2, q^\epsilon)$ ; cf. Section 3.3).

This heavily depends on the uniqueness of the triple  $(R, S, L)$  up to conjugacy in  $G$ .

- Find a (maximally) split torus  $T$  normalizing  $L$  and  $S$ . Use it to construct root systems of  $L$  and  $S$  with respect to the tori  $T \cap L$  and  $T \cap S$ . Use commutators of root groups of  $S$  and  $L$  to find root groups and a root system  $\Phi_G$  for  $G$  (cf. Sections 2.10, 3.3).
- The new generating set  $\mathcal{S}^*$  for  $G$  contains the union of sets of generators of these root groups  $X_\alpha$ ,  $\alpha \in \Phi_G$ . Verify a version of the Steinberg presentation [St] for the subgroup  $G_0$  generated by these subgroups  $X_\alpha$  (cf. Sections 2.12, 3.4).
- Show that each of the given generators for  $G$  is in  $G_0$ , so that  $G_0 = G$  (cf. Sections 2.15, 3.6).

**1.3. Recognition algorithms used.** We will use existing algorithms for constructive recognition of various black box groups. Since their timing is crucial for us, we state the instances and timings in the next result, which refers to the counterparts in our Theorem 1.1:

**Theorem 1.3.** *Let  $G = \langle \mathcal{S} \rangle$  be a black box group that is isomorphic to a nontrivial homomorphic image of  $\mathrm{SL}(2, q)$ ,  $\mathrm{SL}(3, q)$ ,  $\mathrm{Sp}(6, q)$ ,  $\mathrm{SU}(6, q)$ ,  $\mathrm{Spin}_8^-(q)$  or  $\mathrm{Spin}_{12}^+(q)$ . Then there are algorithms for the natural analogues of Theorem 1.1(ii)-(iv), and the following hold:*

- (i) Theorem 1.1(v) holds;
- (ii) Theorem 1.1(ii) takes  $O(\xi q \log q + \mu q \log^2 q)$  Las Vegas time, succeeding with probability  $> 1/2$ ;
- (iii) Theorem 1.1(iii) is deterministic and takes  $O(\mu q \log q)$  time, except in the case  $\mathrm{SU}(6, q)$ , where it takes  $O(\xi q \log q + \mu q \log q)$  Las Vegas time, succeeding with probability  $> 1/2$ ; and
- (iv) Theorem 1.1(iv) is deterministic and takes  $O(\mu \log q)$  time.

*Proof.* This is contained in [KS1], except that the times in [KS1, 6.6.3] contain a factor  $q^3$  for the group  $\mathrm{SU}(6, q)$  (due to the treatment of  $\mathrm{SU}(3, q)$ ), which is avoided as follows.

It is noted in [BrK2, Sec. 5.3] that [KS1, 4.6.3] handles  $P\Omega^-(6, q)$  in the stated times if modified using ideas in [BrK2]. This readily gives the stated result for  $SU(4, q)$ , which can then be used in [KS1, Sec. 6] for all larger-dimensional unitary groups. In particular, this leads to the stated times for  $SU(6, q)$ .  $\square$

The above times do *not* include verification of a presentation of the stated groups (cf. Theorem 1.1(vi)); we will deal with that later in the context of Theorem 1.1. There are more recent versions of the above theorem that run in polynomial time, assuming the availability of suitable oracles [BrK1, BrK2, Br2, Br3, LMO]. Section 4 contains comments concerning possible similar improvements of Theorem 1.1. We also note that [Br2, Br3] obtain better times than [KS1] by avoiding the recursive call in the latter reference, but this has little effect on the present paper's focus on bounded rank groups.

**Convention 1.4.** The proof of Theorem 1.1(vi) uses the Las Vegas portion of Theorem 1.3(iii) for  $SU(6, q)$  when  $G$  has type  ${}^2E_6(q)$ , and the Las Vegas Theorem 1.1(vi) (more precisely, the Theorem 1.1(iii) portion) for type  $E_7$  when  $G$  has type  $E_8(q)$ ; otherwise all of our uses of Theorems 1.3(iii) and 1.1(iii) are deterministic. In the description of our algorithm, we will use deterministic language when employing the aforementioned results. In each instance that is actually Las Vegas (of which there are only  $O(\log q)$ ), up to 20 repetitions of the Las Vegas version can be inserted in order to guarantee that the probability of failure is at most  $1/2^{20}$ , which is insignificant compared to other probabilities of failure that occur elsewhere in our algorithms.

As in [KS1, KS3, KS4, BrK1, BrK2, Br2, Br3], we will use crude probability estimates, making the number of repetitions of calls to previous routines (such as those in Theorem 1.3(ii)) appear to be unreasonably large. The goal has been to prove theorems rather than to obtain best estimates for each type of group.

As in [KS1, KS3, KS4, BrK1, BrK2, Br2, Br3], our algorithms contain statements such as “Choose up to  $10 \cdot 2^{12}$  pairs  $z', y, \dots$ ”. We could instead have used statements such as “Choose  $O(1)$  pairs  $z', y, \dots$ ”; this would have eliminated some calculations, suppressed some very annoying constants, and looked more elegant. However, it is not clear how a computer would deal with such an  $O(1)$  requirement. By contrast, “ $O(\mu \log q)$  time” merely refers to a property of an algorithm.

## 2. GROUPS OF RANK $> 2$

Throughout this section we will assume that

(2.1)  $\hat{G}$  is the simply connected cover of  $F_4(q)$ ,  $E_6(q)$ ,  ${}^2E_6(q)$ ,  $E_7(q)$  or  $E_8(q)$ .

Here,  $\hat{G}$  is a known copy of the group in question, as opposed to a black box version we will eventually handle. There are only a few cases where  $\hat{G}$  is not also the universal cover of  $G$  (cf. [GLS, p. 313]), and we will always assume that  $q$  is large enough to avoid these. Thus,  $\hat{G}$  is precisely the group with that name appearing in Theorem 1.1.

We will assume the availability of the Lie algebra of  $\hat{G}$ . This will be used in Lemma 2.32 (and the Appendix) and in Remark 2.40.

*Notation.*

$\Phi$	the root system for $\hat{G}$
$\Phi^+$	the set of positive roots
$\Delta$	a base of $\Phi$
$p$	the characteristic of $\hat{G}$
$\mathbb{F}$	$\mathbb{F}_q, q = p^e$
$\mathbb{F}'$	$\mathbb{F}_{q^{\epsilon'}}$ , where $\epsilon' = 1$ except for ${}^2E_6(q)$ , where $\epsilon' = 2$
$\{f_1, \dots, f_e\}$	an $\mathbb{F}_p$ -basis of $\mathbb{F}$ , where $f_1 = 1$
$\{f_1, \dots, f_{2e}\}$	an $\mathbb{F}_p$ -basis of $\mathbb{F}'$ if $\hat{G}$ is ${}^2E_6(q)$

The *rank* of  $\hat{G}$  refers to the twisted rank (for example,  ${}^2E_6(q)$  has rank 4).

**2.1. Properties of  $\hat{G}$ .** We will use a standard type of presentation for the simply connected cover  $\hat{G}$  of the simple group of Lie type we are considering. This presentation depends on the root system  $\Phi$  and various integers  $C_{i,j,\alpha,\beta}, \epsilon_{\alpha\beta}, \eta_{\alpha\beta}, A_{\alpha,\beta}$ , all of which we assume have been precomputed.

**Presentation of the target group.** We temporarily exclude groups of type  ${}^2E_6$ . The following is just a straightforward, shortened version of the standard Curtis-Steinberg-Tits presentation [St, BGKLP]. Use generators  $\hat{X}_\alpha(f_k), \alpha \in \Phi, 1 \leq k \leq e$ , satisfying the following relations:

(2.2) Given any  $t = \sum_k z_k f_k \in \mathbb{F}$  with  $0 \leq z_k < p$ , write

$$\hat{X}_\alpha(t) := \prod_k \hat{X}_\alpha(f_k)^{z_k},$$

(2.3)  $\hat{X}_\alpha(f_k)^p = 1$  for  $\alpha \in \Phi, 1 \leq k \leq e$ ,

(2.4)  $[\hat{X}_\alpha(f_k), \hat{X}_\alpha(f_l)] = 1$  for  $\alpha \in \Phi, 1 \leq k < l \leq e$ , and

(2.5)  $[\hat{X}_\alpha(f_k), \hat{X}_\beta(f_l)] = \prod_{i,j>0} \hat{X}_{i\alpha+j\beta}(C_{i,j,\alpha,\beta} f_k^i f_l^j)$  for  $\alpha, \beta \in \Phi, \alpha \neq \beta, 1 \leq k, l \leq e$ .

The right hand side of (2.5) is viewed as expanded, using (2.2), into an expression involving powers of the generators  $\hat{X}_\gamma(f_m)$  for  $\gamma \in \Phi, 1 \leq m \leq e$ . The structure constants  $C_{i,j,\alpha,\beta}$  are integers that are at most 2 in absolute value (since we have rank  $> 2$ ) and are given in [Ca1, Section 5.2]. The non-uniqueness of this presentation is discussed at length in [Ca1, p. 58].

The right side of (2.5) has at most one nontrivial term when there is only one root length (i.e., for types  $E_6, E_7, E_8$ ). In this case, there is a nontrivial term  $\hat{X}_{\alpha+\beta}(C_{1,2,\alpha,\beta} f_k f_l)$  precisely when  $\alpha + \beta \in \Phi$ . A more precise version of (2.5) for groups of type  $F_4$  is in the paragraph following (2.6).

The above relations provide a presentation for the simply connected cover  $\hat{G}$ . An algorithm for finding the center of this group is given in [Ca1, p. 198] using elementary linear algebra; every element of  $Z(\hat{G})$  is expressed as a word in our generators. However,  $Z(\hat{G})$  can easily be found more directly for the groups studied here.

We will need further relations (2.9)–(2.10) that are consequences of the preceding ones and take into account the action of a split torus on the root groups  $\hat{X}_\alpha := \langle \hat{X}_\alpha(f_k) \mid 1 \leq k \leq e \rangle$ .

**The group  ${}^2E_6(q)$ .** This time  $\hat{G}$  is the simply connected central extension of  ${}^2E_6(q)$ ,  $\Phi$  is a root system of type  $F_4$  and  $\hat{G}$  has generators  $\hat{X}_\alpha(f_k)$  with  $\alpha \in \Phi$ , and  $1 \leq k \leq e$  for  $\alpha$  long, while  $1 \leq k \leq 2e$  for  $\alpha$  short. We use the obvious analogues of relations (2.2)–(2.4), along with the relations

$$(2.6) \quad \begin{array}{ll} [\hat{X}_\alpha(f_k), \hat{X}_\beta(f_l)] = & \text{for:} \\ 1 & \alpha + \beta \notin \Phi \\ \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta} f_k f_l) & \alpha, \beta, \alpha + \beta \text{ all short or all long} \\ \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta}(f_k f_l^q + f_k^q f_l)) & \alpha, \beta \text{ short, } \alpha + \beta \text{ long} \\ \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta} f_k f_l) \hat{X}_{\alpha+2\beta}(\epsilon'_{\alpha\beta} f_k f_l f_l^q) & \alpha, \alpha + 2\beta \text{ long, } \beta, \alpha + \beta \text{ short} \end{array}$$

for all appropriate basis elements  $f_k, f_l$ . The right hand side of (2.6) is expanded as above. The structure constants  $\epsilon_{\alpha\beta}$  and  $\epsilon'_{\alpha\beta}$  are  $\pm 1$ , and as before we assume that these have been obtained in advance.

The relations corresponding to (2.5) for  $F_4(q)$  are just the relations (2.6) with all field elements in  $\mathbb{F}$ . In this case, the third relation in (2.6) involves a structure constant  $C_{i,j,\alpha,\beta}$  that is not 0 or  $\pm 1$ , and this is the only time this occurs for groups of rank  $> 2$ .

*We assume that the presentations (2.2)–(2.5) or (2.6) are given as part of the data describing the target group  $\hat{G}$ . Eventually we will find elements of our black box group satisfying them.*

The above presentations are essential for our algorithms. However, there are “variants” [GKKL1, GKKL2] that may be more useful in practice: they only involve a bounded number of relations for any  $q$  (fewer than 1000 in [GKKL1] or 50 in [GKKL2]).

**Additional relations in  $\hat{G}$ ; the subgroups  $T_{\hat{G}}$  and  $N_{\hat{G}}$ .** Following [Ca1, p. 189], if  $\alpha \in \Phi$  and  $t \in \mathbb{F}^*$ , let

$$(2.7) \quad \hat{h}_\alpha(t) := \hat{n}_\alpha(t) \hat{n}_\alpha(-1), \text{ where } \hat{n}_\alpha(t) := \hat{X}_\alpha(t) \hat{X}_{-\alpha}(-t^{-1}) \hat{X}_\alpha(t);$$

when  $\hat{G}$  is of type  ${}^2E_6$  and  $\alpha$  is short then we also allow  $t \in \mathbb{F}'^*$ . Define

$$(2.8) \quad T_{\hat{G}} := \langle \hat{h}_\alpha(t) \mid \alpha \in \Phi, t \in \mathbb{F}^* \rangle \text{ and } N_{\hat{G}} := \langle T_{\hat{G}}, \hat{n}_\alpha(t) \mid \alpha \in \Delta, t \in \mathbb{F}^* \rangle;$$

in type  ${}^2E_6$  we again use  $t \in \mathbb{F}'^*$  when  $\alpha$  is short. If  $\hat{G}$  is an untwisted group, then  $T_{\hat{G}}$  is a maximal split torus of order  $(q-1)^{\text{rank of } G}$ , and if  $\hat{G}$  is  ${}^2\hat{E}_6(q)$ , then  $T_{\hat{G}}$  is a maximally split torus of order  $(q-1)^2(q^2-1)^2$ . Moreover,  $T_{\hat{G}} \triangleleft N_{\hat{G}}$ , and  $N_{\hat{G}}/T_{\hat{G}}$  is the Weyl group of  $\hat{G}$ .

If  $\alpha \in \Phi$ , then  $\hat{X}_\alpha$  is the set of all  $\hat{X}_\alpha(t)$ . The subgroups  $\hat{X}_\alpha$  generate  $\hat{G}$ .

By [Ca1, p. 194], the root groups  $\hat{X}_\alpha$  are invariant under conjugation by  $T_{\hat{G}}$ :

$$(2.9) \quad \begin{array}{ll} \hat{h}_\alpha(t) \hat{X}_\beta(u) \hat{h}_\alpha(t)^{-1} = \hat{X}_\beta(t^{A_{\alpha,\beta}} u) & \text{except for the next instance} \\ \hat{h}_\alpha(t) \hat{X}_\beta(u) \hat{h}_\alpha(t)^{-1} = \hat{X}_\beta((tt^q)^{A_{\alpha,\beta}/2} u) & \text{in type } {}^2E_6, \alpha \text{ short, } \beta \text{ long,} \end{array}$$

where  $A_{\alpha,\beta} := 2(\alpha, \beta)/(\alpha, \alpha)$  for the Killing form  $(\ , \ )$  of the underlying Lie algebra. By [Ca1, p. 190] we also have

$$(2.10) \quad \hat{n}_\alpha(t) \hat{X}_\beta(u) \hat{n}_\alpha(t)^{-1} = \hat{X}_{w_\alpha(\beta)}(\eta_{\alpha,\beta} t^{-A_{\alpha,\beta}} u),$$

where  $w_\alpha$  is the reflection in the Weyl group of  $\hat{G}$  corresponding to the hyperplane  $\alpha^\perp$  and where  $\eta_{\alpha,\beta} = \pm 1$ . Thus, each element of the Weyl group permutes the root groups  $\hat{X}_\beta$  by conjugation.

**How elements of  $\hat{G}$  are described.** Elements of  $\hat{G}$  are most conveniently given in the form  $unu'$ , with  $n \in N_{\hat{G}}$  and  $u, u'$  in the Sylow  $p$ -subgroup  $\langle \hat{X}_{\gamma}(t) \mid t \in \mathbb{F} \text{ or } \mathbb{F}', \gamma \in \Phi^+ \rangle$  (*Bruhat decomposition* [Ca1, Corollary 8.4.4] or [GLS, Theorem 2.3.5]). In this paper we do not have a natural module as occurs in the classical group case [CFL, KS1, Br1, Br2, Br3, BrK1, BrK2, LMO]. However, an element of  $\hat{G}$  could merely be given as an automorphism of the associated Lie algebra. See Remark 2.40 for further discussion.

**Root groups and root elements.** The  $\hat{G}$ -conjugates of the  $\hat{X}_{\alpha}$  are called *root groups*: a *long root group* if  $\alpha$  is long and a *short root group* if  $\alpha$  is short. In case all roots have equal length we call all root groups “long”. Context will determine whether a discussion of long root groups will only be concerned with ones of the form  $\hat{X}_{\alpha}$  rather than arbitrary conjugates of these.

Nontrivial elements of long root groups are called *long root elements*. Each long root element is in a uniquely determined long root group.

The following standard result is in [Coo, Lemma 2.2].

**Lemma 2.11.** *For long root groups  $X_1, X_2$ , of  $\hat{G}$ , one of the following holds:*

- (i)  $[X_1, X_2] = 1$ ,
- (ii)  $|\langle X_1, X_2 \rangle| = q^3$  and  $[X_1, X_2] = Z(\langle X_1, X_2 \rangle)$  is a long root group, or
- (iii)  $\langle X_1, X_2 \rangle \cong \text{SL}(2, q)$ .

Two long root groups are *opposite* if they generate a subgroup isomorphic to  $\text{SL}(2, q)$ , called a *long  $\text{SL}(2, q)$* . Short  $\text{SL}(2, q)$ 's are defined similarly when there are two root lengths. Two long root elements are *opposite* if they lie in opposite long root groups. Note that, when  $q$  is even, two opposite long root elements will merely generate a dihedral group. The preceding lemma provides a simple way to test whether or not two long root elements are opposite:

$$(2.12) \quad \text{Long root elements } a, b \text{ are opposite if and only if } [[a, b], a] \neq 1.$$

**The group  $\hat{R}$ , the highest root  $\nu$  and the root  $\nu'$ .** Let

$$(2.13) \quad \hat{R} := \langle \hat{X}_{\nu}, \hat{X}_{-\nu} \rangle \cong \text{SL}(2, q), \text{ where } \nu \text{ is the highest root of } \Phi.$$

Then  $\nu$  is a long root,  $\Delta \cup \{-\nu\}$  is the set of roots in the extended Dynkin diagram of  $\hat{G}$  [GLS, p. 10], and

$$(2.14) \quad \text{There is a unique long root } \nu' \in \Delta \text{ not orthogonal to } -\nu.$$

Moreover,  $\Delta_{\hat{L}} := \Delta \cap \nu^{\perp}$  is a base of the subroot system  $\Phi_{\hat{L}}$  it generates, and  $\Delta = \Delta_{\hat{L}} \cup \{\nu'\}$ .

**The subgroups  $\hat{L}$  and  $\hat{Q}$ .** Define

$$\hat{L} := \langle \hat{X}_{\alpha} \mid \alpha \in \Phi_{\hat{L}} \rangle \text{ and } \hat{Q} := \langle \hat{X}_{\alpha} \mid \alpha \in \Phi^+ \setminus \Phi_{\hat{L}} \rangle.$$



If  $1 \neq z \in \hat{X}_\nu$  then  $C_{\hat{G}}(z) = \hat{Q} \rtimes \hat{L} = C_{\hat{G}}(\hat{X}_\nu)$ . The groups  $\hat{L}$  and  $\hat{Q}$  are as follows:

(2.15)

$\hat{G}$	$\hat{F}_4(q)$	$\hat{E}_6(q)$	${}^2\hat{E}_6(q)$	$\hat{E}_7(q)$	$\hat{E}_8(q)$
$\hat{L}$	$\text{Sp}(6, q)$	$\text{SL}(6, q)$	$\text{SU}(6, q)$	$\text{Spin}_{12}^+(q)$	$\hat{E}_7(q)$
$\hat{Q}$	$q^{1+14} \text{ } \flat$	$q^{1+20}$	$q^{1+20}$	$q^{1+32}$	$q^{1+56}$
$\hat{T}_*$	$q^3 + 1$	$\frac{q^6 - 1}{q - 1}$	$\frac{q^6 - 1}{q + 1}$	$q^6 - 1$ $\frac{q^8 - 1}{q^2 - 1}$	$\frac{q^8 - 1}{q - 1}$ $\frac{q^9 + 1}{q^2 - q + 1}$

where  $\hat{E}_r(q)$  denotes the simply connected cover of  $E_r(q)$ , and  $Z(\hat{Q}) = \hat{X}_\nu$  except where  $\flat$  indicates that this does not hold for  $F_4(q)$  when  $q$  is even (cf. Lemma 2.18(iv)). We have also listed the orders of some cyclic maximal tori  $\hat{T}_*$  of  $\hat{L}$  containing  $Z(\hat{G})$  that will be used in Section 2.2. The orders in the  $E_8$  case come from [DF,  $T_{30}$  and  $T_{24}$  in Table III].

Note that  $\hat{Q}\hat{L}$  is the derived subgroup of a parabolic subgroup  $N_{\hat{G}}(\hat{X}_\nu)$  for which the unipotent radical is  $\hat{Q}$  and the derived group of a Levi factor is  $\hat{L}$ . Also,

(2.16)  $Z(\hat{G}) < C_{\hat{G}}(\hat{R}) = \hat{L}$ , and  $T_{\hat{G}}$  normalizes both  $\hat{R}$  and  $\hat{L}$ .

Define

(2.17)  $T_{\hat{L}} := \langle \hat{h}_\alpha(t) \mid \alpha \in \Phi_{\hat{L}}, t \in \mathbb{F}^* \rangle$  and  $N_{\hat{L}} := \langle T_{\hat{L}}, \hat{n}_\alpha(t) \mid \alpha \in \Delta_{\hat{L}}, t \in \mathbb{F}^* \rangle$

with  $\hat{n}_\alpha(t)$  in (2.7); in type  ${}^2E_6$ , as in (2.8) use  $t \in \mathbb{F}'^*$  when  $\alpha$  is short, so that  $\hat{L} = \text{SU}(6, q)$  and  $|T_{\hat{L}}| = (q - 1)(q^2 - 1)^2$ . In each case,  $T_{\hat{L}}$  is a maximal torus of  $\hat{L}$ ,  $T_{\hat{L}} < T_{\hat{G}}$ ,  $N_{\hat{L}} < N_{\hat{G}}$  and  $N_{\hat{L}}/T_{\hat{L}}$  is the Weyl group of  $\hat{L}$ .

Let  $\hat{Z} := X_\nu$ .

**Lemma 2.18.** [CKS, pp. 16–18]

- (i) For every root  $\nu \neq \alpha \in \Phi^+ \setminus \Phi_{\hat{L}}$  there is a unique root  $\beta \in \Phi^+ \setminus \Phi_{\hat{L}}$  such that  $\alpha + \beta = \nu$ .
- (ii) If  $\hat{G}$  is not  $F_4(q)$  with  $q$  even, then for each root group  $\hat{X}_\alpha \neq \hat{Z}$  in  $\hat{Q}$  there is a unique root group  $\hat{X}_\beta$  in  $\hat{Q}$  that does not commute with  $\hat{X}_\alpha$  (and then  $\alpha$  and  $\beta$  have the same length).
- (iii) If  $\hat{G}$  is  $F_4(q)$  with  $q$  even, then for each long root group  $\hat{X}_\alpha \neq \hat{Z}$  in  $\hat{Q}$  there is a unique long root group  $\hat{X}_\beta$  in  $\hat{Q}$  that does not commute with  $\hat{X}_\alpha$ .
- (iv) If  $\hat{G}$  is  $F_4(q)$  with  $q$  even, then  $Z(\hat{Q}) = \langle \hat{Z}, \hat{X}_\alpha \mid \alpha \text{ short} \rangle$  has order  $q^7$  and is the standard module for  $\hat{L} = \Omega(7, q)$ .

This follows from the commutator relations, which also provide more information in the situation of this lemma:  $\hat{Q}/[\hat{Q}, \hat{Q}]$  is an  $\mathbb{F}$ -space of dimension 14, 20, 20, 32 and 56 in the respective cases (2.1); and it is an irreducible  $\mathbb{F}\hat{L}$ -module except when  $q$  is even and  $\hat{G} = F_4(q)$  (producing the  $\flat$  in (2.15)), in which case  $\hat{Q}/[\hat{Q}, \hat{Q}]$  has an irreducible 6-dimensional  $\mathbb{F}\hat{L}$ -submodule modulo which it is irreducible (Section 2.14 has computations based on this fact).

**Long subgroups.** We call any subgroup generated by (conjugates of) long root groups a *long subgroup*. We will especially emphasize long subgroups such as  $\hat{R}$ ,

$\hat{L}$ , long  $\mathrm{SL}(3, q)$ -subgroups such as  $\hat{S}$  in (2.19) below, and long subgroups  $\mathrm{Spin}_8^-(q)$  such as  $\hat{J}$  in Lemma 2.23 below.

**The long subgroup  $\hat{S} \cong \mathrm{SL}(3, q)$ .** Let

$$(2.19) \quad \hat{S} = \langle \hat{X}_\nu, \hat{X}_{-\nu}, \hat{X}_{\nu'}, \hat{X}_{-\nu'} \rangle \cong \mathrm{SL}(3, q), \quad T_{\hat{S}} = T_{\hat{G}} \cap \hat{S} \text{ and } N_{\hat{S}} = N_{\hat{G}} \cap \hat{S}.$$

The following are straightforward to check:

- Lemma 2.20.** (i)  $T_{\hat{G}}$  normalizes  $\hat{S}$ .  
 (ii)  $N_{\hat{G}} = \langle N_{\hat{S}}, N_{\hat{L}} \rangle$ .  
 (iii) If  $q > 2$  then  $T_{\hat{G}} = \langle T_{\hat{S}}, T_{\hat{L}} \rangle$  and  $N_{\hat{G}}/T_{\hat{G}}$  is the Weyl group of  $\hat{G}$ .  
 (iv) If  $q > 3$  then  $N_{\hat{L}} = N_{\hat{L}}(T_{\hat{L}})$ ,  $N_{\hat{S}} = N_{\hat{S}}(T_{\hat{S}})$  and  $N_G = N_G(T_G)$ .

**Lemma 2.21.** Let  $\hat{S}_1$  be a long subgroup of  $\hat{G}$  isomorphic to  $\mathrm{SL}(3, q)$ . Then

- (i)  $\hat{S}_1$  is conjugate to  $\hat{S}$ ,
- (ii) if  $\hat{L}_1 \in L^{\hat{G}}$  centralizes a long  $\mathrm{SL}(2, q)$  subgroup of  $\hat{S}_1$ , then the pair  $(\hat{S}_1, \hat{L}_1)$  is conjugate in  $\hat{G}$  to  $(\hat{S}, \hat{L})$ , and
- (iii) if  $\hat{S}_1$  contains  $\hat{X}_\nu$  then  $\mathrm{O}_p(\mathrm{C}_{\hat{S}_1}(\hat{X}_\nu)) \leq \hat{Q}$ .

*Proof.* (i) See [Coo] or [LS].

(ii)  $\hat{S}$  is transitive on its long  $\mathrm{SL}(2, q)$  subgroups.

(iii) Since the pair  $(\hat{S}_1, \hat{X}_\nu)$  is conjugate in  $\hat{G}$  to  $(\hat{S}, \hat{X}_\nu)$ , we may assume that  $\hat{S}_1 = \hat{S}$ . Then  $\mathrm{O}_p(\mathrm{C}_{\hat{S}}(\hat{X}_\nu)) = \hat{X}_{\nu'} \hat{X}_\nu \hat{X}_{\nu-\nu'} \leq \hat{Q}$ . □

**Lemma 2.22.**  $\hat{G}$  acts transitively by conjugation on the set of all 4-tuples  $(\hat{L}_1, \hat{S}_1, T_{\hat{L}_1}, T_{\hat{S}_1})$  with  $\hat{L}_1 \in \hat{L}^{\hat{G}}$ ,  $\mathrm{C}_{\hat{G}}(\hat{L}_1)' < \hat{S}_1 \in \hat{S}^{\hat{G}}$ , and  $T_{\hat{L}_1}$  and  $T_{\hat{S}_1}$  maximally split tori of  $\hat{L}_1$  and  $\hat{S}_1$ , respectively, containing  $\hat{S}_1 \cap \hat{L}_1$ .

Moreover,  $\hat{L}$  and  $\hat{S} \cap \hat{L}$  uniquely determine  $\hat{S}$ . Finally, if  $q > 3$  then  $T := T_{\hat{L}_1} T_{\hat{S}_1}$  is a maximally split torus of  $\hat{G}$ , and  $N/T \cong W$ , where  $N = N_{\hat{G}}(T) = \langle N_{\hat{L}_1}(T_{\hat{L}_1}), N_{\hat{S}_1}(T_{\hat{S}_1}) \rangle$ .

*Proof.* The preceding lemma already handles the pairs  $(\hat{L}_1, \hat{S}_1)$ . Consider our subgroups  $\hat{L}, \hat{S}$  and the 1-dimensional torus  $\hat{A} := \hat{S} \cap \hat{L}$ . Since  $\mathrm{C}_{\hat{G}}(\hat{A})$  is reductive, all of its maximally split tori are conjugate and contain  $\hat{A}$ . Since  $T_{\hat{L}} = \hat{L} \cap T_{\hat{G}}$ , this handles the triples  $(\hat{L}_1, \hat{S}_1, T_{\hat{L}_1})$ .

Clearly  $\hat{L} > \mathrm{C}_{\hat{L}}(\hat{A}) = \mathrm{C}_{\hat{G}}(\hat{A}\hat{R}) \geq \mathrm{C}_{\hat{G}}(\hat{S})$ , where  $\mathrm{C}_{\hat{G}}(\hat{S})$  is generated by  $Z(\hat{G})$  and long root groups. If  $\hat{M}$  is the subgroup of  $\mathrm{C}_{\hat{L}}(\hat{A})$  generated by its long root groups, by examining [Ka1, Coo, LS] we find that  $\hat{M}Z(\hat{G}) = \mathrm{C}_{\hat{G}}(\hat{S})$ . Thus,  $\hat{L}$  and  $\hat{A}$  determine  $\hat{S} = \mathrm{C}_{\hat{G}}(\hat{M})'$ . (In fact,  $\mathrm{C}_{\hat{G}}(\hat{M})' = \mathrm{C}_{\hat{G}}(\hat{M})$  using [LSS, Table 5.1].)

All maximal split tori of  $\hat{S}$  containing  $\hat{A}$  are  $\hat{R}$ -conjugate (as is seen by using a basis of the 3-space underlying  $\hat{S}$  with respect to which  $\hat{A} = \mathrm{C}_{\hat{S}}(\hat{R})$  consists of all matrices  $\mathrm{diag}(\lambda, \lambda, \lambda^{-2})$ ). Since  $\hat{R}$  normalizes  $\hat{L}, \hat{S}$  and  $T_{\hat{L}}$ , this proves the stated transitivity.

The final statements follow from Lemma 2.20. □

The long subgroups  $\hat{J} \cong \text{Spin}_8^-(q)$ .

**Lemma 2.23.** *There are long subgroups  $\hat{J} \cong \text{Spin}_8^-(q)$  containing  $\hat{S}$ .*

*Proof.* Each group  $\hat{G}$  has a long subgroup  $F_4(q)$  containing  $\hat{S}$ . Then it suffices to consider the case  $\hat{G} = F_4(q)$ , where there is a root subsystem subgroup  $\text{Spin}_9(q)$  containing a conjugate of  $\hat{S}$  that lies in a subgroup  $\text{Spin}_8^-(q)$ .  $\square$

**2.2. Primitive prime divisors.** When the rank is  $> 2$ , we will always assume that  $q > 9$  in order to avoid difficulties occurring in the next lemma for small fields. Remark 1 in Section 4 discusses some of the omitted  $q$ .

**Lemma 2.24.** *Let  $pl$  be as follows for the indicated types of  $\hat{G}$ :*

$$pl = \begin{cases} p \cdot \text{ppd}^\#(p; 2e)\text{ppd}^\#(p; 6e) & F_4 \\ p \cdot \text{ppd}^\#(p; 2e)\text{ppd}^\#(p; 3e)\text{ppd}^\#(p; 6e) & E_6 \\ p \cdot \text{ppd}^\#(p; e)\text{ppd}^\#(p; 3e)\text{ppd}^\#(p; 6e) & {}^2E_6 \\ p \cdot \text{ppd}^\#(p; e)\text{ppd}^\#(p; 2e)\text{ppd}^\#(p; 3e)\text{ppd}^\#(p; 6e) & E_7 \\ p \cdot \text{ppd}^\#(p; 4e)\text{ppd}^\#(p; 8e) & E_7 \\ p \cdot \text{ppd}^\#(p; 2e)\text{ppd}^\#(p; 4e)\text{ppd}^\#(p; 8e) & E_8 \\ p \cdot \text{ppd}^\#(p; 2e)\text{ppd}^\#(p; 18e) & E_8. \end{cases}$$

Let  $\varpi = \varpi(\hat{G})$  denote the  $p'$ -part of  $|\hat{G}|$ .

- (i) *If  $\tau \in \hat{G}$  has order of the form  $pl$ , then  $\tau^\varpi$  is a long root element or  $\hat{G}$  has type  $F_4$  and  $\tau^\varpi$  is either a long or a short root element.*
- (ii) *With probability  $\geq 1/315q$ , an element  $\tau \in \hat{G}$  has order of the form  $pl$  and  $\tau^\varpi$  is a long root element.*

*Proof.* We first construct elements  $\tau$  of the stated orders. In (2.15) we provided information concerning the centralizer of both a long root element and of  $\hat{R}$ , a long root  $\text{SL}(2, q)$ , together with the orders of one or two maximal tori  $\hat{T}_*$  in that centralizer. We will choose  $\tau \in \hat{T}_*\hat{R}$ . The integers required in the definition of  $l$  exist by [Zs] or the definition of  $\text{ppd}^\#$  in Section 1.1.

These tori are constructed as follows.

- In  $\hat{F}_4(q)$  a subgroup  $\text{Sp}(6, q)$  centralizing a long root group has a cyclic maximal torus of order  $q^3 + 1$ .
- In  $\hat{E}_6(q)$  or  ${}^2\hat{E}_6(q)$  a subgroup  $\text{SL}(6, q)$  or  $\text{SU}(6, q)$  centralizing a long root group has a cyclic maximal torus of order  $(q^6 - 1)/(q - 1)$  or  $(q^6 - 1)/(q + 1)$ , respectively.
- In  $\hat{E}_7(q)$  a subgroup  $\text{Spin}_{12}^+(q)$  centralizing a long root group contains subgroups  $\text{GL}(6, q)$  and  $\text{Spin}_8^-(q) \circ \text{Spin}_4^-(q)$ , which produce the tori in (2.15).
- In  $\hat{E}_8(q)$  a subgroup  $\hat{E}_7(q)$  centralizing a long root group contains subgroups of type  $\text{SL}(8, q)$  (more precisely, its quotient by a central subgroup of order  $(2, q - 1)$ ) and  $\mathbb{Z}_{q+1} \circ {}^2\hat{E}_6(q)$ , producing the tori in (2.15).

(i) By the Borel-Tits Lemma [GLS, Theorem 3.1.3],  $\tau$  lies in a parabolic subgroup  $U \rtimes L$  of  $\hat{G}$ , with  $U$  unipotent containing  $\tau^\varpi$  and  $L$  a Levi factor containing  $Z(\hat{G})$ . Thus, we need to consider the possibility that a  $p'$ -element of  $L$  of order given in the lemma centralizes a nontrivial element of  $U$ .

An examination of the Levi factors that contain elements of order  $l$  produces the following possibilities: the normalizer of a long root group; a parabolic of type  $q^{7+8} : \hat{E}_3(q)$  in  $\hat{F}_4(q)$  (and then  $\tau^\infty$  is a short root element); a parabolic of type  $q^{2+6+12} : (\text{SL}_2(q) \circ \text{SL}_3(q^2))$  in  ${}^2\hat{E}_6(q)$  (and then an element of order  $l$  fixes no nontrivial element of the unipotent radical); a parabolic of type  $q^{7+35} : \hat{A}_6(q)$  in  $\hat{E}_7(q)$  (and then an element of order  $l$  fixes no nontrivial element of the unipotent radical); and a parabolic of type  $q^{8+28+56} : \hat{A}_7(q)$  in  $\hat{E}_8(q)$  (and then an element of order  $l$  fixes no nontrivial element of the unipotent radical). Here we used [FJ] in the last of these in order to verify the statements about  $\tau^\lambda$ ; references such as [Shi, Sho, Ca2] can also be used for other cases.

(ii) We have  $C_{\hat{L}}(\tau^p) = \hat{T}_*$  in the previous description of one type of  $\tau$ . Also, we have  $|\text{N}_{\hat{G}}(\hat{T}_*\hat{R})|/|\hat{T}_*||\hat{R}| \leq |\text{N}_{\hat{L}}(\hat{T}_*) : C_{\hat{L}}(\hat{T}_*)| \leq 72$  for each of the possible tori  $\hat{T}_*$ .

Thus, there are  $|\hat{G} : \text{N}_{\hat{G}}(\hat{T}_*\hat{R})| \geq |\hat{G}|/72|\hat{T}_*||\hat{R}|$  conjugates of  $\hat{T}_*\hat{R}$ . Even in the exceptional ppd<sup>#</sup> cases (Mersenne primes, Fermat primes and  $2^6 - 1$  in Section 1.1), each such conjugate has at least  $|\hat{T}_*|(1 - 1/2)(1 - 1/3)(1 - 1/5)(1 - 1/7) = |\hat{T}_*|(8/35)$  elements  $\tau^p$  of the required  $p'$ -order (since  $l$  has at most four ppd-factors) and  $|\hat{R}|/q$  elements of order  $p$ . Thus, in each case the number of elements  $\tau$  is at least  $(|\hat{G}|/72)(8/35)(1/q) = |\hat{G}|/315q$ . □

The proof shows that the probability is better than stated. First of all, 2 is never a primitive prime divisor, and in all but one case there are only two or three ppd-factors rather than four. However, for simplicity we will use the estimate  $1/315q$ .

*Notation.* If  $\hat{G}$  is of type  $E_7$  or  $E_8$ , then there are two choices for  $l$  in the above lemma. We will call these  $l$  and  $l_0$ .

**Lemma 2.25.** *Let  $\hat{R}_1$  be a long  $\text{SL}(2, q)$  contained in  $\hat{L}$ , and let  $l$  (or  $l$  and  $l_0$ ) be as in the preceding lemma.*

- (i) *If  $\hat{G}$  is not of type  $E_7$  or  $E_8$  and if  $g \in \hat{L}$  has order  $l$ , then  $\hat{L} = \langle \hat{R}_1, g \rangle$ .*
- (ii) *If  $\hat{G}$  is of type  $E_7$  or  $E_8$  and if  $g \in \hat{L}$  has order  $l$  and  $g_0 \in \hat{L}$  has order  $l_0$ , then  $\hat{L} = \langle \hat{R}_1, g, g_0 \rangle$ .*

*Proof.* Let  $\hat{K} := \langle \hat{R}_1^{(g)} \rangle$  (or  $\langle \hat{R}_1^{(g, g_0)} \rangle$  in (ii)). Since  $\hat{K}$  is normalized by  $g$  (and  $g_0$ ), as above the resulting ppd-factors of  $|\text{N}_{\hat{G}}(\hat{K})|$  and the Borel-Tits Lemma imply that  $\text{O}_p(\hat{K}) = 1$ . Using  $|\text{N}_{\hat{G}}(\hat{K})|$  and the lists in [Ka1, Coo, LS], we see that  $\hat{K} = \hat{L}$ . □

**2.3. Probability and long root elements.** Next we will study the probabilistic behavior of some subgroups of  $\hat{G}$  generated by 2, 3 or 4 long root elements or groups. We assume that  $q > 9$ . Recall that  $\hat{Z} = \hat{X}_\nu$ .

**Lemma 2.26.** *If  $z$  is a long root element, then a randomly chosen long root element  $z'$  is opposite  $z$  with probability  $> 1/3$ . Moreover, with probability  $> 1/12$ , for a randomly chosen long root element  $z'$  either  $\langle z, z' \rangle \cong \text{SL}(2, q)$  or  $p = 2$  and  $\langle z, z' \rangle$  is dihedral of order  $2\text{ppd}^\#(2e, p)$ .*

*Proof.* We may assume that  $z \in \hat{Z}$ . The unipotent radical  $\hat{Q} = \text{O}_p(C_{\hat{G}}(\hat{Z}))$  acts regularly on the set of root groups opposite  $\hat{Z}$ . Then the total number of long root elements opposite  $z$  is  $(q - 1)|\hat{Q}|$ , while the total number of long root elements is  $|\hat{G} : C_{\hat{G}}(z)|$ . Hence, the desired probability is the ratio of these integers, and it is straightforward to check the lower bound  $1/3$  in all cases.

TABLE 1. Number of root  $SL(3, q)$  that contain a given long root  $SL(2, q)$

$\hat{G}$	$n(\hat{S}, \hat{R})$	$q$ -exponent
$G_2(q)$	$\frac{q(q+1)}{2}$	2
${}^3D_4(q)$	$\frac{q^3(q^3+1)}{2}$	6
$F_4(q)$	$\frac{q^6(q^3+1)(q^4-1)}{2(q-1)}$	12
$E_6(q)$	$\frac{q^9(q^3+1)(q^2+1)(q^5-1)}{2(q-1)}$	18
${}^2E_6(q)$	$\frac{q^9(q+1)(q^3+1)(q^5+1)}{2}$	18
$E_7(q)$	$\frac{q^{15}(q^3+1)(q^5+1)(q^8-1)}{2(q-1)}$	30
$E_8(q)$	$\frac{q^{27}(q^9+1)(q^5+1)(q^{14}-1)}{2(q-1)}$	54

Each opposite pair  $z, z'$  lies in a unique long  $SL(2, q)$ . Two elements of order  $p$  in that  $SL(2, q)$  generate the required type of subgroup with probability  $\geq 1/4$  [KS1, Lemma 3.8(iii)].  $\square$

We next turn to generating the long root subgroups  $\hat{S} = SL(3, q)$  and  $\hat{J} = Spin_{\bar{g}}(q)$  appearing in (2.19) and Lemma 2.23. Let  $\hat{R}$  be as in (2.13).

Let  $n(\hat{S}, \hat{R})$  denote the number of conjugates of  $\hat{S}$  containing  $\hat{R}$ , and  $n(\hat{J}, \hat{S})$  the number of conjugates of  $\hat{J}$  containing  $\hat{S}$ . All members of  $\hat{R}^{\hat{G}}$  lying in  $\hat{S}$  are  $\hat{S}$ -conjugate, and all members of  $\hat{S}^{\hat{G}}$  lying in  $\hat{J}$  are  $\hat{J}$ -conjugate. Therefore, the numbers  $n(\mathbf{X}, \mathbf{Y})$ ,  $(\mathbf{X}, \mathbf{Y}) = (\hat{S}, \hat{R})$  or  $(\hat{J}, \hat{S})$  can be obtained from Tables 1 and 2 by simplifying the obvious formula to

$$n(\mathbf{X}, \mathbf{Y}) = \frac{|N_{\hat{G}}(\mathbf{Y})||\mathbf{X}|}{|N_{\hat{G}}(\mathbf{X})||N_{\mathbf{X}}(\mathbf{Y})|}.$$

**Lemma 2.27.** *Let  $\hat{R}, \hat{S}$  and  $\hat{J}$  be as before.*

- (i) *The probability is at least  $1/3$  that  $\hat{R}$ , together with a conjugate of  $\hat{Z}$  opposite  $\hat{Z}$ , generate a conjugate of  $\hat{S}$ .*
- (ii) *The probability is at least  $1/3$  that  $\hat{S}$ , together with a conjugate of  $\hat{Z}$ , generate a conjugate of  $\hat{J}$ .*

*Proof.* For  $(\mathbf{X}, \mathbf{Y}) = (\hat{S}, \hat{R})$  or  $(\hat{J}, \hat{S})$ , the desired probability is at least  $n(\mathbf{X}, \mathbf{Y})\beta/|\hat{Q}|$ , where  $\beta$  is the number of conjugates  $\hat{Z}'$  of  $\hat{Z}$  inside  $\mathbf{X}$  that are opposite  $\hat{Z}$  and satisfy  $\mathbf{X} = \langle \mathbf{Y}, \hat{Z}' \rangle$  (recall that  $|\hat{Q}|$  is the number of  $\hat{G}$ -conjugates of  $\hat{Z}$  opposite  $\hat{Z}$ ). From Tables 1 and 2 we obtain  $n(\hat{S}, \hat{R})/|\hat{Q}| \geq 4q^{-3}/9$  and  $n(\hat{J}, \hat{S})/|\hat{Q}| \geq q^{-9}(1-q^{-3})^2/2$ . It remains to estimate  $\beta$  in our two cases.

TABLE 2. Number of root  $\text{Spin}_8^-(q)$  that contain a given long root  $\text{SL}(3, q)$

$\hat{G}$	$n(\hat{J}, \hat{S})$	$q$ -exponent
$F_4(q)$	$\frac{q^3(q^3 - 1)}{2}$	6
$E_6(q)$	$\frac{q^6(q^3 - 1)^2}{2}$	12
${}^2E_6(q)$	$\frac{q^6(q^3 + 1)^2}{2}$	12
$E_7(q)$	$\frac{q^{12}(q^6 - 1)(q^5 - 1)(q^3 - 1)}{2(q^2 - 1)}$	24
$E_8(q)$	$\frac{q^{24}(q^{12} - 1)(q^9 - 1)(q^5 - 1)}{2(q^2 - 1)}$	48

(i) Let  $V$  be the natural module for  $\hat{S} = \text{SL}(3, q)$ . Then  $V = [V, \hat{R}] \oplus C_V(\hat{R})$ , and the only maximal overgroups of  $\hat{R}$  in  $\hat{S}$  are the parabolics  $N_{\hat{S}}([V, \hat{R}])$  and  $N_{\hat{S}}(C_V(\hat{R}))$ . If  $\hat{Z}' < \hat{S}$  is a conjugate of  $\hat{Z}$  opposite  $\hat{Z}$ , then  $[V, \hat{R}] \neq C_V(\hat{Z}')$  and  $C_V(\hat{R}) \neq [V, \hat{Z}']$ .

Thus, if also  $\hat{S} > \langle \hat{R}, \hat{Z}' \rangle$ , then either  $[V, \hat{R}] > [V, \hat{Z}']$  or  $C_V(\hat{R}) < C_V(\hat{Z}')$ . There are at most  $2q^2$  such  $\hat{Z}'$  out of the  $q^3$  opposite  $\hat{Z}$ . Thus  $\beta \geq q^3 - 2q^2$ , and the desired probability is at least  $(4q^{-3}/9)(q^3 - 2q^2) > 1/3$ .

(ii) Let  $V$  be the natural 8-dimensional module for  $\Omega^-(8, q)$ ; we will view all subgroups of  $\hat{J}$  as subgroups of  $\Omega^-(8, q)$ . Then  $\hat{S}$  splits  $V$  as  $V = V_6^+ \perp V_2^-$ . Long root groups  $\hat{Z}'$  correspond to totally singular 2-spaces  $T$  of  $V$  via  $T = [V, \hat{Z}']$ . If  $V = \langle T, V_6^+ \rangle$  then  $T^\perp \cap V_2^- = 0$  (as otherwise  $T$  and  $V_6^+$  would lie in a 7-space). Consequently,  $\langle \hat{S}, \hat{Z}' \rangle$  is an irreducible subgroup of  $\hat{J}$  generated by long root groups, and hence is  $\hat{J}$  [Ka1, LS].

Thus, we only need to estimate the number of totally singular 2-spaces *not* spanning  $V$  together with  $V_6^+$ . Each such 2-space contains a point of  $V_6^+$ . Since  $V_6^+$  has  $(q^2 + q + 1)(q^2 + 1)$  singular points and each is contained in  $(q^3 + 1)(q + 1)$  totally singular 2-spaces, there are at most  $(q^2 + q + 1)(q^2 + 1)(q^3 + 1)(q + 1) < 3q^8$  totally singular 2-spaces meeting  $V_6^+$  (as  $q > 9$ ). There are  $q^9$  long root groups in  $\hat{J}$  opposite  $\hat{Z}$ . It follows that  $\beta \geq q^9 - 3q^8$ , so that the desired probability is at least  $(q^9 - 3q^8) \cdot q^{-9}(1 - q^{-3})^2/2 \geq 1/3$ .  $\square$

We will need variations on the previous arguments:

- Lemma 2.28.** (i) *Suppose that  $D$  is a subgroup generated by opposite long root elements  $z, z'$  such that either  $D \cong \text{SL}(2, q)$  or  $q$  is even and  $D$  is dihedral of order  $2\text{ppd}^\#(2e, 2)$ . Then the probability is at least  $1/4$  that  $D$ , together with a conjugate  $y$  of  $z$  opposite  $z$ , generate a conjugate of  $\hat{S}$ .*
- (ii) *The probability is at least  $1/3$  that  $C_{\hat{S}}(\hat{R}) = \hat{S} \cap \hat{L}$  and a random conjugate  $\hat{S}^l$ ,  $l \in \hat{L}$ , generate a  $\hat{G}$ -conjugate of  $\hat{J}$  having an element normalizing  $\hat{R}$  and conjugating  $C_{\hat{S}}(\hat{R})$  into  $\hat{S}^l$ .*

*Proof.* (i) By Lemma 2.27(i), with probability at least  $1/3$  the three root groups containing  $z, z'$  or  $y$  generate a conjugate of  $\hat{S}$ . Thus, we only need a lower bound on the conditional probability that  $\hat{S} = \langle D, y \rangle$  for a root element  $y \in \hat{S}$  opposite  $z$ .

In view of the structure of  $D$ , the only maximal overgroups of  $D$  in  $\hat{S}$  are  $N_{\hat{S}}([V, D])$  and  $N_{\hat{S}}(C_V(D))$  (compare [KS1, Lemma 3.7]). Define  $\beta$  as at the start of the proof of Lemma 2.27. Then at least  $\beta(q - 1)$  of the  $q^3(q - 1)$  root elements in  $\hat{S}$  opposite  $z$  generate  $\hat{S}$  together with  $D$ , so that the desired probability is at least  $(1/3)\beta(q - 1)/q^3(q - 1) \geq (q^3 - 2q^2)/3q^3 > 1/4$ .

(ii) Somewhat as in Lemma 2.27(ii),

$$(2.29) \quad \hat{S} \text{ and } \hat{S}^l \text{ generate a long Spin}_8^-(q) \text{ subgroup with probability } > 1/4.$$

For, the number of “good” conjugates  $\hat{S}^l$  such that  $\langle \hat{S}, \hat{S}^l \rangle \in \hat{J}^{\hat{G}}$  is  $n(\hat{J}, \hat{S}) \cdot \gamma$ , where  $n(\hat{J}, \hat{S})$  is in Table 2 and  $\gamma$  is the number of good  $\hat{S}^l$  per  $\hat{J}$ -conjugate containing  $\hat{S}$ . On the other hand,  $|\hat{S}^{\hat{L}}|$  is just the number  $n(\hat{S}, \hat{R})$  of conjugates of  $\hat{S}$  containing  $\hat{R}$  (by Lemma 2.21). Thus, the desired probability is  $n(\hat{J}, \hat{S})\gamma/n(\hat{S}, \hat{R})$ . We will provide a lower bound for  $\gamma$ , from which (2.29) will follow using Tables 1 and 2.

For this purpose, we restrict our attention to the 8-space  $V$  associated with  $\hat{J}$ . As for the preceding lemma,  $\hat{S}^l$  is good if (and only if)  $\langle \hat{S}, \hat{S}^l \rangle$  is irreducible on  $V$ .

If  $V_6^+ := [V, \hat{S}]$ , then  $V_6^+ = U_3 \oplus U_3^*$  for totally singular  $\hat{S}$ -invariant 3-spaces  $U_3, U_3^*$ . Also,  $[V, \hat{R}]$  is a nondegenerate 4-space of type + meeting  $U_3, U_3^*$  at 2-spaces  $U_2, U_2^*$ , respectively.

Since  $l$  centralizes  $\hat{R}$ , the totally singular 3-spaces  $U_3^l, U_3^{*l}$  meet  $[V, \hat{R}]$  in totally singular 2-spaces  $\tilde{U}_2 := U_2^l, \tilde{U}_2^* := U_2^{*l}$ , lying in the same “half” of the set of totally singular 2-spaces of  $[V, \hat{R}]$  as  $U_2, U_2^*$  (this “half” consists of  $q + 1$  totally singular 2-spaces pairwise meeting in 0, all of which are  $\hat{R}$ -invariant); there are  $(q + 1)q$  such ordered pairs  $\tilde{U}_2, \tilde{U}_2^*$  of distinct 2-spaces. Each of the subspaces  $U_3^l, U_3^{*l}$  meets the 4<sup>-</sup>-space  $[V, \hat{R}]^\perp = \langle \tilde{U}_2, \tilde{U}_2^* \rangle^\perp$  in a singular point; there are  $(q^2 + 1)q^2$  ordered pairs  $p_1, p_2$  of distinct singular points in  $[V, \hat{R}]^\perp$ . Each such ordered pairs of 2-spaces and of points determine a unique ordered pair  $\langle \tilde{U}_2, p_1 \rangle, \langle \tilde{U}_2^*, p_2 \rangle$  of totally singular 3-spaces left invariant by a conjugate  $\hat{S}^l$ , and each  $\hat{S}^l$  arises this way exactly twice (twice because the ordered pairs  $\tilde{U}_2, \tilde{U}_2^*$  and  $p_1, p_2$  determine the same conjugate of  $\hat{S}$  as the ordered pairs  $\tilde{U}_2^*, \tilde{U}_2$  and  $p_2, p_1$ ). Of the pairs  $p_1, p_2$  of singular points,  $q^2 - 1$  points  $p_1$  do not lie in  $V_6^+$  and at least  $q^2 - 1 - (q - 1)$  points  $p_2$  do not lie in  $\langle V_6^+, p_1 \rangle$ , in which case  $V = \langle V_6^+, p_1, p_2 \rangle = \langle U_3, U_3^*, U_3^l, U_3^{*l} \rangle$  and  $\langle \hat{S}, \hat{S}^l \rangle$  is irreducible. Thus,  $2\gamma \geq (q + 1)q \cdot (q^2 - 1)(q^2 - q)$ . Now Tables 1 and 2 yield (2.29).

Let  $\hat{A} := \hat{S} \cap \hat{L}$ . It remains to show that  $\langle \hat{S}^l, \hat{A} \rangle \cong \hat{J}$ ,  $l \in L$ , assuming that  $\langle \hat{S}, \hat{S}^l \rangle \cong \hat{J}$ . Instead of this it will be more convenient to show that  $\langle \hat{S}, \hat{A}^l \rangle = \hat{J}$ ,  $l \in L$ , assuming that  $\langle \hat{S}, \hat{S}^l \rangle = \hat{J}$ .

If  $\langle \hat{S}, \hat{A}^l \rangle$  is irreducible on  $V$  then so is  $\langle \hat{S}^{\langle \hat{S}, \hat{A}^l \rangle} \rangle$ , and then both of these groups are  $\hat{J}$  using [Ka1, LS]. Moreover,  $\hat{S}$  and  $\hat{S}^l$  are long  $SL(3, q)$ -subgroups of  $\hat{J}$  containing  $\hat{R}$ , and hence are conjugate under  $N_j(\hat{R})$  (cf. Lemma 2.21(ii)). Then  $\hat{A}^{lj} < \hat{S}^{lj} = \hat{S}$  for some  $j \in N_j(\hat{R})$ , as required in (ii).

We will assume that  $\langle \hat{S}, \hat{A}^l \rangle$  is reducible and obtain a contradiction. A generator of  $\hat{A}^l = C_{\hat{S}^l}(\hat{R})$  acts on  $V$  by centralizing a 2<sup>-</sup>-space (hence with eigenvalue 1 there) while acting on  $V_6^{+l}$  with two invariant totally singular 3-spaces  $U_3^l, U_3^{*l}$  and eigenvalues on them of the form  $\lambda, \lambda, \lambda^{-2}$  and  $\lambda^{-1}, \lambda^{-1}, \lambda^2$ , respectively, where  $\lambda$

has order  $q - 1$ . In particular,  $C_{V_6^{+l}}(\hat{A}^l) = 0$  since  $q > 3$ , so that  $C_V(\hat{A}^l)$  has no singular points. Thus, the only totally singular 3-spaces left invariant by  $\hat{A}^l$  are contained in  $V_6^{+l}$ .

Any proper  $\langle \hat{S}, \hat{A}^l \rangle$ -invariant subspace  $W$  of smallest dimension must be totally singular or nondegenerate. Clearly  $\hat{S}$  and  $\hat{A}^l$  have no fixed common nonzero vector since  $C_V(\hat{S}^l) = C_V(\hat{A}^l)$  and  $\hat{J} = \langle \hat{S}, \hat{S}^l \rangle$ . Thus,  $W$  is  $U_3$  or  $U_3^*$ , and yet we have seen that it must be contained in  $V_6^{+l}$ . Then the 6-spaces  $V_6^+ = [V, \hat{S}]$  and  $V_6^{+l} = [V, \hat{A}^l]$  both contain both  $W$  and the 4<sup>+</sup>-space  $[V, \hat{R}]$ , and those span at least a 5-space. Thus,  $\langle [V, \hat{S}], [V, \hat{S}^l] \rangle = \langle [V, \hat{S}], [V, \hat{A}^l] \rangle < V$  and  $\langle \hat{S}, \hat{S}^l \rangle$  is reducible. This is the desired contradiction. □

**2.4. Start of the proof of Theorem 1.1.** We are given a black box group  $G$  that is a nontrivial epimorphic image of the universal cover  $\hat{G}$  of an exceptional group of Lie type of rank  $> 2$  over a field of order  $q > 9$ . Therefore  $\hat{G}$  is the simply connected cover [GLS, p. 313]. We start by using the Monte Carlo algorithm in [BKPS] in order to (probably) find the type of group we are dealing with. Similarly, every time we call an existing constructive recognition algorithm in Theorem 1.3 we assume that [BKPS] has first been used in order to make it likely that we are testing a group having the desired structure: the algorithm in [BKPS] is far faster than any constructive recognition algorithm (such as Theorem 1.3), although these checks are not necessary for the proof of Theorem 1.1.

Eventually we will test that the group is, indeed, as expected: in Proposition 2.33 and Corollary 2.42 we will verify a presentation (2.2)–(2.5) or (2.6) for  $G$ . Such a presentation is also crucial for uses of Theorem 1.1, such as those in [KS2, LG].

**2.5. Finding a long root element.** Choose up to  $3150q$  elements  $\tau \in G$  until one is found such that  $|\tau| = pl$  for  $l$  in Lemma 2.24. When we obtain  $\tau$  of the desired sort, Lemma 2.24(i) states that  $z := \tau^\varpi$  is a long root element, or possibly a short one when  $G$  has type  $F_4$ . For the latter groups we proceed somewhat differently.

Suppose that  $G$  has type  $F_4$ . If  $q$  is even, then the graph automorphism sends short root elements to long ones, so we may assume that  $z$  is long. If  $q$  is odd, then we run the algorithm up to  $3200q$  times, from finding  $\tau$  until the group  $L$  is constructed and tested at the start of Section 2.9 (specifically, we find  $\tau$  and then find and test  $z', y, S, S_2, Z_1, J$  and  $L$ ).

*Remark 2.30 (Correctness).* There is no subgroup of  $F_4(q)$ ,  $q$  odd, generated by short root elements and isomorphic to  $\text{Sp}(6, q)$ . For,  $F_4(q)$  has exactly 2 classes of involutions, with centralizers  $\text{Spin}_9(q)$  and  $(\text{SL}(2, q) \circ \text{Sp}(6, q)) \cdot 2$  (for a long  $\text{SL}(2, q)$ ) [Sho]; only the latter type has a subgroup  $\text{Sp}(6, q)$ , and the long root groups in  $\text{Sp}(6, q)$  are also long for  $G$ . Thus, if we obtain a subgroup  $L \cong \text{Sp}(6, q)$ , then  $z$  is a long root element.

There are other ways to handle this odd case. For example, the group generated by 4 conjugates of a long root element is isomorphic to  $\text{Spin}_{\bar{8}}(q)$  with probability  $\geq 1/16$ , but the same is not true for short root elements, once again by using the nature of the centralizers of the 2 classes of involutions noted above. In Section 4, Remark 6, this ambiguity is avoided by using an entirely different approach that finds the involution in  $R$  and then its centralizer in  $G$ .



For the cases  $E_7(q)$  and  $E_8(q)$  there are two possibilities,  $l, l_0$ , in Lemma 2.24, and hence we also find a second element  $\tau_0$  of order  $pl_0$ . Then  $z_0 := \tau^\varpi$  is a long root element.

**Reliability:**  $\geq 1 - 1/2^9$  for  $\tau$  and  $\tau_0$  in all but the exceptional  $F_4$  case. For, all  $\tau$  fail to have the required order with probability  $\leq (1 - 1/315q)^{3150q} < 1/2^{10}$ , by Lemma 2.24.

In the exceptional  $F_4$  case, for a given choice  $\tau$ , if  $z$  is a long root element, then we will succeed at showing this and finding the needed elements and subgroups with probability  $\geq 1 - 1/2^8$  (in view of the individual probabilities in the next sections). Hence, we will succeed for a given  $\tau$  with probability  $\geq (1/315q)(1 - 1/2^8) > 1/320q$ . All  $3200q$  repetitions fail with probability  $< (1 - 1/320q)^{3200q} < 1/2^{10}$ .

**Time:**  $O(q[\xi + \mu \log^2 q])$  to choose elements  $\tau$  (and  $\tau_0$ ) and to test the order of each of them using [KS1, Lemma 2.7], but  $O(\xi q \log q + \mu q \log^2 q)$  if the  $F_4$  test is needed.

**2.6. Matching up root elements.** For the cases  $E_7(q)$  and  $E_8(q)$  we have two elements  $\tau$  and  $\tau_0$ , and we have powers  $z$  and  $z_0$  of them that are long root elements. We need to arrange to have  $\langle z \rangle = \langle z_0 \rangle$ .

Repeat up to 240 times: choose a conjugate  $z_1$  of  $z_0$ , test whether  $z$  and  $z_1$  are opposite and for odd  $q$  use Theorem 1.3(ii) to test whether  $\langle z, z_1 \rangle \cong \text{SL}(2, q)$  and, if so, to obtain a constructive isomorphism  $\text{SL}(2, q) \rightarrow \langle z, z_1 \rangle$ . If  $p = 2$  then  $\langle z, z_1 \rangle$  is dihedral of order dividing  $2(q \pm 1)$ .

For each  $q$  it is now easy to conjugate  $\langle z \rangle$  to  $\langle z_1 \rangle$  and hence to  $\langle z_0 \rangle$ .

Thus, we can conjugate  $\tau_0$  in order to arrange that  $\langle z \rangle = \langle \tau^\varpi \rangle = \langle \tau_0^\varpi \rangle = \langle z_0 \rangle$  (recall that  $\varpi$  denotes the  $p'$ -part of  $|\hat{G}|$ ).

**Reliability:**  $\geq 1 - 1/2^{10}$ . For, by Lemma 2.26,  $z_1$  is opposite  $z$  with probability  $> 1/3$ , and we use (2.12) to test this. If this occurs and  $q$  is even, then we are merely conjugating within a dihedral group.

If  $q$  is odd, then  $\langle z, z_1 \rangle \cong \text{SL}(2, q)$  with probability  $\geq 1/12$  (by Lemma 2.26), in which event Theorem 1.3 succeeds with probability  $> 1/2$ . Thus, all 240 repetitions fail with probability  $< (1 - 1/24)^{240} < 1/2^{10}$ .

**Time:**  $O(\xi q \log q + \mu q \log^2 q)$ , dominated by the time to find the constructive isomorphism.

**2.7. The subgroups  $R, Z, Z^-$  and  $S$ .** Choose up to  $10 \cdot 2^{12}$  pairs  $z', y$  of conjugates of  $z$ , and use (2.12) and Theorem 1.3(ii) in order to test whether both are opposite  $z$  and  $S := \langle z, z', y \rangle$  and  $S_2 := \langle z, z'^{\tau^p}, y \rangle$  are both isomorphic to  $\hat{S} = \text{SL}(3, q)$ ; and, if so, to find constructive isomorphisms  $\Psi_S: \hat{S} \rightarrow S$  and  $\Psi_{S_2}: \hat{S} \rightarrow S_2$ , together with generating sets  $\mathcal{S}_{\hat{S}}$  and  $\mathcal{S}_S^*$  of  $\hat{S}$  and  $S$ , respectively, such that  $\mathcal{S}_{\hat{S}}\Psi_S = \mathcal{S}_S^*$ . We may assume that  $\hat{S}$  is the subgroup of  $\hat{G}$  defined in (2.19); we will use the notation in (2.13).

Find  $R := \hat{R}\Psi_S < S$ ,  $Z := \hat{X}_\nu\Psi_S$  and  $Z^- := \hat{X}_{-\nu}\Psi_S$  using Theorem 1.3(iv). Then  $R = \langle Z, Z^- \rangle \cong \text{SL}(2, q)$ .

Conjugate within  $\hat{S}$  in order to have  $z \in Z$  and  $z' \in Z^-$ . Then  $\tau^p$  centralizes  $Z$  since it centralizes  $z \in Z$ . Find the root group  $Y < S$  containing  $y$ .

Use  $\Psi_{S_2}$  to find an element of  $\text{O}_p(C_{S_2}(Z))$  conjugating  $(Z^-)^{\tau^p}$  to  $Y$  (recall that  $Z$  and  $Y$  are opposite), and use  $\Psi_S$  to find an element of  $\text{O}_p(C_S(Z))$  conjugating  $Y$  to  $Z^-$ . The product of these two elements is an element  $c \in \text{O}_p(C_{s_2}(Z))\text{O}_p(C_S(Z)) \subseteq$

$Q := O_p(C_G(Z))$  such that  $(Z^-)^{\tau^{pc}} = Z^-$  (cf. Lemma 2.21(iii); of course we do not yet have  $Q$  to work with). Then  $\tau^{pc}$  and  $\tau^p$  are elements of  $C_G(Z)$  that agree mod  $Q$ , so that  $l$  divides the order of  $\tau^{pc}$ . Moreover,  $\tau^{pc}$  normalizes  $Z^-$  while centralizing  $Z$ .

Thus,  $\tau^{pc}$  centralizes  $R$  and has order divisible by  $l$ .

Recall from the preceding section that  $Z$  contains  $\langle z \rangle = \langle z_0 \rangle$  when  $G$  is of type  $E_7$  or  $E_8$ . In that case we have a second element  $\tau_0$ , and we obtain in the same way a second element  $\tau_0^p c_0$  of  $C_G(R)$ , this time of order divisible by  $l_0$ .

**Reliability:**  $\geq 1 - 1/2^9$ . For, both members of a pair  $z', y$  are opposite  $z$ , with  $z'$  behaving as in the second part of Lemma 2.26 and  $S, S_2 \cong \text{SL}(3, q)$ , with probability  $> (1/12)(1/3)(1/4)^2 > 1/2^{10}$  (by Lemmas 2.26 and 2.28(i)), in which case Theorem 1.3(ii) succeeds for both  $S$  and  $S_2$  with probability  $> (1/2)^2$ . Hence, all  $10 \cdot 2^{12}$  repetitions fail with probability  $< (1 - 1/2^{12})^{10 \cdot 2^{12}} < 1/2^{10}$ . The probability involved in repeating the above for  $\tau_0$ , if needed, is dealt with similarly.

**Time:**  $O(\xi q \log q + \mu q \log^2 q)$ , dominated by finding  $\Psi_S$  and  $\Psi_{S_2}$  using Theorem 1.3(ii).

**2.8. The long subgroups  $J$  and  $R_1$ .** Repeat up to 30 times: choose a conjugate  $Z_1$  of  $Z$ , and use Theorem 1.3(ii) in order to test whether  $J := \langle S, Z_1 \rangle \cong \text{Spin}_{\bar{8}}(q)$ ; and, if so, to obtain a constructive isomorphism  $\Psi_J: \text{Spin}_{\bar{8}}(q) \rightarrow J$ .

Find a long  $\text{SL}(2, q)$ -subgroup  $R_1 < C_J(R)$  using  $\Psi_J$ . *Obtaining this long  $\text{SL}(2, q)$  is the only use we have for  $J$  and  $\Psi_J$ .*

**Reliability:**  $\geq 1 - 1/2^{10}$  using Lemma 2.27(ii).

**Time:**  $O(\xi q \log q + \mu q \log^2 q)$ , dominated by finding  $\Psi_J$  using Theorem 1.3(ii).

**2.9. The subgroups  $L, T$  and  $N$ .** Let  $L := \langle R_1, \tau^p c \rangle$  or  $\langle R_1, \tau^p c, \tau_0^p c_0 \rangle$  in the cases  $F_4, E_6, {}^2E_6$  or  $E_7, E_8$ , respectively. The generators of  $L$  lie in  $C_G(R)$  (cf. Section 2.7). Hence,  $L = C_G(R)$  by Lemma 2.25.

The subgroups  $S$  and  $L$  behave as in Lemma 2.21(ii), and hence the pair  $S, L$  is uniquely determined up to conjugacy in  $G$ . In particular, we can use the information in Section 2.1 to study  $G$  by means of constructive isomorphisms for these subgroups. Note, however, that these isomorphisms might not match up properly, which will make us (possibly) have to modify the pair  $(S, L)$  in Lemma 2.32.

Use up to 10 repetitions of Theorem 1.3(ii), or recursion if  $G = E_8(q)$ , in order to find generating sets  $S_L^*$  of  $L$  and  $\hat{S}_L$  of  $\hat{L}$  and an isomorphism  $\Psi_L: \hat{L} \rightarrow L$  such that  $\hat{S}_L \Psi_L = S_L^*$ . Also find the following subgroups of  $G$  using (2.17) and (2.19):

$$T_L := T_{\hat{L}} \Psi_L, \quad T_S := T_{\hat{S}} \Psi_S, \quad N_L := N_{\hat{L}} \Psi_L \text{ and } N_S := N_{\hat{S}} \Psi_S.$$

(Recall that we already have a generating set  $S_S^*$  of  $S$ .) We will often use the fact that  $\Psi_S$  and  $\Psi_L$  are isomorphisms even though the target epimorphism  $\Psi = \Psi_G$  may not be bijective. In particular,  $\Psi_L^{-1}$  always produces a unique element of  $\hat{G}$ .

**Reliability:**  $\geq 1 - 1/2^{10}$ .

**Time:**  $O(\xi q \log q + \mu q \log^2 q)$ , dominated by finding  $\Psi_L$ .

*Remark 2.31.* A version of the presentation (2.2)–(2.5) or (2.6) is used for  $L$  as part of Theorem 1.3(ii). Conceivably this is not a subpresentation of the presentation (2.2)–(2.5) or (2.6) that we are using for  $\hat{G}$ : the signs may not agree. We assume

that, as part of the recursive call, the signs in the presentation (2.2)–(2.5) or (2.6) for  $\hat{L}$  have been changed so as to coincide with the corresponding ones for  $\hat{G}$ . Since we are only dealing with presentations of groups of small (bounded) rank, there are only a few sign changes required here.

**2.10. Matching up  $T_S$  and  $T_L$  in order to obtain  $T$ .** At this point it need not be the case that  $\langle T_S, T_L \rangle$  is a maximal torus of  $G$ . In order to guarantee this property we need to arrange for the 1-dimensional torus  $S \cap L$  of both  $S$  and  $L$  to lie in both of the tori  $T_S$  and  $T_L$ :

**Lemma 2.32.** *There is an algorithm replacing the pair  $(S, L)$  by a conjugate pair in order to have  $S \cap L = T_S \cap T_L$ . This algorithm is deterministic and runs in  $O(\mu q)$  time, except when  $G$  is  $E_8(q)$ , in which case it is Las Vegas, takes  $O(\xi q \log q + \mu q \log^2 q)$  time and succeeds with probability  $\geq 1 - 1/2^{10}$ .*

*Proof.* Recall from Section 2.7 that  $\hat{S}$  is the subgroup of  $\hat{G}$  defined in (2.19). Since  $R = \hat{R}\Psi_S$ , we can find  $S \cap L = C_S(R) = (C_{\hat{S}}(\hat{R}))\Psi_S$  using Theorem 1.3(iv). Since  $T_{\hat{S}}$  normalizes the root groups  $\hat{X}_\nu, \hat{X}_{-\nu}$  of  $\hat{R}$ ,  $T_{\hat{S}}$  contains  $C_{\hat{S}}(\hat{R})$  (using a basis of the 3-space for  $\hat{S}$  as in the proof of Lemma 2.22). Thus,  $S \cap L = (C_{\hat{S}}(\hat{R}))\Psi_S \leq T_{\hat{S}}\Psi_S = T_S$ .

We will provide two entirely different approaches to the remaining part of the proof: arranging to have  $S \cap L \leq T_L$ . The first is deterministic (as in the statement of the lemma) and simpler for  $G$  not of type  $E_8$ , while the second is more uniform. The timing in the lemma refers to the first method. (For rank 2 groups in Section 3 we will use the first method.)

**Method 1.** We initially assume that  $G$  does not have type  $E_8$ . Then  $\hat{L}$  is (essentially) a classical group (cf. (2.15)); let  $V$  be its natural module. (It will not matter that this module is not faithful when  $\hat{L}$  is a spin group.)

We have found the (cyclic) group  $S \cap L$  using  $S$ . Find  $\hat{A} := (S \cap L)\Psi_L^{-1}$  using Theorem 1.3(iii). Diagonalize  $\hat{A}$  on  $V$  using a hyperbolic basis that determines a maximal split torus  $\hat{T}$  of  $\hat{L}$  containing  $\hat{A}$ . Find  $\hat{l}$  in the classical group  $\hat{L}$  such that  $\hat{T}^{\hat{l}} = T_{\hat{L}}$  (this is just a basis change). Find  $l := \hat{l}\Psi_L$  using Theorem 1.3(iv). Replace  $S$  by  $S^l$  and  $T_S$  by  $T_S^l$ . (*Correctness:* We have  $S^l \cap L = (S \cap L)^l = \hat{A}^{\hat{l}}\Psi_L < \hat{T}^{\hat{l}}\Psi_L = T_{\hat{L}}\Psi_L$ , where the latter is  $T_L$  by definition in Section 2.9. Then  $S^l \cap L = (S \cap L)^l \leq T_S^l \cap T_L \leq S^l \cap L$  since  $S \cap L \leq T_S$ . Therefore, replacing  $S$  by  $S^l$  and  $T_S$  by  $T_S^l$  gives the desired equality  $S \cap L = T_S \cap T_L$ .)

If  $G$  has type  $E_8$  we again find  $\hat{A} := (S \cap L)\Psi_L^{-1}$ , using up to 10 recursive calls to Theorem 1.1(iii),(vii). Then the following are accomplished in the Appendix: find the Lie algebra of  $\hat{L} \cong \hat{E}_7(q)$ , then find a Chevalley basis producing a split torus of  $\hat{L}$  containing  $\hat{A}$ , and finally find  $\hat{l} \in \hat{L}$  conjugating this torus to the torus  $T_{\hat{L}}$  in (2.17). Find  $l := \hat{l}\Psi_L$  using another recursive call to Theorem 1.1, and replace  $S$  by  $S^l$  and  $T_S$  by  $T_S^l$ . (*Correctness:* Once again  $S^l \cap L \leq T_{\hat{L}}\Psi_L = T_L$ , and our replacement again gives  $S \cap L = T_S \cap T_L$ .)

**Method 2.** Find the subgroup  $A := (\hat{S} \cap \hat{L})\Psi_L$  of  $\hat{T}_{\hat{L}}\Psi_L = T_L$  using Theorem 1.3(iii).

Repeat up to 30 times: choose  $l \in L$ , use Theorem 1.3(a) to test whether  $\langle S^l, A \rangle \cong \text{Spin}_8^-(q)$  and, if so, use the resulting constructive isomorphism  $\text{Spin}_8^-(q) \rightarrow \langle S^l, A \rangle$  in order to find  $j \in \langle S^l, A \rangle$  that normalizes  $R$  and conjugates  $A$  into  $S^l$ . Let  $m := lj^{-1}$ . Replace  $S$  by  $S^m$  and  $T_S$  by  $T_S^m$ .

*Correctness:* There is an epimorphism  $\Psi: \hat{G} \rightarrow G$  extending  $\Psi_L$  and hence sending  $\hat{R}$  to  $R$ . Then  $\hat{S}\Psi$  contains  $\hat{R}\Psi = R$ , and  $A = (\hat{S} \cap \hat{L})\Psi_L = (\hat{S} \cap \hat{L})\Psi = \hat{S}\Psi \cap \hat{L}\Psi = C_{\hat{S}\Psi}(R)$  behaves as in Lemma 2.28(ii).

By that lemma, we may assume that  $\langle S^l, A \rangle$  is isomorphic to  $\text{Spin}_8^-(q)$  and has an element normalizing  $R$  and conjugating  $A$  into  $S^l$ . With  $m \in N_G(R)$  as above,  $A \leq S^m \cap L$ , so that  $A = S^m \cap L$  by Lemma 2.21(ii) since  $A = \hat{S}\Psi \cap L$ . Then  $A = (S \cap L)^m < T_S^m$  (by the start of the proof of this lemma), while  $A < T_L$  by definition. Thus,  $A \leq T_S^m \cap T_L \leq S^m \cap L = A$ . Replacing  $S$  by  $S^m$  and  $T_S$  by  $T_S^m$  gives  $T_S \cap T_L = S \cap L$ .

**Time:** Method 2 requires  $O(\xi q \log q + \mu q \log^2 q)$  time, dominated by the test for isomorphism with  $\text{Spin}_8^-(q)$ .

Method 1 uses Theorem 1.3(iii),(iv) for  $\Psi_L$ , and hence runs in  $O(\mu q \log q)$  time if  $G$  does not have type  $E_8$ . However, in the  $E_8$  case it again takes  $O(\xi q \log q + \mu q \log^2 q)$  time since a constructive isomorphism is used in the Appendix. (N.B.—The faster  $O(\mu q \log q)$  time is significant, but it does not influence the overall time for the algorithm in Theorem 1.1.)

**Reliability:**  $\geq 1 - 1/2^{10}$  in Method 2, in view of Lemma 2.28(ii) and the 30 repetitions of Theorem 1.3(ii). The same probability can be obtained in the  $E_8$  case of Method 1. □

At this point we could also arrange to have  $\Psi_S|_{\hat{S} \cap \hat{L}} = \Psi_L|_{\hat{S} \cap \hat{L}}$ , but we will not need this.

**The subgroups  $T$ ,  $N$  and  $W$ .** By Lemmas 2.22 and 2.32,  $T := \langle T_S, T_L \rangle$  is a maximal torus and  $W := N/T$  is the Weyl group of  $G$ , where  $N := \langle N_S, N_L \rangle$ .

**2.11. The root groups  $X_\alpha$ .** Associated with  $W$  there is a root system  $\Phi$  having a subsystem  $\Phi_L$  corresponding to  $L$ . In Section 2.7 we already used the roots  $\nu, \nu'$  appearing in (2.13), (2.14) since  $\hat{S}$  was defined using (2.19). There is a base  $\Delta_L$  for  $\Phi_L$  such that  $\Delta := \Delta_L \cup \{\nu'\}$  is a base for  $\Phi$ .

We next find the  $|\Phi|$  root groups  $X_\alpha, \alpha \in \Phi$ . We already have  $X_\nu = Z$  and  $X_{-\nu} = Z^-$ . Use the isomorphism  $\Psi_L$  and Theorem 1.3(iv) to find the  $T_L$ -invariant root groups  $X_\alpha, \alpha \in \Phi_L$ . Conjugate these using  $N$  in order to obtain all  $|\Phi| \leq 240$  root groups  $X_\alpha, \alpha \in \Phi$ .

**Time:**  $O(\mu \log q)$  using  $\Psi_L$  (Theorem 1.3(iv)). For, we only need one nontrivial root element in one root group  $X_\alpha$  of each length, an element  $h_\alpha(t)$  generating the corresponding 1-dimensional torus, and a “reflection”  $n_\beta(1)$  for each  $\beta \in \Delta_L$ , after which we can conjugate using (2.9) and (2.10).

Note also that we only need coset representatives in  $N$  of the stabilizer in  $N$  of the long root  $\nu$ ; this stabilizer is  $N_L T$ . A similar remark holds for short roots, if there are any. There are at most 240 such coset representatives for each type of root, and these can be quickly found in  $O(1)$  time using standard permutation

group algorithms for  $W$  [Ser, Ch. 4]. Alternatively, it is straightforward to write coset representatives as explicit products of fundamental reflections in the Weyl group.

**2.12. The epimorphism  $\Psi: \hat{G} \rightarrow G_0$ .** Let  $G_0 := \langle X_\alpha \mid \alpha \in \Phi \rangle$ . We next show that  $G_0$  is an epimorphic image of  $\hat{G}$ . In Corollary 2.42 we will test whether each member of the original generating set  $\mathcal{S}$  of  $G$  lies in  $G_0$ , thereby verifying that  $G_0$  is  $G$ .

The isomorphism  $\Psi_L$  lets us “coordinatize” each root group  $X_\alpha, \alpha \in \Phi_L$ : labeling the elements of  $X_\alpha$  as  $X_\alpha(t), t \in \mathbb{F}$  or  $\mathbb{F}'$ , in a manner preserved by the conjugations (2.10) for  $\alpha \in \Phi_L$  and satisfying the relations (2.2)–(2.5) or (2.6). This was already noted in Remark 2.31. We need to coordinatize each root group  $X_\alpha, \alpha \in \Phi$ , in the same manner:

**Proposition 2.33.** *There is a deterministic  $O(\mu \log^2 q)$ -time algorithm that labels any given element of any root group  $X_\alpha, \alpha \in \Phi$ , as  $X_\alpha(t)$  for some  $t$  in  $\mathbb{F}$  or  $\mathbb{F}'$ , in such a way that the map  $\hat{X}_\alpha(f_k) \mapsto X_\alpha(f_k)$  (for all appropriate  $\alpha$  and  $k$ ) extends to an epimorphism  $\Psi: \hat{G} \rightarrow G_0$ . Moreover,  $\Psi|_{\hat{L}} = \Psi_L$ .*

*Proof.* We have  $\hat{G}$  and its presentation, and we have already coordinatized all  $X_\alpha(f_k) = \hat{X}_\alpha(f_k)\Psi_L, \alpha \in \Phi_L$ .

We also already have the long root  $\nu'$  in (2.14). By (2.9),  $N_{\hat{R}}(\hat{X}_{\nu'})$  centralizes  $\hat{L}$  and is transitive on the nontrivial elements of  $\hat{X}_{\nu'}$ . Hence, we can choose any nontrivial element of  $X_{\nu'}$  and label it  $X_{\nu'}(1)$ . We now show that *all remaining labels are uniquely determined*.

Let  $\delta \in \Delta_L$  be the long root not perpendicular to  $\nu'$ . Using (2.9) for  $h_\delta(f_k)$  we can correctly label  $X_{\nu'}(f_k)$  and hence any given element of  $X_{\nu'}$ .

By (2.5), we have relations  $[\hat{X}_\alpha(f_k), \hat{X}_\beta(f_l)] = \hat{X}_{\alpha+\beta}(\epsilon_{\alpha,\beta} f_k f_l)$  in  $\hat{G}$  whenever  $\alpha \in \Phi_L, \beta$  and  $\alpha + \beta$  are long. Each subgroup  $X_\alpha$  of  $L$  has already been coordinatized. Starting with all root groups of  $L$  together with  $X_\beta := X_{\nu'}$ , by repeatedly using these relations with hats removed we coordinatize all positive long root groups. Alternatively, we could achieve this by using (2.10) for  $n_\beta(1), \beta \in \Phi_L$ .

We next coordinatize  $X_{-\nu'}$  using  $\alpha = \nu - \nu' \in \Phi_L, \beta = -\nu'$  together with the desired relation  $[X_{\nu'+\alpha}(1), X_{-\nu'}(u)] = X_\alpha(\epsilon_{\nu'+\alpha, -\nu'} u)$  in (2.5) or (2.6) (here  $\epsilon_{\nu'+\alpha, -\nu'} := C_{1,1,\nu'+\alpha, -\nu'}$  in (2.5)). First, find an  $\mathbb{F}_p$ -basis for the elementary abelian group  $X_{-\nu'}$  (recall that this root group was obtained as a conjugate of a root group of  $L$ ). For each element  $x$  in this basis, find its coordinate  $u$  via  $[X_{\nu'+\alpha}(1), x] = X_\alpha(\epsilon_{\nu'+\alpha, -\nu'} u)$  using linear algebra in  $X_\alpha$ . This produces the coordinates of a basis of  $X_{-\nu'}$  and hence of any given element of  $X_{-\nu'}$ .

Now coordinatize all negative long root groups as above.

This leaves us with the groups of type  $F_4$  or  ${}^2E_6$ , where there are also short roots to consider. Here we use the last relation in (2.6) as above in order to coordinatize  $X_{\alpha+\beta}$  whenever  $\alpha, \alpha + 2\beta$  are long and  $\beta \in \Phi_L, \alpha + \beta$  are short. Namely  $[X_\alpha(1), X_\beta(f_l)] = X_{\alpha+\beta}(\epsilon_{\alpha\beta} f_l) X_{\alpha+2\beta}(\epsilon'_{\alpha\beta} f_l f_l^q)$ , where we already know  $X_{\alpha+2\beta}(\epsilon'_{\alpha\beta} f_l f_l^q)$ .

Finally, we verify all of the relations (2.2)–(2.5) or (2.6). This proves our assertions concerning both  $\Psi$  and  $\Psi|_{\hat{L}}$ .

This algorithm is deterministic. The stated time includes verifying the relations (cf. [KS1, 7.2.2]). □

Note that this same commutator method could have been used to *produce* all of the root groups  $X_\alpha$ , not just to label them. This may, in fact, be more efficient in practice. Also note that  $\Psi$  extends  $\Psi_L$  but not necessarily  $\Psi_S$ .

*Remark 2.34.* We have  $G_0 = \langle \mathcal{S}^* \rangle$ , where  $\mathcal{S}^*$  consists of all of the  $X_\alpha(f_k)$ ,  $\alpha \in \Phi$ . Let  $\hat{\mathcal{S}}$  consist of the elements  $\hat{X}_\alpha(f_k)$  of  $\hat{G}$ , so that  $\hat{\mathcal{S}}\Psi = \mathcal{S}^*$  is the defining property of  $\Psi$ .

**Corollary 2.35.** *A random element of  $G_0$  can be constructed as a straight-line program of length  $O(\log q)$  in  $\hat{\mathcal{S}}$  in time  $O(\mu \log q)$ .*

*Proof.* Let  $\hat{U} := \prod_{\alpha > 0} \hat{X}_\alpha$  and  $\hat{U}_w := \prod_{\alpha > 0 > w(\alpha)} \hat{X}_\alpha$  for each  $w \in W = N_{\hat{G}}/T_{\hat{G}}$  (for a suitable order of the factors). Also, let  $h_\delta$  be a generator of  $\hat{h}_\delta(\mathbb{F}^*)$  (or of  $\hat{h}_\delta(\mathbb{F}'^*)$  if  $\delta$  is short), for each  $\delta \in \Delta$ . Then  $T_{\hat{G}}$  is the direct product of the groups  $\langle h_\delta \rangle$ ,  $\delta \in \Delta$ . For  $w \in W$  choose  $n_w \in N_{\hat{G}}$  such that  $w = n_w T_{\hat{G}}$ .

By [Ca1, Corollary 8.4.4] or [GLS, Theorem 2.3.5], every element of  $\hat{G}$  has the unique Bruhat normal form  $unv$  with  $u \in \hat{U}$ ,  $n \in N_{\hat{G}}$ ,  $w := nT_{\hat{G}} \in W$  and  $v \in \hat{U}_w$ .

Hence, a random element of  $\hat{G}$  is obtained by choosing  $w$  and hence  $n_w$ , then  $t \in T_{\hat{G}}$  and hence  $n := n_w t$ , and finally letting  $u$  and  $v$  be products of randomly chosen elements of the relevant root groups. By (2.2), each of the  $O(1)$  root group elements appearing in the definition of  $\hat{U}$  or  $\hat{U}_w$  is a product of powers of elements of  $\hat{\mathcal{S}}$  with exponents between 0 and  $p - 1$ , and hence can be obtained using a straight-line program of length  $O(\log q)$  from  $\hat{\mathcal{S}}$ . Similarly,  $t = \prod_{\delta \in \Delta} h_\delta^{a(\delta)}$  with  $0 \leq a(\delta) < |h_\delta|$ , and (2.7) shows that  $t$  can also be obtained using a straight-line program of length  $O(\log q)$  from  $\hat{\mathcal{S}}$ . Thus, the required random root group elements and  $t$  are obtained by randomly choosing  $w$  and all of the preceding exponents.

Finally, apply  $\Psi$  in order to obtain a random element of  $\hat{G}\Psi = G_0$ . □

Note that this corollary involves the more classical notion of “random” element rather than the more subtle version in [Bab] (cf. Section 1.1). In particular, the parameter  $\xi$  is not involved.

**2.13. Effective transitivity of  $Q$ .** The set  $Z^G$  of long root groups is far too large to be managed effectively using standard permutation group methods (cf. [Ser]). Nevertheless, as in [KS1, Br2, BrK1, BrK2, LMO], we need to circumvent this difficulty when using the action of  $Q := \langle X_\alpha \mid \alpha \in \Phi^+ \setminus \Phi_L \rangle$  on this set. As in the above references, the following *effective transitivity* of  $Q$  will be crucial later (in Section 2.15):

**Lemma 2.36.** *There is an  $O(\xi q \log q + \mu q \log^2 q)$ -time Las Vegas algorithm which, with probability  $> 1 - 1/2^{10}$ , when given long root groups  $A$  and  $B$  opposite to  $Z$ , finds the unique element  $u \in Q$  such that  $A^u = B$ .*

*Proof.* Each long root group opposite  $Z$  has the form  $B^v$  for a unique  $v \in Q$ . Repeat up to 60 times: choose  $v \in Q$ , and test whether  $S(v) := \langle Z, A, B^v \rangle \cong \text{SL}(3, q)$  using Theorem 1.3(ii); if so obtain a constructive isomorphism  $\Psi_{S(v)}: \text{SL}(3, q) \rightarrow Y$ , and finally use  $\Psi_{S(v)}$  and Theorem 1.3(iii),(iv) in order to obtain an element of  $O_p(C_{S(v)}(Z))$  conjugating  $A$  to  $B^v$ . Since  $O_p(C_{S(v)}(Z))$  is transitive on  $A^Q \cap S(v)$ , such an element exists, and it is in  $Q$  by Lemma 2.21(iii).

**Reliability:**  $\geq 1 - 1/2^{10}$ , since  $\langle Z, A, B^v \rangle \cong \text{SL}(3, q)$  with probability  $\geq 1/3$  by Lemma 2.27(i), and Theorem 1.3(ii) succeeds with probability  $> 1/2$ , so that all 60 repetitions fail with probability  $\leq (1 - 1/6)^{60} < 1/2^{10}$ .

**Time:**  $O(\xi q \log q + \mu q \log^2 q)$ , dominated by finding  $\Psi_{S(v)}$ . □

**2.14. Linear algebra in  $Q/Z$ .** We next address the problem of writing an element  $g \in Q$  as a word in the generators  $X_\alpha(t)$ .

Fix an ordering of the roots for  $Q$ , with  $Z = X_\nu$  first. (For example, modify the ordering in [Ca1, p.78] so that  $\nu$  is first.) Then each  $g \in Q$  can be written as a product  $g = \prod_{\alpha \in \Phi^+ \setminus \Phi_L} X_\alpha(t_\alpha)$  in the chosen order, with each  $t_\alpha \in \mathbb{F}$  or  $\mathbb{F}'$  written as  $\mathbb{F}_p$ -linear combinations of the given bases of  $\mathbb{F}$  or  $\mathbb{F}'$ . We will call this product the *standard form* of  $g$ .

**Proposition 2.37.** *The standard form of any given  $g \in Q$  can be computed deterministically in  $O(\mu \log q)$  time.*

*Proof.* We first deal with the case in which  $G$  is not  $F_4(q)$  with  $q$  even. (The omitted case is handled in the following lemma.) We must find the standard form  $\prod_{\alpha \in \Phi^+ \setminus \Phi_L} X_\alpha(t_\alpha)$  of  $g$ . Let  $X_\gamma(t_\gamma)$  be the rightmost nontrivial factor in the product. By Lemma 2.18(ii) there is a unique root group  $X_\beta$  in  $Q$  that does not commute with  $X_\gamma$ . Then we can find  $t_\gamma$  using linear algebra in  $X_\nu$ :

$$[g, X_\beta(1)] = [X_\gamma(t_\gamma), X_\beta(1)] = X_\nu(C_{\gamma, \beta, 1, 1} t_\gamma)$$

by (2.5) and (2.6), since  $X_\beta$  commutes with  $g_1 := gX_\gamma(-t_\gamma)$ .

Now compute  $g_1$  and repeat  $O(1)$  times. The procedure ends with  $g \in X_\nu = Z$  after we have processed  $O(1)$  roots in  $\Phi^+ \setminus \Phi_L$ .

This procedure is deterministic. The time takes into account the need to write a given field element  $C_{\gamma, \beta, 1, 1} t_\gamma$  in terms of the basis vectors  $f_k$ .

**The case  $F_4(q)$  with  $q$  even.** Here we will modify the above procedure using explicit knowledge of the positive roots of the root system of type  $F_4$  together with the explicit presentation (2.2)–(2.5) or (2.6).

**Conventions:** The roots in our base  $\Delta$  are ordered  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ , so that the high root is  $\nu = 2342$ , where we write  $\alpha = abcd$  if  $\alpha = a\alpha_1 + b\alpha_2 + c\alpha_3 + d\alpha_4$ .

**The positive roots:**

1000, 0100, 0010, 0001, 1100, 0110, 0011, 1110, 0120, 0111, 1120, 1111, 0121, 1220, 1121, 0122, 1221, 1122, 1231, 1222, 1232, 1242, 1342, 2342.

**The roots for  $Q$ :** those of the form  $1bcd$  or  $2342$ .

**The short roots for  $L$ :**  $\pm 0001, \pm 0011, \pm 0010, \pm 0110, \pm 0111, \pm 0121$ .

**The long roots for  $L$ :**  $\pm 0122, \pm 0120, \pm 0100$ .

**The short roots for  $Q$ :** 1232, 1231, 1221, 1121, 1111, 1110.

**The long roots  $\neq 2342$  for  $Q$ :** 1341, 1242, 1222, 1122, 1220, 1120, 1100, 1000.

The above lists of  $n = 6$  or  $8$  roots in  $Q$  are listed so that the  $i$ th and  $(n - i + 1)$ st roots sum to the highest root. For example,  $1231 + 1111 = 2342$  and  $1222 + 1120 = 2342$ . □

**Lemma 2.38.** Proposition 2.37 holds if  $G$  is  $F_4(q)$  with  $q$  even.

*Proof.* We must find the standard form  $\prod_{\alpha \in \Phi^+ \setminus \Phi_L} X_\alpha(t_\alpha)$  of  $g$ . As all short root groups of  $Q$  lie in the center of  $Q$ , we can move all long root factors of  $g$  to the end (the right hand side) of the product, and then compute the long root “coordinates” as above for the root groups  $\neq X_\nu$ .

It remains to find the standard form of an element  $g \in Z(Q) = \langle X_{2342}, X_{1232}, X_{1231}, X_{1221}, X_{1121}, X_{1111}, X_{1110} \rangle$ . We repeatedly use (2.5) for these short root groups.

Compute  $s_0 := [[g, X_\alpha(1)], X_{-\alpha_4}(1)]$ , where  $\alpha = 0121$ . By (2.5),  $s_0 = X_{1232}(t_{1110})$ , from which we find  $t_{1110}$ .

Define  $s_1 := gX_{1110}(t_{1110})$  and compute  $[s_1, X_{0111}(t)] = X_{1232}(t_{1121})$  in order to find  $t_{1121}$ .

Define  $s_2 := s_1X_{1121}(t_{1121})$  and compute  $[s_2, X_{0121}(t)] = X_{1232}(t_{1111})$  in order to find  $t_{1111}$ .

Define  $s_3 := s_2X_{1111}(t_{1111})$  and compute  $[s_3, X_{0011}(t)] = X_{1232}(t_{1221})$  in order to find  $t_{1221}$ .

Define  $s_4 := s_3X_{1221}(t_{1221})$  and compute  $[s_4, X_{0001}(t)] = X_{1232}(t_{1231})$  in order to find  $t_{1231}$ .

Define  $s_5 := s_4X_{1231}(t_{1231})$  and compute  $[s_5, X_{-0001}(t)] = X_{1231}(t_{1232})$  in order to find  $t_{1232}$ .

Finally, compute  $s_5X_{1232}(t_{1232}) = X_{2342}(t_{2342}) \in Z = X_{2342}$  in order to find  $t_{2342}$ .

Once again this procedure is deterministic and the time is clear. □

**2.15. Straight-line programs; testing that  $G = G_0$ .** We can now prove parts (ii) and (iii) of Theorem 1.1. First of all we may need to slightly increase the set  $\mathcal{S}^*$  in Remark 2.34 in order to use recursion. In Section 2.9 we used either Theorem 1.3(ii), or a recursive call when  $G$  is  $E_8(q)$ , in order to find a new generating set  $\mathcal{S}_L^*$  for  $L$ . If necessary, increase  $\mathcal{S}^*$  by adjoining this set, in which case adjoin  $\hat{\mathcal{S}}_L = \mathcal{S}_L^* \Psi_L^{-1}$  to  $\hat{\mathcal{S}}$  (cf. Remark 2.34). Thus,  $\hat{\mathcal{S}}$  and  $\mathcal{S}^*$  still have size  $O(\log q)$  and  $\hat{\mathcal{S}}\Psi = \mathcal{S}^*$ . This takes  $O(\mu q \log q)$  time by Theorem 1.3(iii).

**Proposition 2.39.** (i) *There is a deterministic  $O(\mu \log q)$ -time algorithm which, when given  $\hat{g} \in \hat{G}$ , finds  $\hat{g}\Psi$  and a straight-line program of length  $O(\log q)$  from  $\hat{\mathcal{S}}$  to  $\hat{g}$ .*

(ii) *There is a deterministic  $O(\mu \log q)$ -time algorithm that finds a generator of  $Z(\hat{G})$ .*

(iii) *There is an  $O(\xi q \log q + \mu q \log^2 q)$ -time Las Vegas algorithm which, with probability  $\geq 1 - 1/2^7$ , when given  $g \in G$  finds a preimage  $g\Psi^{-1}$  and a straight-line program of length  $O(\log q)$  from  $\mathcal{S}^*$  to  $g$ .*

*Proof.* (i) We have assumed the availability of the Lie algebra for  $\hat{G}$  and the action of  $\hat{G}$  on that algebra. Use [CMT, Theorem 8.1] and [CHM] to write  $\hat{g}$  in the Bruhat form  $unu'$ , with  $n \in N_{\hat{G}}$  and  $u, u'$  in the Sylow  $p$ -subgroup  $\langle \hat{X}_\gamma(f_k) \mid \text{all appropriate } k \text{ and } \gamma \in \Phi^+ \rangle$ . Then use (2.2)–(2.5) or (2.6), together with (2.9)–(2.10), in order to write  $u, u'$  and  $n$  in terms of straight-line programs from  $\hat{\mathcal{S}}$  [Ri, CMT, CHM] (compare Corollary 2.35). Apply  $\Psi$  in order to obtain a straight-line program from  $\hat{\mathcal{S}}\Psi$  to  $\hat{g}\Psi$ .



(ii) There is an algorithm in [Ca1, pp. 198–199] for finding  $Z(\hat{G})$ . However, for each of the present small number of exceptional groups (2.1) one can instead readily write the center of  $\hat{G}$  in terms of the elements  $\hat{h}_{\alpha_i}(t)$ , and hence in terms of the elements  $\hat{X}_{\pm\alpha_i}(f_k)$ , in  $O(\log q)$  time (cf. (2.7)). Now the center of  $G$  is obtained using (i).

(iii) Use Corollary 2.35 to choose up to 30 elements  $y \in G_0$  in order to find one such that  $[[z^{gy}, z], z] \neq 1$ , so that  $Z$  and  $Z^{gy}$  are opposite by (2.12).

Find  $u \in Q$  such that  $Z^{gyu} = Z^-$  using Lemma 2.36; find a straight-line program of length  $O(\log q)$  from  $\mathcal{S}^*$  to  $u$  using Proposition 2.37. Now  $gyun_\nu$  normalizes  $Z$ , where  $n_\nu := n_\nu(1)$  is defined using (2.7) without the hats. It follows that the desired result holds for  $g$  if it holds for  $gyun_\nu$ .

Thus, we will replace  $g$  by  $gyun_\nu$  so that  $g$  normalizes  $Z$ . Now  $Z^{-g}$  is opposite  $Z$ . Again use Lemma 2.36 and Proposition 2.37 in order to find  $u' \in Q$  such that  $Z^{-gu'} = Z^-$ , as well as a straight-line program of length  $O(\log q)$  from  $\mathcal{S}^*$  to  $u'$ . Thus, we may now assume that  $g$  normalizes both  $Z$  and  $Z^-$ .

Find  $h = h_\nu(t)$  acting on  $Z$  and  $Z^-$  in the same manner as  $g$  by using (2.14) and (2.9). Find a straight-line program of length  $O(\log q)$  from  $\mathcal{S}^*$  to  $h^{-1}$  using (2.7).

Now  $gh^{-1} \in C_G(\langle Z, Z^- \rangle) = L$  (cf. (2.16)). Find a straight-line program of length  $O(\log q)$  from  $\mathcal{S}_L^*$  to  $gh^{-1}$  using Theorem 1.3(iii). This produces the desired straight-line program to  $g$ .

**Reliability:**  $\geq 1 - 1/2^8$ : we obtain  $y$  with probability  $> 1 - 1/2^{10}$  by Lemma 2.26, and both calls to Lemma 2.36 succeed with probability  $> 1 - 2/2^{10}$ . (N. B.—Recall that we are assuming that  $G_0 = G$ , in which case Corollary 2.35 provides us with a random element of  $G$  and hence a random conjugate  $Z^{gy}$  of  $Z$ . We will test this assumption in Corollary 2.42.)

**Time:**  $O(\xi q \log q + \mu q \log^2 q)$  in (iii), dominated by the time to find the elements  $u$  and  $u'$  using Lemma 2.36. (N.B.—It also takes  $O(\mu q)$  time to find  $h$ .)  $\square$

*Remark 2.40.* We have assumed in (i) that our element of  $\hat{G}$  was given either in terms of the Bruhat decomposition or as an automorphism of the Lie algebra for  $\hat{G}$ . In the latter situation, the input to the algorithm in [CMT, Theorem 8.1] or [CHM] is a linear transformation and the algorithm carries out a form of row reduction to get the Bruhat form. This is essential for our use in the Appendix and nicely parallels the classical group situation [KS1]. In fact, [CMT, CHM] deal with the same question for a variety of irreducible representations of  $\hat{G}$ .

Alternatively,  $\hat{g}$  could just be given as a *word* in  $\hat{\mathcal{S}}$ . This possibility has already been considered: in [Ri, pp. 44–45] and [CMT] there are deterministic algorithms which, when given  $g$  as a word in  $\hat{\mathcal{S}}$ , uses the relations (2.2)–(2.5) or (2.6), together with (2.9)–(2.10), in order to rewrite  $g$  as an element  $unu'$  as above.

In (iii) an element of the black box group  $G$  is given as a string; it is not necessarily given in terms of any available generating set. This is essential for uses of Theorem 1.1 such as Corollary 1.2.

*Remark 2.41.* Alternative approach to (i) *avoiding* [CMT, CHM, Ri]: Apply the algorithm in Proposition 2.39(iii) to the given element  $\hat{g} \in \hat{G}$  (this uses Lemma 2.36 and Proposition 2.37 for  $\hat{G}$ ).

Here  $\hat{g}$  might once again merely be known as an automorphism of the associated Lie algebra. This routine has the disadvantage of requiring more time and being probabilistic; its advantage is that it uses the present paper's relatively standard black-box methodology employed in (iii).

**Corollary 2.42.** *There is an  $O(|\mathcal{S}| \log |\mathcal{S}| (\xi q \log q + \mu q \log^2 q))$ -time Las Vegas algorithm which, with probability  $\geq 1 - 1/2^6$ , checks that  $G = G_0$ .*

*Proof.* Recall that  $G$  is given as  $\langle \mathcal{S} \rangle$ . In order to prove that  $\Psi$  is an epimorphism we verify that every generator  $s \in \mathcal{S}$  lies in  $G_0$  by applying Proposition 2.39(iii) to each  $s$  up to  $\lceil \log |\mathcal{S}| \rceil$  times.

**Reliability:**  $\geq 1 - 1/2^6$ : the applications of Proposition 2.39(iii) for a single  $s \in \mathcal{S}$  all fail with probability  $< 1/2^{7 \log |\mathcal{S}|} \leq 1/(2^6 |\mathcal{S}|)$ , so that at least one of our tests fails for some  $s \in \mathcal{S}$  with probability  $< |\mathcal{S}| \cdot 1/(2^6 |\mathcal{S}|)$ .

**Time:**  $O(|\mathcal{S}| \log |\mathcal{S}| (\xi q \log q + \mu q \log^2 q))$  using Proposition 2.39(iii) to obtain straight-line programs from  $\mathcal{S}^*$  to each  $s \in \mathcal{S}$ .  $\square$

The timing in the preceding result differs from [KS1, p. 145] since the membership test used there is deterministic, unlike our Proposition 2.39(iii).

**2.16. Proof of Theorem 1.1 for rank  $> 2$ .** In Section 2.12 we produced a homomorphism  $\Psi: \hat{G} \rightarrow G$  with image  $G_0$ . We consider the various parts of Theorem 1.1.

(i) We already used [BKPS].

(ii) See Sections 2.12 and 2.15.

(iii), (iv), (vii) See Proposition 2.39.

(v) This follows from Theorem 1.3(i) in view of the new generators  $X_\alpha(f_k)$  we introduced in Sections 2.12 and 2.15.

(vi) The second part is Corollary 2.42.

The first part is the content of Sections 2.4–2.12. The probability of success is at least  $1/2$ , and the total time is as stated, due to all of the individual probabilities and times obtained earlier.

(viii) Find  $Z(\hat{G})$  using Proposition 2.39(ii), and then find  $Z(G) = Z(\hat{G})\Psi$  using Proposition 2.39(i).  $\square$

### 3. RANK 2 GROUPS

We now turn to the groups  $G_2(q)$  and  ${}^3D_4(q)$ . For the most part we will be able to mimic and simplify the previous approach. However, there are differences, such as the use of a subgroup  $L$  that does not contain any long root elements.

We assume that  $q > 9$  in order to avoid some exceptional situations. In particular, we will always have  $\hat{G} \cong G$  [GLS, p. 313], where  $\hat{G}$  will be known and “concrete”, whereas  $G$  will be a black box group.

**3.1. Background.** In addition to  $\mathbb{F} = \mathbb{F}_q$  we need to consider  $\mathbb{F}' = \mathbb{F}_{q^\epsilon}$ , where  $\epsilon$  is 1 for  $G_2(q)$  and 3 for  ${}^3D_4(q)$ . We retain our notation from Section 2, except that now  $\mathbb{F}'$  is  $\mathbb{F}_q$  or  $\mathbb{F}_{q^\epsilon}$  and  $\{f_1, \dots, f_{\epsilon\epsilon}\}$  is an  $\mathbb{F}_p$ -basis of  $\mathbb{F}_{q^\epsilon}$ .

**Presentation.** The groups  $G_2(q)$  and  ${}^3D_4(q)$  have a root system  $\Phi$  of type  $G_2$ .

First consider  $\hat{G} = {}^3D_4(q)$ . We start with generators  $x_\alpha(t)$ , where either  $\alpha$  is long and  $t \in \mathbb{F}$ , or  $\alpha$  is short and  $t \in \mathbb{F}' = \mathbb{F}_{q^3}$ . Define  $T: \mathbb{F}' \rightarrow \mathbb{F}'$  by  $T(t) = t + t^q + t^{q^2}$ . Then the Steinberg relations [St] become (2.2)–(2.4), where the field elements are in  $\mathbb{F}$  or  $\mathbb{F}'$  for  $\alpha$  long or short, respectively, together with

$$\begin{aligned}
 (3.1) \quad [\hat{X}_\alpha(f_k), \hat{X}_\beta(f_l)] = & \quad \text{for} \\
 & 1 \qquad \qquad \qquad \alpha + \beta \notin \Phi \\
 & \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta} f_k f_l) \qquad \alpha, \beta, \alpha + \beta \text{ long} \\
 & \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta} T(f_k f_l)) \qquad \alpha, \beta \text{ short}, \alpha + \beta \text{ long} \\
 & \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta} (f_k^q f_l^{q^2} + f_k^{q^2} f_l^q)) \hat{X}_{2\alpha+\beta}(\eta_{\alpha\beta} T(f_k f_k^q f_l^{q^2})) \\
 & \qquad \qquad \qquad \cdot \hat{X}_{\alpha+2\beta}(\delta_{\alpha\beta} T(f_k f_l^q f_l^{q^2})) \\
 & \qquad \qquad \qquad \alpha, \beta, \alpha + \beta \text{ short}, 2\alpha + \beta, \alpha + 2\beta \text{ long} \\
 & \hat{X}_{\alpha+\beta}(\epsilon_{\alpha\beta} f_k f_l) \hat{X}_{2\alpha+\beta}(\epsilon'_{\alpha\beta} f_k^q f_k^{q^2} f_l) \hat{X}_{3\alpha+\beta}(\epsilon''_{\alpha\beta} f_k f_k^q f_k^{q^2} f_l) \\
 & \qquad \qquad \qquad \cdot \hat{X}_{3\alpha+2\beta}(2\epsilon'''_{\alpha\beta} f_k f_k^q f_k^{q^2} f_l^2) \\
 & \qquad \qquad \qquad \alpha, \alpha + \beta, 2\alpha + \beta \text{ short}, \beta, 3\alpha + \beta, 3\alpha + 2\beta \text{ long}
 \end{aligned}$$

for all basis elements  $f_k, f_l$  of  $\mathbb{F}$  or  $\mathbb{F}'$  (as appropriate). Once again the coefficients  $\epsilon_{\alpha\beta}, \eta_{\alpha\beta}, \delta_{\alpha\beta}, \epsilon'_{\alpha\beta}, \epsilon''_{\alpha\beta}, \epsilon'''_{\alpha\beta}$  are  $\pm 1$  and depend only on  $\alpha$  and  $\beta$ . Once again the right hand sides are viewed as products of powers of generators  $\hat{X}_\gamma(f_m)$  for the roots  $\gamma$  appearing on the right side.

We again use (2.7), where  $t \in \mathbb{F}'^*$  when  $\alpha$  is short. Then the analogues of (2.9) and (2.10) hold. For example:

$$\begin{aligned}
 (3.2) \quad \hat{h}_\alpha(t) \hat{X}_\beta(u) \hat{h}_\alpha(t)^{-1} &= \hat{X}_\beta(t^{A_{\alpha,\beta}} u) && \text{except for the next instance} \\
 \hat{h}_\alpha(t) \hat{X}_\beta(u) \hat{h}_\alpha(t)^{-1} &= \hat{X}_\beta((tt^q t^{q^2})^{A_{\alpha,\beta}/3} u) && \alpha \text{ short}, \beta \text{ long.}
 \end{aligned}$$

For  $G_2(q)$  we obtain the required presentation by restricting all of the above field elements to  $\mathbb{F}$ .

We include a sketch of a proof of the second line in (3.2) when  $\hat{G} = {}^3D_4(q)$ . The twisted root system for  ${}^3D_4(q)$  has a base  $\{\alpha, \beta\}$  arising from a base  $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$  of a  $D_4$ -root system, where  $\beta = \alpha_2$  is the central node and  $\alpha$  corresponds to  $\{\alpha_1, \alpha_3, \alpha_4\}$ . We will follow [Ca1, pp. 233-237]. If  $u \in \mathbb{F}$  and  $t \in \mathbb{F}_{q^3}$ , then  $\hat{X}_\beta(u) = \hat{X}_{\alpha_2}(u)$  and  $\hat{h}_\alpha(t) = \hat{h}_{\alpha_1}(t) \hat{h}_{\alpha_3}(t^q) \hat{h}_{\alpha_4}(t^{q^2})$ . Moreover,

$$\begin{aligned}
 \hat{h}_\alpha(t) \hat{X}_\beta(u) \hat{h}_\alpha(t)^{-1} &= \hat{h}_{\alpha_1}(t) \hat{h}_{\alpha_2}(t^q) \hat{h}_{\alpha_3}(t^{q^2}) \hat{X}_{\alpha_2}(u) \hat{h}_{\alpha_1}(t)^{-1} \hat{h}_{\alpha_2}(t^q)^{-1} \hat{h}_{\alpha_3}(t^{q^2})^{-1} \\
 &= \hat{X}_\beta(t^{A_{\alpha_1,\alpha_2}}(t^q)^{A_{\alpha_3,\alpha_2}}(t^{q^2})^{A_{\alpha_4,\alpha_2}} u)
 \end{aligned}$$

with  $A_{\alpha_1,\epsilon\alpha_2} = A_{\alpha_3,\epsilon\alpha_2} = A_{\alpha_4,\epsilon\alpha_2} = \epsilon = A_{\alpha,\epsilon\beta}/3$  for  $\epsilon = \pm 1$ , which implies the second assertion in (3.2).

**The subgroup  $\hat{S}$ .** For both  $G_2(q)$  and  ${}^3D_4(q)$  the subgroup  $\hat{S}$  generated by the long root groups  $\hat{X}_\alpha$  is isomorphic to  $SL(3, q)$ .

**The subgroups  $\hat{Q}$  and  $\hat{L}$ .** If  $\hat{Z}$  is a long root subgroup of  $\hat{G}$  and  $1 \neq z \in \hat{Z}$ , then  $C_{\hat{G}}(z) = C_{\hat{G}}(\hat{Z}) = \hat{Q} \rtimes \hat{L}$  with  $\hat{Q}$  and  $\hat{L}$  as follows:

$\hat{G}$	$G_2(q), q \neq 3^a$	$G_2(q), q = 3^a$	${}^3D_4(q)$
$\hat{L}$	$SL(2, q)$	$SL(2, q)$	$SL(2, q^3)$
$\hat{Q}$	$q^{1+4}$	$q^{1+(2+2)}$	$q^{1+8}$
$\hat{T}$	$\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$	$\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$	$\mathbb{Z}_{q-1} \times \mathbb{Z}_{q^3-1}$
$T_{\hat{L}}$	$\mathbb{Z}_{q-1}$	$\mathbb{Z}_{q-1}$	$\mathbb{Z}_{q^3-1}$

where we have included the structure of maximal tori  $\hat{T}$  of  $\hat{G}$  and  $T_{\hat{L}}$  of  $\hat{L}$ .

- Lemma 3.3.** (i) *With probability  $\geq 1/3q$ , an element  $\tau \in G_2(q)$  has order  $p \cdot \text{ppd}^\#(p; 2e)$ , and then  $\tau^{q+1}$  is a long or short root element.*  
 (ii) *With probability  $\geq 1/9q$ , an element  $\tau \in {}^3D_4(q)$  has order  $p \cdot \text{ppd}^\#(p; 6e)$ , and then  $\tau^{q^3+1}$  is a long root element.*

*Proof.* We first construct elements of the indicated orders. There is a central product  $SL(2, \mathbb{F}') \circ SL(2, q)$  of a short root  $SL(2, \mathbb{F}')$  and a long root  $SL(2, q)$ , and this contains elements of the desired order. As in Lemma 2.24, an element  $\tau$  of the stated order lies in a parabolic, hence in a central product as above, and hence powers to a root element.

The probability estimates are obtained as in Lemma 2.24, but are simpler. □

*Opposite* long root elements and root groups are defined as in Section 2.1.

**Lemma 3.4.** *Let  $z$  be a long root element.*

- (i) (2.12) holds.
- (ii) Lemma 2.26 holds.
- (iii) Lemma 2.28(i) holds.
- (iv) All long subgroups isomorphic to  $SL(3, q)$  are conjugate.
- (v) If  $p \neq 3$ , then three short root elements of  $G_2(q)$  never generate a group isomorphic to  $SL(3, q)$ .

*Proof.* (i) This follows from the analogue of Lemma 2.11.

(ii), (iii) These are proved exactly as in Section 2.3 (cf. Table 1).

(iv) See [Coo] or [K11, K12].

(v) See [K11]. □

Of course, the conclusion in (v) is false for  $p = 3$  due to the graph automorphism of  $G_2(q)$ .

**3.2. Finding a root group  $Z$  and the subgroups  $Z^-, R$  and  $S$ .** As in Section 2.4, we now consider a black box group  $G$  that is a nontrivial homomorphic image of the universal cover  $\hat{G}$  of  $G_2(q)$  or  ${}^3D_4(q)$ . Since  $q > 4$ ,  $\hat{G} \cong G$  [GLS, p. 313]. Find the probable type of  $G$  using [BKPS].

We now imitate parts of Sections 2.5 and 2.7. Choose up to  $90q$  elements  $\tau$  in order to find one of order  $pl = p \cdot \text{ppd}^\#(p; 2ee)$ ; for  $z := \tau^{e+1}$  choose up to 120 pairs  $z', y$  of conjugates of  $z$ ; for each pair, test whether both are opposite  $z$  and whether  $S := \langle z, z', y \rangle$  and  $S_2 := \langle z, z'^{\tau^p}, y \rangle$  are both isomorphic to  $\hat{S} = SL(3, q)$ ; and, if so, find constructive isomorphisms  $\Psi_S: \hat{S} \rightarrow S$  and  $\Psi_{S_2}: \hat{S} \rightarrow S_2$ , together with generating sets  $\mathcal{S}_{\hat{S}}$  and  $\mathcal{S}_S^*$  of  $\hat{S}$  and  $S$ , respectively, such that  $\mathcal{S}_{\hat{S}}\Psi_S = \mathcal{S}_S^*$ .

Find the root groups  $Z$  and  $Z^-$  in  $S$  such that  $z \in Z$  and  $z' \in Z'$ .

Let  $R := \langle Z, Z^- \rangle \cong \mathrm{SL}(2, q)$ .

As in Section 2.7, find  $c \in \mathrm{O}_p(\mathrm{C}_{S_2}(Z))\mathrm{O}_p(\mathrm{C}_S(Z)) \subseteq \mathrm{O}_p(\mathrm{C}_G(Z))$  such that  $\tau^p c$  centralizes  $R$  and has order divisible by  $l$ .

*Correctness:* By Lemma 3.3(ii), the element  $z$  just constructed is a long root element if  $G$  is  ${}^3D_4(q)$ . If  $G$  is  $G_2(q)$  and  $p = 3$ , it makes no difference whether we are using long or short root elements, since these are conjugate in  $\mathrm{Aut}G$ , so we may assume that  $z$  is long. If  $G$  is  $G_2(q)$  and  $p \neq 3$ , then we might have obtained a short root element  $z$ , but then we will not obtain  $S \cong \mathrm{SL}(3, q)$  by Lemma 3.4(v).

**Reliability:**  $\geq 1 - 1/2^9$ . For, a choice  $\tau$  has the correct order and produces a long root element with probability  $\geq 1/9q$  by Lemma 3.3(i), so that we fail to obtain an element  $\tau$  of the desired type with probability  $\leq (1 - 1/9q)^{90q} < 1/2^{10}$ . The tests involving a single choice  $z', y, S, S_2$  all succeed with probability  $\geq (1/12)(1/3)(1/4)^2(1/2)^2 > 1/2^{12}$  (by Lemma 3.4(ii),(iii) and Theorem 1.3(ii)), so that the tests for all 120 pairs  $z', y$  all fail with probability  $< (1 - 1/2^{12})^{120} < 1/2^{10}$ .

**Time:**  $O(\xi q e + \mu q \log^2 q)$ , dominated by finding  $\Psi_S$  and  $\Psi_{S_2}$ .

**3.3. The subgroups  $L, T$  and  $N$ .** We will use additional subgroups analogous to ones in Sections 2.5–2.11.

**The group  $L := \langle \mathrm{C}_S(R), \tau^p c \rangle$**  is a subgroup of  $\mathrm{C}_G(R) = \mathrm{SL}(2, q^\epsilon)$  of order divisible by both  $|\mathrm{C}_S(R)| = q - 1$  and  $|\tau^p c|$ , which is a  $\mathrm{ppd}^\#(p; 2\epsilon e)$ . Then  $L = \mathrm{C}_G(R)$  since  $\mathrm{SL}(2, q^\epsilon)$  has no such proper subgroup for  $q > 9$  [Di, Sec. 260].

As in Lemma 2.21(ii), *the pair  $(S, L)$  is uniquely determined up to conjugacy in  $G$ .*

Use Theorem 1.3(ii) up to 10 times in order to obtain a constructive isomorphism  $\Psi_L : L \rightarrow \mathrm{SL}(2, \mathbb{F}')$ .

**Reliability:**  $\geq 1 - 1/2^{10}$ .

**Time:**  $O(\xi |\mathbb{F}'| \log q + \mu |\mathbb{F}'| \log^2 q)$  to obtain  $\Psi_L$ .

**The subgroups  $T_S, T_L, T$  and  $N$ .** First note that  $\hat{G}$  acts transitively by conjugation on the set of triples  $(\hat{S}_1, \hat{R}_1, T_{\hat{S}_1})$  with  $T_{\hat{S}_1}$  a maximal split torus of  $\hat{S}_1 \in \hat{S}^{\hat{G}}$  normalizing  $\hat{R}_1 \in \hat{R}^{\hat{G}}$ . Hence  $\hat{G}$  is also transitive on the set of 4-tuples  $(\hat{L}_1, \hat{S}_1, T_{\hat{L}_1}, T_{\hat{S}_1})$  with  $T_{\hat{S}_1}$  a maximal split torus of  $\hat{S}_1$  normalizing  $\hat{L}_1 = \mathrm{C}_{\hat{G}}(\hat{R}_1)$  and centralizing a (unique) maximal split torus  $T_{\hat{L}_1}$  of  $\hat{L}_1$  (which must therefore contain the torus  $\mathrm{C}_{\hat{S}_1}(\hat{R}_1) = \hat{S}_1 \cap \hat{L}_1$ ). Then  $T_{\hat{S}_1} T_{\hat{L}_1}$  is a maximal torus of  $\hat{G}$  and is normal in  $\langle \mathrm{N}_{\hat{S}_1}(T_{\hat{S}_1}), \mathrm{N}_{\hat{L}_1}(T_{\hat{L}_1}) \rangle$  (compare Lemma 2.22).

With this in mind, use  $\Psi_S$  (and Theorem 1.3(iii),(iv)) to find a maximal split torus  $T_S$  of  $S$  normalizing  $R, Z$  and  $Z^-$ . Then  $T_S$  normalizes  $\mathrm{C}_G(R) = L$ , and hence normalizes and so centralizes the unique maximal split torus  $T_L \geq S \cap L$  of  $L$  (by the preceding paragraph). Find  $T_L$  using  $\Psi_L$ . (Compare Lemma 2.32 – but here we are only working with a 2-dimensional vector space. Moreover, unlike in the large rank case, the torus  $T_L$  is uniquely determined by  $S \cap L$ .)

Then  $T := T_S T_L$  is a maximal torus of  $G$ .

Find  $\mathrm{N}_S(T_S)$  and  $\mathrm{N}_L(T_L)$  using  $\Psi_S$  and  $\Psi_L$ . The above observations concerning  $\hat{G}$  imply that  $T \triangleleft N := \langle \mathrm{N}_S(T_S), \mathrm{N}_L(T_L) \rangle$  and  $N/T$  is the Weyl group of  $G$ .

From this point on we will no longer explicitly use  $S$ .

**3.4. Root groups.** Let  $\{\alpha_1, \alpha_2\}$  be a base for a root system  $\Phi$  associated with the Weyl group  $N/T$ , with  $\alpha_1$  long. Let  $\nu = 2\alpha_1 + 3\alpha_2$  be the highest root, and label  $Z = X_\nu$  and  $Z^- = X_{-\nu}$ .

Find the two (short!) root groups of  $L$  normalized by  $T$  using  $\Psi_L$ , pick one of them and label it  $X_{\alpha_2}$ , and then label the other one  $X_{-\alpha_2}$ . The  $N$ -conjugates of  $X_{\pm\nu}$  and  $X_{\pm\alpha_2}$  are the 12 root groups of  $G$  normalized by  $T$ ; the action of  $N$  labels each as  $X_\alpha$  with  $\alpha \in \Phi$ .

Coordinatize  $L$  using  $\Psi_L$ , obtaining  $X_{\pm\alpha_2}(f_k)$ ,  $n_{\alpha_2}(1)$  and  $h_{\alpha_2}(f_k)$  for  $f_k \in \mathbb{F}'$ .

**Time:**  $O(\mu q \log^2 q)$ , dominated by  $O(e)$  uses of Theorem 1.3(iii),(iv) for  $\Psi_L$ .

As in Section 2.12, we next show that  $\hat{G}$  maps onto  $G_0 := \langle X_\alpha \mid \alpha \in \Phi \rangle$ :

**Proposition 3.5.** *There is a deterministic  $O(\mu \log^2 q)$ -time algorithm that labels any given element of any root group  $X_\alpha$ ,  $\alpha \in \Phi$ , as  $X_\alpha(t)$  for some  $t \in \mathbb{F}$  or  $\mathbb{F}'$ , in such a way that the map  $\hat{X}_\alpha(f_k) \mapsto X_\alpha(f_k)$  (for all appropriate  $\alpha$  and  $k$ ) extends to an epimorphism  $\Psi: \hat{G} \rightarrow G_0$ .*

*Proof.* By (3.2),  $\hat{T}_L$  acts transitively on the nontrivial elements of  $\hat{X}_{\alpha_1}$ . Thus, we can choose any nontrivial element  $X_{\alpha_1}$  and label it  $X_{\alpha_1}(1)$ , after which the remaining labels  $X_{\alpha_1}(f_k)$  are forced by (3.2). Namely,  $h_{\alpha_2}(t)^{-A_{\alpha_2, \alpha_1}/3}$  conjugates  $X_{\alpha_1}(1)$  to  $X_{\alpha_1}(tt^q t^{q^2})$ . Applying this for distinct  $t = f_k, f_k + 1, af_k + 1$  in  $\mathbb{F}$  gives us  $X_{\alpha_1}(u)$  for  $u = f_k^3, (f_k + 1)^3$  and  $(af_k + 1)^3$ . We may assume that  $p \neq 3$  (as otherwise the elements  $f_k^3$  span  $\mathbb{F}$ ). Since  $f_1 = 1$ , it is easy to see that we now have obtained all of the elements  $X_{\alpha_1}(f_k)$ .

By the rank 2 analogues of (2.7) and (2.10), we can now coordinatize  $X_{\alpha_1}^{n_{\alpha_2}(1)} = X_{-\alpha_1 - 3\alpha_2}$ .

By (3.1),  $[[X_{\alpha_2}(1), X_{\alpha_1}(f_k)], X_{\alpha_1}(1)] = X_{2\alpha_1 + 3\alpha_2}(\epsilon_{\alpha_1 + 3\alpha_2, \alpha_1} \epsilon''_{\alpha_2, \alpha_1} f_k)$  whenever  $f_k \in \mathbb{F}$ , so we can coordinatize  $X_{2\alpha_1 + 3\alpha_2}$ .

For each element  $x$  in an  $\mathbb{F}_p$ -basis of  $X_{-\alpha_1}$ , find its coordinate  $u$  via the relation  $[X_{2\alpha_1 + 3\alpha_2}(1), x] = X_{\alpha_1 + 3\alpha_2}(\epsilon_{2\alpha_1 + 3\alpha_2, -\alpha_1} u)$  in (3.1) by using linear algebra in  $X_{\alpha_1 + 3\alpha_2}$ . This produces the coordinates of a basis of  $X_{-\alpha_1}$  and hence of any given element of  $X_{-\alpha_1}$ .

Use (2.7) and (2.10) to coordinatize all  $\langle n_{\alpha_1}(1), n_{\alpha_2}(1) \rangle$ -conjugates of  $X_{\alpha_1}$  and  $X_{\alpha_2}$ , and hence of all root groups  $X_\alpha$ .

Thus, we have obtained a map  $\Psi: \hat{X}_\alpha(f_k) \mapsto X_\alpha(f_k)$  (for all appropriate  $\alpha$  and  $k$ ). Verify (3.1) in order to show that  $\Psi$  extends to an epimorphism  $\hat{G} \rightarrow G_0$ . As in the proof of Proposition 2.33, this algorithm is deterministic and runs in the stated time. □

**3.5. Linear algebra in  $Q/Z$ .** Next we imitate Section 2.14.

**Effective transitivity of the subgroup  $Q$ .** Lemma 2.36 holds for  $Q := \langle X_\alpha \mid \alpha \in \Phi^+ \rangle$ , using the exact same proof, still requiring  $O(\xi q \log q + \mu q \log^2 q)$  time and still succeeding with probability  $> 1 - 1/2^{10}$ .

**Linear algebra in  $Q/Z$ .** If we exclude  $G_2(q)$  with  $p = 3$ , this is the same as in Proposition 2.37. Namely,  $Q$  is still of “extraspecial type” (i.e., it behaves exactly as in Lemma 2.18(ii)), and we can again peel off the root elements by commutations as in the proof of Proposition 2.37.

However, since this “peeling” involves traces of field elements, we will be more careful. List the positive roots  $2\alpha_1 + 3\alpha_2 = \nu, \alpha_1 + 3\alpha_2, \alpha_1 + 2\alpha_2, \alpha_1 + \alpha_2, \alpha_2, \alpha_1$ .

Our given  $g \in Q$  can be written  $g = \prod_{\gamma \in \Phi^+ \setminus \Phi_L} X_\gamma(t_\gamma)$  in this order, and we must find the field elements  $t_\gamma$ .

By (3.1),  $X_{\alpha_1+3\alpha_2}$  commutes with the positive root groups other than  $X_{\alpha_1}$ . Since  $[g, X_{\alpha_1+3\alpha_2}(1)] = X_{2\alpha_1+3\alpha_2}(\epsilon_{\alpha_1, \alpha_1+3\alpha_2} t_{\alpha_1})$ , as in Lemma 2.18(i) we deduce  $t_{\alpha_1}$  using linear algebra in  $\mathbb{F}$ .

Let  $g_1 := gX_{\alpha_1}(t_{\alpha_1})^{-1}$ . By (3.1),

$$\begin{aligned} g'_1 &:= [g_1, X_{\alpha_1+\alpha_2}(1)] = [X_{\alpha_1+2\alpha_2}(t_{\alpha_1+2\alpha_2}), X_{\alpha_1+\alpha_2}(1)][X_{\alpha_2}(t_{\alpha_2}), X_{\alpha_1+\alpha_2}(1)] \\ &= X_{\alpha_1+2\alpha_2}(\epsilon_{\alpha_2, \alpha_1+\alpha_2}(t_{\alpha_2}^q + t_{\alpha_2}^{q^2}))X_{\alpha_1+3\alpha_2}(\eta_{\alpha_2, \alpha_1+\alpha_2} T(t_{\alpha_2} t_{\alpha_2}^q)) \\ &\quad \cdot X_{2\alpha_1+3\alpha_2}(\delta_{\alpha_2, \alpha_1+\alpha_2} T(t_{\alpha_2}))X_{2\alpha_1+3\alpha_2}(\epsilon_{\alpha_1+\alpha_2, \alpha_1+2\alpha_2} T(t_{\alpha_1+2\alpha_2})). \end{aligned}$$

Then  $[g'_1, X_{\alpha_1}(\epsilon_{\alpha_1+3\alpha_2, \alpha_1} 1)] = X_{2\alpha_1+3\alpha_2}(\eta_{\alpha_2, \alpha_1+\alpha_2} T(t_{\alpha_2} t_{\alpha_2}^q))$  gives us  $T(t_{\alpha_2} t_{\alpha_2}^q)$ .

Also,

$$\begin{aligned} [g'_1, X_{-\alpha_1}(\epsilon_{\alpha_1+3\alpha_2, -\alpha_1} 1)] &= X_{\alpha_1+3\alpha_2}(\delta_{\alpha_2, \alpha_1+\alpha_2} T(t_{\alpha_2}) + \epsilon_{\alpha_1+\alpha_2, \alpha_1+2\alpha_2} T(t_{\alpha_1+2\alpha_2})), \\ g'_1[g'_1, X_{\alpha_1}(\epsilon_{\alpha_1+3\alpha_2, \alpha_1} 1)]^{-1}[g'_1, X_{-\alpha_1}(\epsilon_{\alpha_1+3\alpha_2, -\alpha_1} 1)]^{-1} \\ &= X_{\alpha_1+2\alpha_2}(\epsilon_{\alpha_2, \alpha_1+\alpha_2}(t_{\alpha_2}^q + t_{\alpha_2}^{q^2})). \end{aligned}$$

Hence, we deduce  $t_{\alpha_2}^q + t_{\alpha_2}^{q^2}$ . The identity  $(t_{\alpha_2}^q + t_{\alpha_2}^{q^2})(t_{\alpha_2}^q + t_{\alpha_2}^{q^2})^q = (t_{\alpha_2}^q)^2 + T(t_{\alpha_2} t_{\alpha_2}^q)$  along with  $T(t_{\alpha_2} t_{\alpha_2}^q)$  give us  $(t_{\alpha_2}^q)^2$ , and hence also  $t_{\alpha_2}^q$  up to sign. Since we already know  $t_{\alpha_2}^q + t_{\alpha_2}^{q^2}$ , we deduce  $t_{\alpha_2}^q$ , and hence also  $t_{\alpha_2}$ .

The same procedure, with the roles of  $\alpha_2$  and  $\alpha_1 + \alpha_2$  reversed, yields  $t_{\alpha_1+\alpha_2}$ .

Let  $g_2 := g_1 X_{\alpha_2}(t_{\alpha_2})^{-1} X_{\alpha_1+\alpha_2}(t_{\alpha_1+\alpha_2})^{-1}$ . As above,

$$[g_2, X_{\alpha_1}(\epsilon_{\alpha_1+3\alpha_2, \alpha_1} 1)] = X_{2\alpha_1+3\alpha_2}(\epsilon_{\alpha_1+3\alpha_2, \alpha_1} t_{\alpha_1+3\alpha_2})$$

yields  $t_{\alpha_1+3\alpha_2}$ . We obtain  $t_{2\alpha_1+3\alpha_2}$  and  $t_{\alpha_1+2\alpha_2}$  similarly.

As in Proposition 2.37, this linear algebra routine is deterministic and takes  $O(\mu \log q)$  time.

**3.6. Proof of Theorem 1.1 for rank 2.** We can now complete the proof of Theorem 1.1.

**Straight-line programs.** The analogue of Proposition 2.39 is proved in the same manner as in that proposition. The timing for the analogue of Proposition 2.39(iii) is  $O(\xi |\mathbb{F}'| \log q + \mu |\mathbb{F}'| \log q)$ , dominated by finding the elements  $u$  and  $u'$  occurring in the proof of Proposition 2.39 and finding straight-line programs in  $L$ .

**Completion of the proof.** This is exactly as in Section 2.16, in view of Proposition 3.5 and the analogue of Proposition 2.39. As usual, (viii) is unnecessary since  $Z(\hat{G}) = 1$ . □

4. CONCLUDING REMARKS

**1. Small  $q$ .** If  $q$  is bounded then so is  $|G|$ , and the questions dealt with in this paper can be handled in constant time by brute force. Of course, our algorithm can still be used in that case when  $q > 9$ .

When  $q \leq 9$ , in place of Lemmas 2.24 or 3.3 we can simply find exact orders of elements (replacing the stated  $l$  by  $l := |\hat{T}^*|$  using (2.15)). We still need the fact that  $q > 3$  in order to have elements behaving as in the conclusions of Lemmas 2.24(i) or 3.3(i). We also used the fact that  $q > 4$  in order to avoid exceptional universal covers.

When  $q = 9$ , two opposite long root elements never generate an  $\mathrm{SL}(2, 9)$ , but instead generate  $\mathrm{SL}(2, 5)$ . However, as in Lemma 2.28(i), inclusion of a third long root element generates  $\mathrm{SL}(3, 9)$  with high probability, after which the rest of our algorithm goes through.

For  $q > 4$ , in rank  $> 2$  the only other needed change is (possibly) to select more elements in order to handle the fact that the probabilities in situations such as Lemmas 2.24 and 2.26–2.28 are no longer as high as in those lemmas.

However, for rank 2 a different approach is needed when  $q$  is 5 or 7: in Section 3.3, elements of  $C_G(R)$  of order  $q - 1$  and  $q + 1$  need not generate  $C_G(R)$ . One way is to use the fact that elements of the stated orders generate  $C_G(R)$  with probability  $> 1/2$ , while another proceeds as in Remark 6 below.

**2. Speculations on implementation.** We expect that versions of the algorithms will be implemented. For rank  $> 2$  we suspect that there is no need to find  $J$ . Instead,  $\langle C_S(L), \tau \rangle$  or  $\langle C_S(L), \tau, \tau_0 \rangle$  appears to be the desired group  $L$  when  $q > 2$  (in the notation of Section 2.9). For example, if  $G$  does not have type  $E_8$ , then  $L$  is essentially a classical group and  $\langle C_S(L), \tau \rangle$  or  $\langle C_S(L), \tau, \tau_0 \rangle$  acts irreducibly and primitively on its natural module. Now the ppd-orders and [GPPS] can be used to obtain a small list of possibilities to check, and presumably to rule out most of them by careful examination of the elements  $\tau$  and  $\tau_0$ .

**3. The omitted groups  ${}^2F_4(q)$ .** We expect that the groups  ${}^2F_4(q)$  will eventually be handled in a manner resembling Section 3. However, those groups involve more intricate commutator relations than other groups of Lie type.

The natural representation of  ${}^2F_4(q)$  is dealt with in [Baa4], assuming the correctness of a complicated conjecture concerning  $\mathbb{F}_q = \mathbb{F}_{2^{2e+1}}$  and of a conjecture concerning the actions of elements of  ${}^2F_4(q)$  on the natural module. Apparently this approach does not work for other absolutely irreducible representations of  ${}^2F_4(q)$  in characteristic 2.

Remarks 4–6 concern variants of Theorem 1.1 that (almost) run in polynomial time. However, these have yet to be carefully checked before there can be a sequel to this paper.

**4. The factor  $q$  and oracles: rank  $> 2$ .** Our algorithm searched for a long root element  $z \in G$ , and then  $\langle z, z^g \rangle$  ( $g \in G$ ) is guaranteed to be a proper subgroup of  $G$ . In fact, with high probability  $\langle z, z^g, z^h \rangle$  ( $g, h \in G$ ) is a long root  $\mathrm{SL}(3, q)$ . Unfortunately, the probability of finding by random search an element for which some power is a long root element is unreasonably small for groups defined over large fields. An alternative strategy is to search for semisimple elements closely related to long root elements.

This was accomplished in a number of the papers cited following Theorem 1.3. More significantly, the factor  $q$  in the timing of analogues of Theorem 1.1 was removed by assuming the availability of an  $\mathrm{SL}(2, q)$ -oracle to constructively recognize  $\mathrm{SL}(2, q)$  as well as a Discrete Log oracle for  $\mathbb{F}_q^*$ , and possibly also for  $\mathbb{Z}_{q+1}$  (cf. Section 1). Then suitable  $p'$ -elements were used to construct subgroups such as  $\mathrm{SL}(3, q)$ ,  $\mathrm{SU}(3, q)$  or  $\mathrm{Sp}(4, q)$ .

Here we comment on the requirements in order for this approach to be used with exceptional groups of rank  $> 2$  when  $q > 4$ . Find and use an element  $\tau$  of order  $\mathrm{ppd}^\#(p; e)l$  or  $\mathrm{ppd}^\#(p; 2e)l$  in the notation of Lemma 2.24; such an element is obtained as the product of elements of  $R = \mathrm{SL}(2, q)$  and  $L = C_G(R)$ . The element



$\tau$  needs to have two further properties: (a)  $\tau^l$  lies in a long  $\mathrm{SL}(2, q)$ , and (b) two conjugates of  $\tau^l$  probably generate a subgroup  $\tau$  containing long root groups (in which case a long root group is obtained via constructive recognition of the subgroup).

Condition (a): As in Section 2.5, we obtain an element  $\tau^l$  of a long  $\mathrm{SL}(2, q)$ , except perhaps in type  $F_4$  where this might belong to a short  $\mathrm{SL}(2, q)$ . In the latter case, we obtain an element of order  $p$  of this  $\mathrm{SL}(2, q)$  and then proceed exactly as in Section 2.5 to distinguish long and short root elements in odd characteristic (or use Remark 6 below).

There is a problem with the first element order  $|\tau| = pl$  in Lemma 2.24 for  $E_7(q)$ . This is the only instance with a factor  $\mathrm{ppd}^\#(p; e)\mathrm{ppd}^\#(p; 2e)$ . One way around this difficulty is to modify Lemma 2.25: use elements  $\tau_1$  of order  $\mathrm{ppd}^\#(p; e)\mathrm{ppd}^\#(p; 9e)$  and  $\tau_2$  of order  $\mathrm{ppd}^\#(p; 2e)\mathrm{ppd}^\#(p; 18e)$  normalizing subgroups of type  $E_6(q)$  and  ${}^2E_6(q)$ , respectively. Once conjugates of the powers  $\tau_1^{(q^9-1)/(q^3-1)}$  and  $\tau_2^{(q^9+1)/(q^3+1)}$  have been arranged (by conjugation) to generate a subgroup  $\mathrm{Spin}_4^+(q)$ , we will have two commuting long subgroups  $R \cong R_1 \cong \mathrm{SL}(2, q)$ ; and once other conjugates of  $\tau_1^{(q^9-1)/(q^3-1)}$  and  $\tau_2^{(q^9+1)/(q^3+1)}$  have been arranged to lie in that long subgroup  $R = \mathrm{SL}(2, q)$ , then  $\langle R_1, \tau_1^{q-1}, \tau_2^{q+1} \rangle$  will be  $L = C_G(R)$ .

Condition (b): If  $\tau^l$  lies in a long  $\mathrm{SL}(2, q)$ , then two of its conjugates lie in the group generated by two such subgroups  $\mathrm{SL}(2, q)$ , and hence for rank  $> 2$  everything reverts to an orthogonal group setting [Ka2, Proposition 3.2], where the required (probable) generation was proved in [BrK1, BrK2].

Starting from a long root element obtained by generating a suitable subgroup in this manner, and by assuming the availability of suitable oracles, the remainder of our algorithm goes through. These oracles are the aforementioned ones for  $\mathrm{SL}(2, q)$  and  $\mathbb{F}_q^*$ , and, in the  ${}^2E_6$  case, one for Discrete Logs in  $\mathbb{Z}_{q+1}$  (cf. [Br2]).

**5. Rank 2, even  $q$ .** The method in the preceding remark also works for type  $G_2$  in characteristic 2, using an element of order  $3\mathrm{ppd}^\#(p; \delta e)$  when  $\hat{G} = G_2(q)$  (where  $\delta$  is 2 if  $3 \mid q-1$  and 1 if  $3 \mid q+1$ ).

Unfortunately, when  $q$  is even  ${}^3D_4(q)$  does not possess any class  $x^G$  of semisimple elements for which  $\langle x, x^g \rangle$  ( $g \in G$ ) is a proper subgroup with high probability. Therefore, our approach in Section 3 appears to be the only option for these groups.

**6. Odd  $q$  and involution centralizers.** There is a different way to handle part of Theorem 1.1 that can produce a long  $\mathrm{SL}(2, q)$  in polynomial time when  $q$  is odd, assuming the availability of suitable oracles as in Remark 4. With high probability, a random element has even order and a power is an involution  $t$  conjugate to the one in  $R$ . (There may be other involutions encountered, but the desired conjugacy class will occur with high probability.) Then  $C_G(t) = R \circ L$  can be found in polynomial time with high probability [Bor, Br, HLORW, PW], after which it is easy to find both  $R$  and  $L$ . As in Remark 4, given suitable oracles the rest of our algorithm appears to go through. Note that, using this approach, we have already obtained the crucial subgroup  $L$ , and hence there is no need for the subgroup  $J$ .

In rank 2, the  ${}^3D_4(q)$  case appears to need oracles to constructively recognize  $\mathrm{SL}(2, q^3)$  and for Discrete Logs in  $\mathbb{F}_{q^3}^*$ .

**7. Rank 1 groups.** An early version of this paper contained Las Vegas algorithms for handling rank 1 exceptional groups – Suzuki groups  $\mathrm{Sz}(q) = {}^2B_2(q)$  and Ree groups  ${}^2G_2(q)$  – with timing that involved a factor  $q^2$  or  $q^3$ , respectively,

as well as use of a length  $O(q^3 \log^2 q)$  presentation for  ${}^2G_2(q)$ . (This result implies that, in Corollary 1.2, there is no need to exclude  ${}^2G_2(q)$  composition factors.)

However, that older approach now seems far less interesting. A lovely black box Las Vegas algorithm for  $Sz(q)$  is in [BrB], with timing involving a factor  $q$ . An alternative approach [Baa1, Baa2] deals with  $Sz(q)$  as a matrix group and avoids any such factor but assumes the correctness of a complicated conjecture concerning  $\mathbb{F}_q = \mathbb{F}_{2^{2e+1}}$ .

The Ree groups  ${}^2G_2(q)$  were studied in [Baa3] as 7-dimensional matrix groups using an involution centralizer and an  $SL(2, q)$  oracle (cf. Remarks 4 and 6), this time assuming a complicated conjecture concerning the field  $\mathbb{F}_q = \mathbb{F}_{3^{2e+1}}$ . There is some hope that a different use of an involution centralizer (together with suitable oracles) can handle the black box setting without a need for any such conjecture or any factor  $q$  in the timing.

APPENDIX: THE GROUP  $\hat{E}_7(q)$  AND ITS LIE ALGEBRA

The proof of Lemma 2.32 required finding  $\hat{g} \in \hat{L} = \hat{E}_7(q)$  such that  $((S \cap L)\Psi_L^{-1})^{\hat{g}} = \hat{S} \cap \hat{L}$ . Since  $\hat{A} := (S \cap L)\Psi_L^{-1}$  and  $\hat{S} \cap \hat{L}$  are conjugate in  $\hat{L}$ , we can use the behavior of the latter group in order to deduce properties of the former one.

The group  $C_{\hat{G}}(\hat{S}) = \hat{E}_6(q)$  acts on the Lie algebra  $\mathcal{L}(\hat{E}_7(q))$  of  $\hat{L}$ , decomposing it as  $133 = 78 \oplus 27 \oplus 27^* \oplus 1$ , where 78 is the Lie algebra  $\mathcal{L}(\hat{E}_6(q))$  of  $C_{\hat{G}}(\hat{S})$ , the 27s are the usual dual pair of irreducible  $C_{\hat{G}}(\hat{S})$ -modules of that dimension, and the 1-space is centralized. The torus  $\hat{S} \cap \hat{L}$  centralizes  $C_{\hat{G}}(\hat{S}) = \hat{E}_6(q)$ ; each of its elements acts as a scalar  $\rho$  on 27 and  $\rho^{-1}$  on its dual  $27^*$ , so that  $\hat{S} \cap \hat{L}$  is nontrivial on both of those subspaces (since  $q > 2$ ); and each of its elements is 1 on  $\mathcal{L}(\hat{E}_6(q))$  since each is both an automorphism of that algebra and a scalar by Schur’s Lemma. Then  $\hat{S} \cap \hat{L}$  centralizes  $78 \oplus 1$ , so that 78 is the derived Lie algebra  $C_{\mathcal{L}(\hat{E}_7(q))}(\hat{S} \cap \hat{L})' \cong \mathcal{L}(\hat{E}_6(q))$ .

With this background we proceed as follows. Find  $C_{\mathcal{L}(\hat{E}_7(q))}(\hat{A})$  and then  $C_{\mathcal{L}(\hat{E}_7(q))}(\hat{A})' \cong \mathcal{L}(\hat{E}_6(q))$ , using elementary linear algebra.

Find a Chevalley basis  $\{e_\alpha, e_{-\alpha}, h_\alpha \mid \alpha \in \Phi_6\}$  of  $C_{\mathcal{L}(\hat{E}_7(q))}(\hat{A})'$  using [CM, CR].

Let  $\Delta_6$  be a base for  $\Phi_6$ .

Find the linear transformations  $E_\alpha(t) = \text{ad}t e_{-\alpha}$  and  $E_{-\alpha}(t) = \text{ad}t e_{-\alpha}$  for  $\alpha \in \Delta_6$  and  $t = f_k$  or  $-f_k^{-1}$  in  $\mathbb{F}$ ; and then also  $h_\alpha(f_k)$  as in (2.7). Then  $\langle h_\alpha(\mathbb{F}^*) \mid \alpha \in \Delta_6 \rangle$  is a maximal split torus of a group (isomorphic to  $\hat{E}_6(q)$ ) of automorphisms of  $C_{\mathcal{L}(\hat{E}_7(q))}(\hat{A})'$ .

We saw above that  $\hat{A}$  is 1 on the 78-space  $C_{\mathcal{L}(\hat{E}_7(q))}(\hat{A})'$ . It follows that  $T_7 := \langle h_\alpha(f_k), \hat{A} \mid \alpha \in \Delta_6, 1 \leq k \leq e \rangle$  is the direct product  $\langle h_\alpha(f_k) \mid \alpha \in \Delta_6, 1 \leq k \leq e \rangle \times \langle \hat{A} \rangle$ , and hence has the correct order  $(q - 1)^6(q - 1)$  to be a maximal torus of  $\hat{L}$ .

We can now obtain a Chevalley basis of  $\mathcal{L}(\hat{E}_7(q))$ : diagonalize the action of  $T_7$  on  $\mathcal{L}(\hat{E}_7(q))$  and normalize the basis as in [Ca1, Sec. 4.2].

We now have two Chevalley bases of  $\mathcal{L}(\hat{E}_7(q))$ : the one we started with (which was implicitly used to write the generators of  $\hat{E}_7(q)$  in the presentation (2.2)–(2.5)) and the one just constructed. Let  $\hat{g}$  be the linear transformation effecting the corresponding base change. It is in  $\hat{E}_7(q)$ , so we can use our  $E_7(q)$  algorithm for

Theorem 1.1(iv) (a recursive call) to write it using a straight-line program in the generators of  $\hat{L}$ , as required.

#### ACKNOWLEDGEMENT

The authors are grateful to the referee, as well as to Peter Brooksbank and Ákos Seress, for many helpful comments and suggestions.

#### REFERENCES

- [Baa1] H. Bäärnhielm, Recognising the Suzuki groups in their natural representations. *J. Algebra* 300 (2006) 171–198. MR2228642 (2007f:20031)
- [Baa2] H. Bäärnhielm, Tensor decomposition of the Suzuki groups (unpublished).
- [Baa3] H. Bäärnhielm, Recognising the Ree groups in their natural representations (unpublished).
- [Baa4] H. Bäärnhielm, Algorithmic problems in twisted groups of Lie type. Ph.D. thesis, Queen Mary, U. of London 2007.
- [Bab] L. Babai, Local expansion of vertex-transitive graphs and random generation in finite groups, pp. 164–174 in: *Proc. ACM Symp. on Theory of Computing* 1991.
- [BB] L. Babai and R. Beals, A polynomial-time theory of black-box groups I, pp. 30–64 in: *Groups St. Andrews 1997 in Bath* (eds. C. M. Campbell et al.), LMS Lecture Note Series 260, Cambridge U. Press, Cambridge 1999. MR1676609 (2000h:20089)
- [BGKLP] L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks and P. P. Pálffy, Short presentations for finite groups. *J. Algebra* 194 (1997) 79–112. MR1461483 (98h:20044)
- [BKPS] L. Babai, W. M. Kantor, P. P. Pálffy 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. MR1931364 (2003i:20022)
- [BLNPS] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger and Á. Seress, A black-box group algorithm for recognizing finite symmetric and alternating groups. I. *Trans. Amer. Math. Soc.* 355 (2003) 2097–2113. MR1953539 (2003k:20002)
- [Bor] A. V. Borovik, Centralisers of involutions in black box groups, pp. 7–20 in: *Computational and statistical group theory* (Las Vegas, NV/Hoboken, NJ, 2001), *Contemp. Math.* 298, Amer. Math. Soc., Providence 2002. MR1929713 (2003i:60010)
- [Br] J. N. Bray, An improved method for generating the centralizer of an involution. *Arch. Math.* 74 (2000) 241–245. MR1742633 (2001c:20063)
- [BrB] J. N. Bray and H. Bäärnhielm, Standard generators for the Suzuki groups (unpublished).
- [Br1] P. A. Brooksbank, Constructive recognition of classical groups in their natural representation. *J. Symbolic Computation* 35 (2003) 195–239. MR1958954 (2004c:20082)
- [Br2] P. A. Brooksbank, Fast constructive recognition of black box unitary groups. *LMS J. Comput. Math.* 6 (2003) 162–197. MR2051584 (2005e:20075)
- [Br3] P. A. Brooksbank, Fast constructive recognition of black box symplectic groups. *J. Algebra* 320 (2008) 885–909. MR2422320 (2009f:20071)
- [BrK1] P. A. Brooksbank and W. M. Kantor, On constructive recognition of a black box  $\mathrm{PSL}(d, q)$ , pp. 95–111 in: *Groups and Computation III* (eds. W. M. Kantor and Á. Seress), Ohio State Univ. Math. Res. Inst. Publ. 8, de Gruyter, Berlin-New York, 2001. MR1829473 (2002m:20078)
- [BrK2] P. A. Brooksbank and W. M. Kantor, Fast constructive recognition of black box orthogonal groups. *J. Algebra* 300 (2006) 256–288. MR2228648 (2007f:20085)
- [Ca1] R. W. Carter, *Simple groups of Lie type*. Wiley, London–New York–Sydney 1972. MR0407163 (53:10946)
- [Ca2] R. W. Carter, *Finite groups of Lie type. Conjugacy classes and complex characters*. Wiley, New York 1985. MR794307 (87d:20060)
- [CHM] A. M. Cohen, S. Haller and S. H. Murray, Computing with root subgroups of twisted reductive groups (preprint).

- [CLG] F. Celler and C. R. Leedham-Green, A constructive recognition algorithm for the special linear group, pp. 11–26 in: *The atlas of finite groups: ten years on* (Birmingham, 1995), LMS Lecture Note Series 249, Cambridge U. Press, Cambridge 1998. MR1647410 (99g:20001)
- [CLMNO] 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. Alg.* 23 (1995) 4931–4948. MR1356111 (96h:20115)
- [CM] A. M. Cohen and S. H. Murray, An algorithm for Lang's Theorem. *J. Algebra* 322 (2009) 675–702. MR2531217 (2010j:20069)
- [CMT] A. M. Cohen, S. H. Murray and D. E. Taylor, Computing in groups of Lie type. *Math. Comp.* 73 (2004) 1477–1498. MR2047097 (2005a:20068)
- [CR] A. M. Cohen and D. Roozmond, Computing Chevalley bases in small characteristics. *J. Algebra* 322 (2009) 703–721. MR2531218 (2010d:17025)
- [CFL] G. Cooperman, L. Finkelstein and S. Linton, Recognizing  $GL(n, 2)$  in non-standard representation, pp. 85–100 in: *Groups and Computation II*, Proc. DIMACS Workshop (eds. L. Finkelstein and W. M. Kantor), Amer. Math. Soc., Providence 1997. MR1444132 (98d:20054)
- [CoLG] M. Conder and C. R. Leedham-Green, Fast recognition of classical groups over large fields, pp. 113–121 in: *Groups and Computation III* (eds. W. M. Kantor and Á. Seress), Ohio State Univ. Math. Res. Inst. Publ. 8, de Gruyter, Berlin-New York 2001. MR1829474 (2002g:20001)
- [CoLGO] M. D. E. Conder, C. R. Leedham-Green and E. A. O'Brien, Constructive recognition of  $PSL(2, q)$ . *Trans. Amer. Math. Soc.* 358 (2006) 1203–1221. MR2187651 (2006j:20017)
- [Coo] B. N. Cooperstein, The geometry of root subgroups in exceptional groups. I. *Geom. Dedicata* 8 (1979) 317–381. MR550374 (81e:20022)
- [CKS] C. W. Curtis, W. M. Kantor and G. M. Seitz, The 2-transitive permutation representations of the finite Chevalley groups. *Trans. Amer. Math. Soc.* 218 (1976) 1–59. MR0422440 (54:10429)
- [DF] D. I. Deriziotis and A. P. Fakiolas, The maximal tori of the finite Chevalley groups of type  $E_6$ ,  $E_7$  and  $E_8$ . *Comm. Alg.* 19 (1991) 889–903. MR1102992 (92c:20081)
- [Di] L. E. Dickson, *Linear Groups, with an Exposition of the Galois Field Theory* (1900). Reprinted, Dover, New York, 1958. MR0104735 (21:3488)
- [Dix] J. D. Dixon, Generating random elements in finite groups. *Electronic J. Combinatorics* 13 (2008), #R94. MR2426157 (2009j:20093)
- [FJ] P. Fleischmann and I. Janiszczak, The semisimple conjugacy classes and the generic class number of the finite simple groups of Lie type  $E_8$ . *Comm. Alg.* 22 (1994) 2221–2303. MR1268550 (95b:20025)
- [GLS] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups*. No. 3. Part I. Chapter A. Almost simple K-groups. Amer. Math. Soc., Providence 1998. MR1490581 (98j:20011)
- [GKKL1] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: a quantitative approach. *J. Amer. Math. Soc.* 21 (2008) 711–774. MR2393425 (2010c:20011)
- [GKKL2] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: a computational approach. *J. Eur. Math. Soc.* 13 (2011) 391–458. MR2746771 (2011m:20035)
- [GPPS] R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, Linear groups with orders having certain primitive prime divisors. *Proc. Lond. Math. Soc.* 78 (1999) 167–214. MR1658168 (99m:20113)
- [HLORW] P. E. Holmes, S. A. Linton, E. A. O'Brien, A. J. E. Ryba and R. A. Wilson, Constructive membership in black-box groups. *J. Group Theory* 11 (2008) 747–763. MR2466905 (2009i:20001)
- [Ka1] W. M. Kantor, Subgroups of classical groups generated by long root elements. *Trans. Amer. Math. Soc.* 248 (1979) 347–379. MR522265 (80g:20057)
- [Ka2] W. M. Kantor, Primitive permutation groups of odd degree, and an application to finite projective planes. *J. Algebra* 106 (1987) 15–45. MR878466 (88b:20007)

- [Ka3] W. M. Kantor, Simple groups in computational group theory, pp. 77–86 in: Proc. International Congress of Mathematicians, Vol. II, Documenta Math., Berlin 1998. MR1648058 (99h:20002)
- [K11] P. B. Kleidman, The maximal subgroups of the Chevalley groups  $G_2(q)$  with  $q$  odd, the Ree groups  ${}^2G_2(q)$ , and their automorphism groups. J. Algebra 117 (1988) 30–71. MR955589 (89j:20055)
- [K12] P. B. Kleidman, The maximal subgroups of the finite Steinberg triality groups  ${}^3D_4(q)$  and of their automorphism groups. J. Algebra 115 (1988) 182–199. MR937609 (89f:20024)
- [KS1] W. M. Kantor and Á. Seress, Black box classical groups. Mem. Amer. Math. Soc. 149 (2001), No. 708. MR1804385 (2001m:68066)
- [KS2] W. M. Kantor and Á. Seress, Permutation group algorithms via black box recognition algorithms, pp. 436–446 in: Groups St Andrews 1997 in Bath (eds. C. Campbell et al.), LMS Lectures Notes Series 261, Cambridge U. Press, Cambridge 1999. MR1676640 (2000h:20007)
- [KS3] W. M. Kantor and Á. Seress, Prime power graphs for groups of Lie type. J. Algebra 247 (2002) 370–434. MR1877859 (2003a:20026)
- [KS4] W. M. Kantor and Á. Seress, Large element orders and the characteristic of Lie-type simple groups. J. Algebra 322 (2009) 802–832. MR2531224 (2010d:20018)
- [LG] C. R. Leedham-Green, The computational matrix group project, pp. 229–247 in: Groups and Computation III (eds. W. M. Kantor and Á. Seress), Ohio State Univ. Math. Res. Inst. Publ. 8, de Gruyter, Berlin-New York 2001. MR1829483 (2002d:20084)
- [LO] 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. MR2352733 (2008i:20058)
- [LS] M. W. Liebeck and G. M. Seitz, Subgroups generated by root elements in groups of Lie type. Ann. of Math. 139 (1994) 293–361. MR1274094 (95d:20078)
- [LSS] M. W. Liebeck, J. Saxl and G. M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type. Proc. Lond. Math. Soc. 65 (1992) 297–325. MR1168190 (93e:20026)
- [LMO] F. Lübeck, K. Magaard and E. A. O’Brien, Constructive recognition of  $SL(3, q)$ . J. Algebra 316 (2007) 619–633. MR2356848 (2008j:20039)
- [NP] P. M. Neumann and C. E. Praeger, A recognition algorithm for special linear groups. Proc. Lond. Math. Soc. 65 (1992), 555–603. MR1182102 (93m:20063)
- [PW] C. W. Parker and R. A. Wilson, Recognizing simplicity of black-box groups by constructing involutions and their centralisers. J. Algebra 324 (2010) 885–915. MR2659204 (2011j:20032)
- [Ri] R. J. Riebeck, Computations in association schemes. Ph.D. thesis, Techn. U. Eindhoven 1998. MR1620656 (99d:05089)
- [Ser] Á. Seress, Permutation group algorithms, Cambridge U. Press, Cambridge 2002. MR1970241 (2004c:20008)
- [Shi] K. Shinoda, The conjugacy classes of Chevalley groups of type  $F_4$  over fields of characteristic 2. J. Fac. Sci. Univ. Tokyo 21 (1974) 133–159. MR0349863 (50:2356)
- [Sho] T. Shoji, The conjugacy classes of Chevalley groups of type  $F_4$  over fields of characteristic  $\neq 2$ . J. Fac. Sci. Univ. Tokyo 21 (1974) 1–17. MR0357641 (50:10109)
- [St] R. Steinberg, Generators, relations and coverings of algebraic groups, II. J. Algebra 71 (1981) 527–543. MR630615 (83d:14025)
- [Zs] K. Zsigmondy, Zur Theorie der Potenzreste. Monatsh. Math. Phys. 3 (1892) 265–284. MR1546236

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OREGON, EUGENE, OREGON 97403  
*E-mail address:* [kantor@uoregon.edu](mailto:kantor@uoregon.edu)

SCHOOL OF MATHEMATICS, UNIVERSITY OF BIRMINGHAM, EDGBASTON, BIRMINGHAM B15 2TT  
 UNITED KINGDOM  
*E-mail address:* [k.magaard@bham.ac.uk](mailto:k.magaard@bham.ac.uk)