Black box exceptional groups of Lie type II

Magaard, Kay; Kantor, W. M.

DOI:
10.1016/j.jalgebra.2014.09.003

Document Version
Early version, also known as pre-print

Citation for published version (Harvard):
Magaard, K & Kantor, WM 2015, 'Black box exceptional groups of Lie type II', *Journal of Algebra*, vol. 421, pp. 524-540. https://doi.org/10.1016/j.jalgebra.2014.09.003

BLACK BOX EXCEPTIONAL GROUPS OF LIE TYPE II

WILLIAM M. KANTOR AND KAY MAGAARD

ABSTRACT. If a black box group G is known to be isomorphic to an exceptional simple group $\hat{G}$ of Lie type of (twisted) rank > 1, other than any ${}^2F_4(2^e)$ or ${}^3D_4(2^e)$, over a field of known size q, and if suitable SL2 and Discrete Log oracles are available when q is odd, then a polynomial-time Las Vegas algorithm is given that produces a constructive isomorphism between $\hat{G}$ and G.

Dedicated to the memory of Ákos Seress

1. INTRODUCTION

Given generators for a (quotient of a) finite permutation group or matrix group that is known (probably) to be simple, [LG, Ka2, Se2, BBS] and other papers require a computationally efficient isomorphism with an explicitly defined simple group. This type of result has been extensively studied in the more general setting of black box classical groups [KS, Br1, Br2, Br3, BrK1, BrK2, LMO]. In [KM] we handled most but not all families of black box exceptional groups of Lie type, providing algorithms that do not quite run in polynomial time when the field size is large.

At present, for groups of odd characteristic there are no polynomial-time algorithms for such problems, neither in the black box setting nor even in the matrix group one. (For characteristic 2 see Section 2.2.) A standard way around this obstacle involves a lovely idea in [CLG] (used in [BrK1, BrK2, Br2, Br3, LMO] and discussed further in [Se2]): *use an oracle* that constructively recognizes the groups $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$. This was motivated by [CLG, LGO], which provide a constructive polynomial-time Las Vegas algorithm for handling a group isomorphic to $\mathrm{SL}(2,q)$ or $\mathrm{PSL}(2,q)$ 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. These oracles have the effect of removing annoying factors q. The present paper requires such oracles for odd q in order to achieve polynomial time. For statements of our results it is convenient to presuppose oracles for all q, but for even q this should be ignored, as discussed at length in Section 2.2.

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; we will assume that $|\mathcal{S}|$ is small and hence suppress it in our timing estimates. Let μ be an upper bound on the time required for each group operation in G, let $\xi \geq \mu|\mathcal{S}|$ be an upper bound on the time requirement per element for the construction of independent, (nearly) uniformly distributed random elements of G [Ba, Di], and let $\chi \geq \mu \log q$ be an upper bound on the time requirement for each application of one

2000 *Mathematics Subject Classification.* Primary: 20D06, 20G40 Secondary: 20B40, 20G41, 20P05, 68Q25.

This research was supported in part by NSF grant DMS 0900932 and NSA grant MDA-9049810020.

of the hypothesized oracles in the following theorem, *or let* $\chi = \mu \log^3 q \log\log q$ when q is even. (*When q is even we do not require any oracle.*)

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 finite simple exceptional group of Lie type of (twisted) rank > 1 and given field size q, other than any ${}^2F_4(2^e)$ or ${}^3D_4(2^e)$ – also assuming* for odd q *the availability of an $\mathrm{SL}(2,q)$-oracle and a Discrete Log oracle for $\mathbb{F}_q^*$ (and also a $\mathrm{PSL}(2,q^2)$-oracle and a Discrete Log oracle for $\mathbb{Z}_{q+1}$ when G has type ${}^2E_6(q)$, and also an $\mathrm{SL}(2,q^3)$-oracle and a Discrete Log oracle for $\mathbb{F}_{q^3}^*$ when G has type ${}^3D_4(q)$) – finds the following*:*

(i) *The name of the simple group of Lie type to which $G/\mathrm{Z}(G)$ 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 $\Psi : \hat{G} \to G$, specified by the requirement that $\hat{\mathcal{S}}\Psi = \mathcal{S}^*$.*

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 $O(\log q)$ 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 Las Vegas, running in $O(\xi \log q \log\log q + \chi \log^2 q \log\log q + \log^4 q)$ time and succeeding with probability $> 1/2$.*
In additional $O(\xi + \chi \log^2 q)$ time it can be verified that G is isomorphic to a perfect central extension of the exceptional group in (i).

(vii) *The algorithm for* (iii) *is Las Vegas, running in $O(\xi + \chi \log q)$ time and succeeding with probability $> 1/2$; while the algorithm for* (iv) *is deterministic and runs in $O(\mu \log q)$ time except for G of type ${}^2E_6$, where it is Las Vegas, takes $O(\xi + \chi \log q)$ time and succeeds with probability $> 1/2$.*

(viii) *The center of G can be found in $O(\mu \log q)$ time.*

Parts (ii-iv) are the requirements for a *constructive epimorphism* $\Psi : \hat{G} \to G$. It may be worth noting that the algorithm for (iii) also works for (iv), but is much slower. 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 (as in Section 3.3, and in each of the later sections of this paper; cf. [KM]). In practice, it is hard to imagine that this test would be omitted.

The stated times are designed to deal with all types of groups G simultaneously. As in [KS, KM], we will see that the times are significantly less for most G.

For the proof of the theorem we will modify the previous approach [KM], simplifying some parts outlined in [KM, Sec. 6]. The main goal is to find a long root group, after which much of [KM] can be reused. It seems undesirable to entirely rewrite the previous paper since many of the same ideas can be used. Thus, the present paper is essentially a long addendum to that one, and the two should be used side by side. However, there are some new ideas involved, including [KK] and elementary cohomology (Section 4.3). Related results appear in [LO] in a different context that presupposes, among other things, an absolutely irreducible module for the group.

We will use standard notions discussed at length in [KS, KM], such as black box groups, straight-line programs, the parameters ξ and μ in the theorem, and primitive prime divisors. See [BrK1, p. 97] for a discussion of χ. We will use the notation $\hat{G}$, $\hat{R}$, $\hat{L}$, $\hat{Q}$ in [KM, Secs. 2.1, 3.1] for the "standard" models of the groups studied here, and for some of their subgroups. Finding nearly uniformly distributed elements of a black box group G originated in [Ba], with another version in [Di] (cf. [KS, Se1]).

As in [KS, KM] and other papers, our probabilistic estimates are very crude, leading to the use of samples of unreasonably large numbers of group elements in order to simplify the exposition.

This paper owes its existence to Ákos Seress. Even before the previous version [KM] had been accepted for publication, he had already strongly urged us to provide details for a polynomial-time version assuming suitable standard oracles. This led us to outline methodology for this purpose in [KM, Sec. 6], with the expectation that would lead to the present paper.

The first author is also indebted to Ákos for teaching him many things about the subject matter of this paper - such as why explicit probability estimates (even very poor or ugly ones) are needed for implementations.

2. Preliminaries

2.1. **Background.** See [Ca] and [KM] for the required notation and properties concerning the groups in Theorem 1.1. Let $\mathbb{F} = \mathbb{F}_q$, $q = p^e$, for a prime p, and $\mathbb{F}' = \mathbb{F}$ except that $\mathbb{F}' = \mathbb{F}_{q^2}$ in the case ${}^2E_6(q)$. These fields are equipped with $\mathbb{F}_p$-bases, one of whose elements is assumed to generate the multiplicative group when q is odd (for use with the hypothesized Discrete Log oracle); the basis for $\mathbb{F}'$ contains one for $\mathbb{F}$. We will ignore fields of very small order. Among other things, this allows us to avoid exceptional parts of Schur multipliers [GLS, p. 313].

2.2. **Avoiding Discrete Logs.** Discrete Logs are a fundamental tool in [CLG, LGO] for recognizing $\mathrm{SL}(2,q)$ in its absolutely irreducible representations over fields of characteristic $p|q$. As a result, both $\mathrm{SL}(2,q)$ and Discrete Log oracles were used for black box groups in [Br1, Br2, Br3, BrK1, BrK2, LMO], which constructed subgroups isomorphic to $\mathrm{SL}(2,q)$ that were then constructively recognized using the $\mathrm{SL}(2,q)$-oracle. We refer to [Br1, Br2, Br3, BrK1] for discussions of the definition and uses of such oracles.

Now that constructive recognition can be achieved in some characteristics without an $\mathrm{SL}(2,q)$-oracle, we will explain why *Discrete Logs are not needed at all if they are not used to produce isomorphisms with* $\mathrm{SL}(2,q)$ *subgroups.*

In characteristic 2 [KK] and in bounded odd characteristic [BY], a field $F \cong \mathbb{F}_q$ is constructed internally, using operations occurring in the underlying black box group G. Therefore any standard types of field calculations can be accomplished using black box group operations. For example, if $s \in F$ and if $f \in F[x]$ has "small" degree, then $f(s)$ can be found by means of operations in the underlying group G.

This was used in [KK] to find values of the trace map $\mathrm{Tr}\colon F \to \mathbb{F}_p$, which were used in turn to *express any given element* $t \in F$ as $t = f(s)$ when $F = \mathbb{F}_p[s]$, for some polynomial $f \in F[x]$. *We emphasize that* t *is obtained as* $f(s)$ *rather than as a power* s^n, *using operations in* G. In particular, these operations are not performed within the cyclic group $\langle s \rangle$, so that Discrete Logs are not needed.

Theorem 1.1 also uses an $\mathrm{SL}(2,q^3)$-oracle, which is again not needed in characteristic 2. Theorem 1.1 also uses Discrete Logs in $\mathbb{Z}_{q+1}$. This group arises inside the multiplicative group of a field of order q^2, which in turn comes from a (short root) $\mathrm{SL}(2,q^2)$ subgroup of the black box group. Therefore, all of the comments made above continue to hold in this situation: once again Discrete Logs can be avoided for fields of characteristic 2.

2.3. **Smaller rank preliminaries.** As in [KM, Theorem 1.3], we summarize the known results we need concerning classical groups (where μ, ξ and χ are as before):

Theorem 2.1. *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), *where when q is odd we assume the availability of an* $\mathrm{SL}(2,q)$*-oracle and a Discrete Log oracle for $\mathbb{F}_q^*$ (and also a* $\mathrm{PSL}(2,q^2)$*-oracle and a Discrete Log oracle for $\mathbb{Z}_{q+1}$ when G has type* $\mathrm{SU}(6,q)$*). Moreover*,

(i) Theorem 1.1(v) *holds*;
(ii) Theorem 1.1(ii) *takes $O(\xi\log q\log\log q+\chi\log^2 q\log\log q+\log^4 q)$ Las Vegas time, succeeding with probability $>1/2$*;
(iii) Theorem 1.1(iii) *takes $O(\xi+\chi\log q)$ Las Vegas time, succeeding with probability $>1/2$; and*
(iv) Theorem 1.1(iv) *is deterministic and takes $O(\mu\log q)$ time, except in type* $\mathrm{SU}(6,q)$, *where it takes $O(\xi+\chi\log q)$ Las Vegas time, succeeding with probability $>1/2$.*

Theorem 2.1(ii)-(iv) correspond to Theorem 1.1(vi)-(vii).

Proof. This is contained in [Br1, Br2, Br3, BrK1, BrK2], except for the avoidance of oracles for even q as explained in Section 2.2, where each use of an $\mathrm{SL}(2,q)$-oracle in (ii) is replaced by [KK] and χ is replaced by $\mu\log^3 q\log\log q$. The need for a Discrete Log oracle for $\mathbb{F}_q^*$ or $\mathbb{Z}_{q+1}$ occurs in a long or short root $\mathrm{SL}(2,q)$ or $\mathrm{SL}(2,q^2)$ subgroup (cf. [Br2, p. 183]), where it can be dealt with in characteristic 2 as in Section 2.2. □

2.4. **Primitive prime divisors and generation.** The notation $\mathrm{ppd}^\sharp(p;e)$ associated with primitive prime divisors is defined in [KM, Sec. 1.1]. The next two lemmas and their proofs are very similar to [KM, Lemmas 2.24, 2.25], and hence the proofs are omitted.

Long (*root*) *subgroups* are subgroups generated by long root groups. *Short root subgroups* are defined similarly. Examples are a long root $\mathrm{SL}(2,q)$ subgroup $\hat{R}$ of $\hat{G}$ and its centralizer $\hat{L}$.

For now we restrict to rank >2:

Lemma 2.2. *For $\epsilon \in \{1,2\}$ let $k(\epsilon) = \mathrm{ppd}^\sharp(p;\epsilon e)$, and let $\varpi(\epsilon)$ denote the $(p^e+(-1)^\epsilon)'$-part of $|\hat{G}|$. Let l be as follows for the indicated types of $\hat{G}$:*

$$k(\epsilon)\cdot l = \begin{cases} \mathrm{ppd}^\sharp(p;e)\cdot\mathrm{ppd}^\sharp(p;2e)\mathrm{ppd}^\sharp(p;6e) & F_4 \\ \mathrm{ppd}^\sharp(p;e)\cdot\mathrm{ppd}^\sharp(p;2e)\mathrm{ppd}^\sharp(p;3e)\mathrm{ppd}^\sharp(p;6e) & E_6 \\ \mathrm{ppd}^\sharp(p;2e)\cdot\mathrm{ppd}^\sharp(p;e)\mathrm{ppd}^\sharp(p;3e)\mathrm{ppd}^\sharp(p;6e) & {}^2E_6 \\ \mathrm{ppd}^\sharp(p;e)\cdot\mathrm{ppd}^\sharp(p;9e) & E_7 \\ \mathrm{ppd}^\sharp(p;2e)\cdot\mathrm{ppd}^\sharp(p;18e) & E_7 \\ \mathrm{ppd}^\sharp(p;e)\cdot\mathrm{ppd}^\sharp(p;2e)\mathrm{ppd}^\sharp(p;4e)\mathrm{ppd}^\sharp(p;8e) & E_8 \\ \mathrm{ppd}^\sharp(p;e)\cdot\mathrm{ppd}^\sharp(p;2e)\mathrm{ppd}^\sharp(p;18e) & E_8 \end{cases}$$

(i) *If $\tau \in \hat{G}$ has order of the form $k(\epsilon)l$, then $\tau^{\varpi(\epsilon)}$ lies in a long root* $\mathrm{SL}(2,q)$ *subgroup or $\hat{G}$ has type F_4 and $\tau^{\varpi(\epsilon)}$ lies in either a long or short root* $\mathrm{SL}(2,q)$ *subgroup.*

(ii) *With probability $\geq 1/2^9$, an element $\tau \in \hat{G}$ has order of the form $k(\epsilon)l$ and $\tau^{\varpi(\epsilon)}$ lies in a long root* $\mathrm{SL}(2,q)$ *subgroup.*

(iii) *With probability $\geq 1/2^9$, an element $\tau \in \mathrm{N}_{\hat{G}}(\hat{R}\hat{L})$ has order of the form $k(\epsilon)l$ and $\tau^{\varpi(\epsilon)} \in \hat{R}$.*

The integers l are almost the same as in [KM, Sec. 2.9], changed only in order to guarantee in each case that $k(\epsilon)$ and l are relatively prime. Note that $(1-1/2)(1-1/3)(1-1/5)(1-1/7)/72 > 1/2^9$, where $72 = 2\cdot2\cdot3\cdot6$ is the largest possible index $|\mathrm{N}_G(T):\mathrm{C}_G(T)|$ for a maximal torus T of G containing an element of the stated order (see the argument in [KM, Lemma 2.24]). As usual, this estimate is far cruder than needed.

Remark 2.3. We do not know the primes dividing l, hence we do not know l. Consequently, we cannot write τ^l in our algorithm (this was not noticed in [KM, Sec. 2.9]). Instead we have used $\tau^{\varpi(\epsilon)}$. In the E_7- and E_8-cases there are two choices for both $k(\epsilon)$ and $\varpi(\epsilon)$ (although in the E_8-case the two choices coincide). We will write $k(\epsilon)$ and $\varpi(\epsilon)$ for an element τ occurring in the first of these choices, and $k(\epsilon_0)$ and $\varpi(\epsilon_0)$ for an element τ_0 occurring in the second choice.

Lemma 2.4. *Let $\hat{R}_1$ be a long* $\mathrm{SL}(2,q)$ *subgroup contained in $\hat{L}$, and let l (or two such numbers, l and l_0) be as in* Lemma 2.2.

(i) *If $\hat{G}$ is not of type E_7 or E_8, and if $y \in \hat{L}$ has order of the form l, then $\hat{L} = \langle \hat{R}_1, y^{q^2-1}\rangle$.*

(ii) *If $\hat{G}$ is of type E_7 or E_8, and if $y \in \hat{L}$ has order of the form l and $y_0 \in \hat{L}$ has order of the form l_0, then $\hat{L} = \langle \hat{R}_1, y^{q^2-1}, y_0^{q^2-1}\rangle$.*

2.5. **Bray's algorithm.** Since we know the order of the group $\hat{G}$, we can precompute its odd part $2k+1 := |\hat{G}|_{2'}$.

If $t \in G$ is any involution, then Bray's algorithm [Br] (cf. [AB, Bo]) finds elements of $\mathrm{C}_G(t)$: *if g is a* (nearly) *random element of G such that $|tt^g|$ is odd, then*

$$\tilde{g} := (tt^g)^k g^{-1} \text{ is a (nearly) random element of } \mathrm{C}_G(t). \tag{2.5}$$

For the timing of this algorithm we need [PW, Thm. 1] for the groups G in Theorem 1.1: *with probability $\geq 1/1000$, $|[t,g]| = |tt^g|$ is odd for a random conjugate t^g of t.* Note that the actual lower bound is significantly larger than the stated bound,

which will require us to choose unreasonably large numbers of (nearly) random elements. Two random elements generate G with high probability [KL, LSh].

2.6. **General strategy.** Our goal is to reduce to situations already dealt with in [KM]. For this purpose we need to provide substitutes for all parts of [KM] that require a factor of q in the timing. Once this has been accomplished we refer to [KM] for the remainder of the algorithm. In particular, probability and timing estimates require the inclusion of ones from parts of [KM].

We use [BKPS] for Theorem 1.1(i) and [BGKLP] for the last requirement in Theorem 1.1(vi).

3. Rank > 2 in odd characteristic

In this section we assume that G is a black box group in Theorem 1.1 of rank > 2 over a field of odd order $q > 9$.

3.1. **Finding R and L.**

Lemma 3.1. *The following can all be found in $O(\xi \log q \log\log q + \chi \log^2 q \log\log q + \log^4 q)$ time with probability $> 1 - 1/2^9$: (i) an involution t such that $\mathrm{C}_G(t)$ has commuting, normal long root subgroups $R \cong \hat{R}$ and $L \cong \hat{L}$, (ii) these subgroups R and L, and (iii) constructive isomorphisms $\Psi_R \colon \hat{R} \to R$ and $\Psi_L \colon \hat{L} \to L$.*

Proof. Find up to 10^4 nearly uniformly distributed elements $y \in G$ [Ba, Di], for each test whether $|y|$ is even, and if so let $t \in \langle y \rangle$ be an involution.

Find up to $10 \cdot 2^{40}$ pairs g, h of nearly uniformly distributed elements of G. For each such pair, test whether $|tt^g|$ and $|tt^h|$ are both odd, in which case use (2.5) to obtain $\tilde{g}, \tilde{h} \in C := \mathrm{C}_G(t)$; test whether $\tilde{g}$ and $\tilde{h}$ both have orders of the form $k(\epsilon) \cdot l$ appearing in Lemma 2.2 (require that $\tilde{g}$ and $\tilde{h}$ have the two different order possibilities in the E_7- and E_8-cases; cf. Remark 2.3); use the hypothesized $\mathrm{SL}(2,q)$-oracle to test whether $R := \langle \tilde{g}^{\varpi(\epsilon)}, \tilde{h}^{\varpi(\epsilon)} \rangle \cong \mathrm{SL}(2,q)$ and to obtain a constructive isomorphism $\Psi_R \colon \mathrm{SL}(2,q) \to R$ (use $R := \langle \tilde{g}^{\varpi(\epsilon)}, \tilde{h}^{\varpi(\epsilon_0)} \rangle$ in the E_7- and E_8-cases); use Ψ_R to check whether $\tilde{g}$ and $\tilde{h}$ induce inner automorphisms on R induced by some $g_R, h_R \in R$; and finally use Theorem 2.1 (or Theorem 1.1 for groups of type E_7 in the E_8-case) to test whether $\hat{L} \cong L := \langle \tilde{g} g_R^{-1}, \tilde{h} h_R^{-1} \rangle$ and to find a constructive isomorphism $\Psi_L \colon \hat{L} \to L$.

For correctness, note that the order of $\tilde{g}$ implies that t is the type of involution whose centralizer is as in the lemma. Then C has a subgroup of index 2 that is the central product of subgroups isomorphic to $\hat{R}$ and $\hat{L}$. Moreover, by [KL, LSh], $\langle \tilde{g}, \tilde{h} \rangle$ is (probably) either C or its subgroup of index 2 (since $\tilde{g}, \tilde{h} \in C$ are nearly uniformly distributed elements (2.5)), and we have found the latter subgroup RL together with R and L.

Time: $O(\xi \log q \log\log q + \chi \log^2 q \log\log q + \log^4 q)$, dominated by Theorem 2.1.

Reliability: $> 1 - 1/2^9$. For, by [PW, Thm. 3], a single choice $\langle y \rangle$ will contain an involution t central in a Sylow 2-subgroup of G with probability $\geq 1/10^3$, so that all 10^4 choices fail with probability $\leq (1 - 1/10^3)^{10^4} < 1/2^{10}$.

By [PW, Thm. 1], $|tt^g|$ and $|tt^h|$ are both odd with probability $\geq (1/10^3)^2$. Then by [KL, Ka1, LSh], $\langle \tilde{g}, \tilde{h} \rangle$ is either C or its subgroup of index 2 with probability $> (1/5)(1/10)$ (recall that $q > 9$). By Lemma 2.2(iii) and (2.5), $\tilde{g}$ and $\tilde{h}$ have the

desired order(s) with probability $\geq (1/2^9)^2$; both induce inner automorphisms of R with probability $(1/2)^2$. Each test of $\hat{L} \cong L$ using Theorem 2.1 (or Theorem 1.1 in the E_8-case) succeeds with probability $> 1/2$. Hence, one of our pairs g, h produces the desired result with probability $> (1/10^3)^2(1/5)(1/10)(1/2^9)^2(1/2)^2(1/2) > 1/2^{40}$, so that all $10 \cdot 2^{40}$ pairs fail with probability $< 1/2^{10}$. $\square$

Note that we could have used a Monte Carlo algorithm to find the derived subgroup of C [BCFLS] (cf. [Se1, Thm. 2.3.12]). However, we still needed to find R and L, which led to the above procedure in place of normal closure and derived subgroup routines.

3.2. **Root groups and Q.** At this point we can use $\hat{R}$ and $\hat{L}$ together with Ψ_R and Ψ_L to perform standard calculations in RL. For G not of type E_8 this involves straightforward linear algebra. When G has type E_8 we refer to [KM, Appendix], which uses the Lie algebra of $\hat{E}_7(q)$.

Use Ψ_R and Ψ_L to find maximally split tori of R and of L; their product T_0 is a maximally split torus of RL. Similarly, find $\mathrm{N}_{RL}(T_0)$. (Although T_0 has index 2 in a maximal torus for G, it suffices for our purposes since $q > 9$.)

Find the set Γ_L of all root groups of L normalized by T_0. Two of them generate a long $\mathrm{SL}(2, q)$ subgroup $R_1 < L$. Let t_1 be the involution in R_1. Using up to 10^7 choices, find a conjugate t_2 of t such that both $|tt_2|$ and $|t_2t_1|$ are odd, and therefore find an element $y := (tt_2)^m(t_2t_1)^m$ conjugating t to t_1 and hence L to $L_1 := \mathrm{C}_G(R_1)$, where $2m - 1 = |\hat{G}|_{2'}$. Then R_1L_1 has index 2 in $\mathrm{C}_G(t_1)$, and T_0 normalizes L_1 since it normalizes R_1. Also obtain a constructive isomorphism $\Psi_{L_1} \colon \hat{L} \to L_1$ using y and Ψ_L.

Use Ψ_{L_1} to find the maximally split torus T_1 of L_1 normalized by T_0, together with $\mathrm{N}_{L_1}(T_1)$. Then $N := \langle \mathrm{N}_{RL}(T_0), \mathrm{N}_{L_1}(T_1) \rangle$ is the normalizer in G of a maximally split torus of G. (Note the simplification compared to [KM, Sec. 2.10] due to the use of both L and L_1.)

Use Ψ_{L_1} to find the set Γ_{L_1} of all root groups of L_1 normalized by T_1, so that $\Gamma_L \cup \Gamma_{L_1}$ lies in a set Γ of at most 240 root groups of G permuted by N. Find this set Γ using conjugation by elements of N, labelling these root groups X_α using elements α of the root system Φ for G containing the root system for RL (cf. [KM, Sec. 2.11]). We now have a root group X_α corresponding to each $\alpha \in \Phi$.

Let Δ be a base of Φ containing a base of L, and let $\nu \in \Delta$ be the highest root. We may assume that $X_{\pm\nu} < R$. Then $L = \langle X_\alpha \mid \alpha \in \Phi \text{ is perpendicular to } \nu \text{ and } -\nu \rangle$.

Let Q be the group generated by those X_α for which $\alpha \in \Phi$ is positive and not a root of L (as in [KM, Sec. 2.13]). Then $X_\nu \leq \mathrm{Z}(Q)$ and $\mathrm{C}_G(X_\nu) = LQ$.

There is a unique long root $\nu' \in \Delta$ not orthogonal to ν.

Time: $O(\xi + \chi \log q)$.

Reliability: $> 1 - 1/2^{10}$. For, by [PW, Thm. 1], we find a single t_2 with probability $\geq (1/10^3)^2$. Then all 10^7 choices fail with probability $< 1/2^{10}$.

3.3. **The group G_0.** Proceed as in [KM, Sec. 2.12] in order to obtain

- a label $X_\alpha(t)$ of any given element of any root group X_α by an element t in $\mathbb{F}$ or $\mathbb{F}'$, and then also
- generating sets $\mathcal{S}^* \subset \cup_{\alpha \in \Phi} X_\alpha$ of $G_0 := \langle X_\alpha \mid \alpha \in \Phi \rangle$ and $\hat{\mathcal{S}} \subset \cup_{\alpha \in \Phi} \hat{X}_\alpha$ of $\hat{G}$ of size $O(\log q)$, as well as
- the natural epimorphism $\Psi \colon \hat{G} \to G_0$ sending $\hat{\mathcal{S}} \to \mathcal{S}^*$.

3.4. **Completion of the proof.** Both effective transitivity with the help of long $\mathrm{SL}(3,q)$ subgroups, and linear algebra in Q/X_ν, are handled exactly as in [KM, Secs. 2.13 and 2.14].

We find a straight-line program from $\mathcal{S}^*$ to any given element of G as in [KM, Sec. 2.15]. More precisely, in order to deal with [KM, Prop. 2.39(iii)] we use a call to the hypothesized Discrete Log oracle: we are given $g \in G$ and need to find a straight-line program to g from our new generators. We reduce to the situation where g normalizes both X_ν and $X_{-\nu}$. As in [KM, Prop. 2.39(iii)] we also have the element $h_{\nu'}(\zeta)$ for a generator ζ of $\mathbb{F}^*$. Both g and $h_{\nu'}(\zeta)$ act on $R = \langle X_\nu, X_{-\nu}\rangle$, and the Discrete Log oracle provides us with an exponent k such that $gh_{\nu'}(\zeta)^k$ centralizes R. At this point the rest of the argument used in [KM, Prop. 2.39(iii)] goes through.

Now [KM, Cor. 2.42 and Sec. 2.16] complete the proof of Theorem 1.1 for rank > 2 and odd q.

4. Rank > 2 in characteristic 2

In this section we assume that G is a black box group in Theorem 1.1 of rank > 2 over a field of even order $q > 4$. We will modify the previous approach [KM, Sec. 2] slightly, and also in Section 4.3 outline a second modification for one part of the algorithm.

4.1. **Preliminaries.**

Lemma 4.1. *Two elements r_1, r_2 of G that lie in long $\mathrm{SL}(2,q)$ subgroups R_1, R_2, respectively, and have order either $\mathrm{ppd}^\sharp(p,e)$ or $\mathrm{ppd}^\sharp(p,2e)$, satisfy the condition that $\langle r_1, r_2\rangle = \langle R_1, R_2\rangle$ is a long $\mathrm{Spin}_8^-(q)$ subgroup with probability $> 1/100$.*

Proof. We first show that *two long $\mathrm{SL}(2,q)$ subgroups of G generate a $\mathrm{Spin}_8^-(q)$ subgroup with probability $> 1/81$.* (As usual, our estimate is rather weak in order to simplify arguments.) For probability purposes, we can start with a long $\mathrm{SL}(2,q)$ subgroup R together with one of its long root groups Z; and choosing a conjugate of R is the same as choosing two opposite long root groups Z_1, Z_2. Therefore, we choose a long root group Z_1. With probability $> 1/3$ it is opposite Z [KM, Lemma 2.26], in which case $S := \langle R, Z_1\rangle \cong \mathrm{SL}(3,q)$ with probability $\geq 1/3$ [KM, Lemma 2.27(i)]. Choose a long root group Z_2. With probability $> 1/3$ it is opposite Z_2. If $S \cong \mathrm{SL}(3,q)$, then $\langle S, Z_2\rangle \cong \mathrm{Spin}_8^-(q)$ with probability $\geq 1/3$ [KM, Lemma 2.27(ii)]. Hence, $\langle R, Z_1, Z_2\rangle \cong \mathrm{Spin}_8^-(q)$ with probability $> (1/3)^4$, as claimed.

Now consider two elements r_i of order as in the lemma, lying in long $\mathrm{SL}(2,q)$ subgroups R_i $(i = 1,2)$. We will show that, *if $J := \langle R_1, R_2\rangle \cong \mathrm{Spin}_8^-(q)$, then $\langle r_1, r_2\rangle = J$ with probability $> 1 - 1/2^{10}$.* In view of the preceding paragraph, the resulting lower bound $(1/81)(1 - 1/2^{10}) > 1/100$ will prove the lemma.

If V is the natural module for $J = \mathrm{Spin}_8^-(q) \cong \Omega^-(8,q)$, then $[V, r_i] = [V, R_i]$ for $i = 1,2$, so that $J_0 := \langle r_1, r_2\rangle$ is irreducible on V. We will repeatedly use the fact that $[V, r_i] = [V, R_i]$ is of type 4^+, as well as the assumption that q is even.

We consider the possible maximal overgroups M of J_0 using [KL, p. 74, Table 3.5.f], starting with the possible "geometric" groups

(1) $\Omega^-(8, q_0)$ with $q_0^r = q$ for some prime r, or $\Omega^-(4, q^2) \cong \mathrm{SL}(2, q^4)$ (a member of the class $\mathcal{C}_3$).

The possibility $M = \Omega^-(4, q^2)$ is eliminated using $[V, r_i]$.

For the possible overgroups M in class $\mathcal{S}(\Omega^-(8, q))$ in characteristic 2 we use Steinberg's Tensor Product Theorem: we need tensor products of 2-restricted representations, hence of dimension 2 or 4. By [Lu, Tables 6.6–6.53], only

(2) $\mathrm{SL}(3, q)$ and $\mathrm{SU}(3, q)$

have degree 8 representations. (Note: The irreducible 8-dimensional group $\mathrm{Spin}_7(q)$ lies in $\mathrm{Spin}_8^+(q)$ rather than $\mathrm{Spin}_8^-(q)$, due to triality.)

We next consider twisted tensor product possibilities. The only groups having 2-restricted representations of dimension 2 are $\mathrm{SL}(2, q)$, whereas the ones having 2-restricted representations of degree 4 are $\mathrm{SL}(2, q^2) \cong \Omega^-(4, q)$, $\mathrm{Sz}(q)$, $\mathrm{Sp}(4, q)$ and $\mathrm{SL}(4, q)$. None of the latter embeds into $\Omega^-(8, q)$. Similarly, the 8-dimensional representation of $\mathrm{SL}(2, q^3)$ that is the twisted tensor product of three 2-dimensional representations of $\mathrm{SL}(2, q^3)$ embeds into $\Omega^+(8, q)$ and hence not into $\Omega^-(8, q)$.

To find the maximal overgroups in Aschbacher class $\mathcal{S}(\Omega^-(8, q))$ having odd characteristic, we use [HM2, Table 2, p. 97] and [HM1, Table 2, p. 31]. With the exception of $\mathrm{PSL}(2, 7) \cong \mathrm{SL}(3, 2)$ occurring in (2), there is no example. (Note: The irreducible 8-dimensional $\mathbb{F}_q$-representations of $A_6 \cong \mathrm{PSL}(2, 9)$ and A_9 embed into $\Omega^+(8, 2)$ and hence not into $\Omega^-(8, 2)$.)

For each possible overgroup M we need to estimate the number of pairs (t_1, t_2) lying in a J-conjugate of M, where t_i is G-conjugate to r_i.

For the groups in (1), elements r_i of the required ppd order centralizing a 4^--subspace of V cannot lie in a subfield group $M = \mathrm{Spin}_8^-(q_0)$ unless $q = q_0^2$, in which case r_1 and r_2 have ppd order dividing $q - 1$. Since $q \geq 8$, we find that the proportion of pairs (t_1, t_2) lying in J-conjugates of M is $|M^J||r_i^M|^2/|r_i^J|^2 \leq 1/2^{11}$.

Finally, for the groups $M \cong \mathrm{SL}(3, q)$ or $\mathrm{SU}(3, q)$ in (2), V is the adjoint module and $q \equiv 2$ resp. 1 (mod 3) in order to have M contained in $\mathrm{Spin}_8^-(q)$. Since $\dim \mathrm{C}_V(r_i) = 4$, it follows that (in the natural M-module) each element r_i is conjugate to $r_i' = \mathrm{diag}(\alpha_i, \alpha_i, \alpha_i^{-2})$ for some α_i, where $\alpha_i \bar{\alpha}_i = 1$ in the unitary case. Then $\mathrm{C}_V(r_i')$ consists of all $\left(\begin{smallmatrix} A & 0 \\ 0 & \mathrm{Tr}(A) \end{smallmatrix}\right)$ for 2×2 matrices A that are hermitian in the unitary case, and $\mathrm{C}_V(r_i')$ has type 4^- due to the nature of q (mod 3). This time we find that the proportion of pairs (t_1, t_2) lying in J-conjugates of M is $|M^J||r_i^M|^2/|r_i^J|^2 < 1/2^{12}$.

The previous probabilities produce the desired lower bound $1 - 1/2^{10}$. □

Lemma 4.2. *Let g be an element of a long $\mathrm{SL}(2, q)$ subgroup R and have order either $\mathrm{ppd}^\sharp(p, e)$ or $\mathrm{ppd}^\sharp(p, 2e)$. Then R is the unique long $\mathrm{SL}(2, q)$ subgroup containing g.*

Proof. Suppose that $g \in R, R^x$ with $R \neq R^x$, $x \in G$. Then $L < H := \langle L, L^x \rangle$. The maximal overgroups M of L in G are $\mathrm{N}_G(Q)$ and $\mathrm{N}_G(L)$, and also $M = \mathrm{Sp}(8, q)$ when $G = F_4(q)$ since q is even (e. g., by [LSe, Thm. 1.1]).

If $H \leq \mathrm{N}_G(Q)$ then $H = H' \leq \mathrm{C}_G(Q) = QL$, so that $H = QL$. Then $g \in \mathrm{C}_G(QL) = \mathrm{Z}(Q)$, whereas $|g| \neq 2$.

The group $\mathrm{N}_G(L)$ contains only one copy of L.

Finally, if $L < H \leq M = \mathrm{Sp}(8, q)$ with $G = F_4(q)$ then, since H is not in $\mathrm{N}_M(L)$, we see that H is M or $\Omega^\pm(8, q)$, or lies in $\mathrm{N}_M(\mathrm{Z}(Q))$, where $|\mathrm{Z}(Q)| = q^7$. Each of the first three possibilities contains a maximal torus T of G, which produces the contradiction $g \in \mathrm{C}_G(H) = \mathrm{C}_G(H) \cap \mathrm{C}_G(T) = \mathrm{C}_G(H) \cap T = 1$. In the final

case, $H = (Q \cap M)L = \mathrm{C}_M(\mathrm{Z}(Q))$, so that $g \in \mathrm{C}_G(H) = \mathrm{Z}(Q)$, which is again a contradiction. □

4.2. **Finding** J, R**.** Choose up to 2^{18} elements $g \in G$ to find one whose order has the form $k(\epsilon)l$ in Lemma 2.2 and, in the E_7- and E_8-cases, another element g_0 of the second order $k(\epsilon_0)l_0$, say, in that lemma. Let $\varpi(\epsilon_1)$ denote $\varpi(\epsilon_0)$ in the latter situations and $\varpi(\epsilon)$ otherwise (cf. Remark 2.3).

Choose up to 1000 conjugates g_1 of g (or of g_0 in the E_7- and E_8-cases), in order to find one such that $J := \langle g^{\varpi(\epsilon)}, g_1^{\varpi(\epsilon_1)} \rangle$ is a long $\mathrm{Spin}_8^-(q)$ subgroup (cf. Lemma 4.1), using Theorem 2.1 (or a recursive call to Theorem 1.1) up to 10 times for each g_1 to test whether $\hat{J} := \mathrm{Spin}_8^-(q) \cong J$ and to find a constructive isomorphism $\Psi_J \colon \hat{J} \to J$.

Use $\hat{J}$ and Ψ_J to find long root $\mathrm{SL}(2,q)$ subgroups R and R_1 of J containing $g^{\varpi(\epsilon)}$ and $g_1^{\varpi(\epsilon_1)}$, respectively (cf. Lemma 4.1). In addition, find $\mathrm{C}_J(R)$ and opposite long root groups Z and Z^- in R, together with R_2, a long root $\mathrm{SL}(2,q)$ subgroup of $\mathrm{C}_J(R)$ (lying in a long root $\Omega^+(4,q)$ subgroup of J containing R).

In the E_7- and E_8-cases use Ψ_J to find a J-conjugate g_* of g_1 such that $g_*^{\varpi(\epsilon_1)} \in R$.

Time: $O(\xi \log q \log\log q + \chi \log^2 q \log\log q + \log^4 q)$, dominated by Theorem 2.1.

Reliability: $> 1 - 1/2^8$. For, by Lemma 2.2(ii), g has the desired order with probability $\geq 1/2^9$, so that one of our 2^{18} choices behaves correctly with probability $> 1 - 1/2^9$. We obtain g_0 with the same probability. By Lemma 4.1, one of our 1000 choices for g_1 produces the desired generation with probability $> 1 - 1/2^{10}$. Finally, one of the 10 calls to Theorem 2.1 (or a recursive call to Theorem 1.1) succeeds with probability $> 1 - 1/2^{10}$.

4.3. **Finding** L**.** Recall that $|g|$ has the form $k(\epsilon)l$. Since $g^{k(\epsilon)}$ centralizes $g^{\varpi(\epsilon)} \in R$ it normalizes R (by Lemma 4.2). Then $g^{q^2-1} \in \mathrm{C}_G(R)$ since $|g^{q^2-1}|$ is relatively prime to $|R|$. If we exclude the E_7- and E_8-cases, then $L := \langle g^{q^2-1}, R_2 \rangle$ is $\mathrm{C}_G(R)$ by Lemma 2.4. Similarly, in the excluded cases $g_*^{q^2-1} \in \mathrm{C}_G(R)$, so that $L := \langle g^{q^2-1}, g_*^{q^2-1}, R_2 \rangle$ is $\mathrm{C}_G(R)$, again by Lemmas 4.2 and 2.4.

Cohomological digression. We will present an alternative method for finding L*.* The preceding approach recycled the elements g (and g_0) already used to find J. It was natural since these elements (or J-conjugates of them) were also used to write a generating set for L. The following alternative approach does not seem as fast in general, and certainly has no effect on the overall timing, but nevertheless might have some interest. We will take a much more relaxed and less detailed approach than usual, ignoring crucial details of timing and probability. We start with a very elementary cohomological observation (which does not even involve finite groups or finite vector spaces):

Lemma 4.3. *Assume that H is a group acting on a vector space V. Let $h \in \mathrm{Z}(H)$ be such that the linear transformation $-h \colon v \mapsto -v^h$ fixes no nonzero vector and has order dividing the odd integer $2m+1$. If $V \rtimes H = \langle X \rangle$, then H is generated by the elements $x^\bullet := [h,x][h,x]^{h^2} \cdots [h,x]^{h^{2m}} x^{-1}$, $x \in X$. Moreover, $x^\bullet = ([h,x]h^{-2})^{m+1}(-h)x^{-1}$.*

Proof. Let $h' := -h$, of order dividing $2m+1$. Then $h'-1$ is invertible, so from $0 = (h'-1)\sum_0^{2m} h'^i$ we obtain $0 = \sum_0^{2m} h'^i$. If $x = sv \in HV$ with $s \in H, v \in V$,

then $[h,x] = h^{-1}h^{sv} = h^{-1}h^v = (v^{-1})^h v = v^{h'+1}$, so that

$$\begin{aligned} x^\bullet &= [h,x][h,x]^{h'^2}\cdots[h,x]^{h'^{2m}}x^{-1} \\ &= v^{1+h'}v^{(1+h')h'^2}\cdots v^{(1+h')h'^{2m}}x^{-1} = v^{0+h'^{2m+1}}x^{-1} = vx^{-1} = s^{-1}. \end{aligned}$$

Since $\langle x^\bullet\rangle \equiv \langle x\rangle \pmod V$, it follows that $H = \langle X^\bullet\rangle$.

For the last part, use the group-theoretic version of "Horner's Rule" [BKL, p. 512]: $x^\bullet = [h,x]\cdot h'^{-2}[h,x]h'^2\cdot h'^{-4}[h,x]h'^4\cdots h'^{-2m}[h,x]h'^{-2}\cdot h'^{2m+2}\cdot x^{-1}$ collapses to $([h,x]h^{-2})^{m+1}h'x^{-1}$. □

We now use the lemma to find L. Let $1 \neq z \in Z$. Define $C := \mathrm{C}_G(z) = QL$, where $Q := \mathrm{O}_2(C)$ and $L = \mathrm{C}_G(R)$ have yet to be found. A conjugate z' of z is opposite z (i. e., $|zz'|$ is odd) with probability $> 1/3$ [KM, Lemma 2.26]. Two random elements generate L with high probability since L is a simple group of Lie type [KL, LSh], so that three random elements of C generate C with high probability. Hence, we (probably) find C using (2.5).

There is a maximal torus $\langle h\rangle$ of R normalizing Z. Then h has order $q-1 > 1$ and is fixed point free on the elementary abelian 2-groups Q/Z and Z. In particular, $L = \mathrm{C}_C(h)$.

Random elements x_1, x_2, x_3 of $L\langle h\rangle Q$ generate $L\langle h\rangle Q \bmod \langle h\rangle Z$ with high probability. Lemma 4.3 with $V = Q/Z$ implies that $x_1^\bullet, x_2^\bullet, x_3^\bullet$ and $h^\bullet = h^{-1}$ (probably) generate $L\langle h\rangle Z \bmod Z$. Lemma 4.3 with $V = Z$ produces generators x_1', x_2', x_3', h of $L\langle h\rangle$. Here x_i' acts on Z as some element of $\langle h\rangle$ does. Find that element $h_i' \in \langle h\rangle$ using Section 2.2. Then we have found $L = \langle x_1'{h_1'}^{-1}, x_2'{h_2'}^{-1}, x_3'{h_3'}^{-1}\rangle$.

As in Section 3.1 we could have used derived subgroups [BCFLS] to obtain L from $x_1^\bullet$, $x_2^\bullet$ and $x_3^\bullet$, but the above seems simpler and possibly more efficient.

Remark 4.4. (1) In the lemma, h can be replaced by h^n for suitable integers n (such as -1 or 2), so that there are other words in h and x that evaluate to s^{-1}. Using suitable products of such words and their inverses produces infinitely many words that behave like $x^\bullet$ but do not appear to be "equivalent" to one another in any standard sense.

(2) While the preceding lemma is pleasantly independent of finiteness, in odd characteristic there is an even easier way to accomplish the same goal. *Assume that H is a group acting on a vector space V over a field of odd characteristic p. Let $h \in \mathrm{Z}(H)$ induce -1 on V. If $V{\rtimes}H = \langle X\rangle$, then $H = \langle [h,x]^{(p+1)/2}x^{-1} \mid x \in X\rangle$.* For, if $x = sv$ with $s \in H, v \in V$, then $[h,x] = h^{-1}h^v = v^{1-h} = v^2$, so that $[h,x]^{(p+1)/2}x^{-1} = s^{-1}$.

This ends our digression.

4.4. **Conclusion.** As in [KM, Sec. 2.13] (cf. Section 3.2 above), find constructive isomorphisms $\Psi_R : \hat{R} \to R$ and $\Psi_L : \hat{L} \to L$, and then T_0 (which is a maximally split torus of G in characteristic 2), the root system Φ, the root groups X_α, and Q. Using Section 2.2, as in Sections 3.3 and 3.4 we can now repeat the remainder of [KM, Sec. 2] in order to complete the proof.

5. Odd characteristic and rank 2

In this section we assume that G is a black box group in Theorem 1.1 of rank 2 over a field of odd order $q > 9$. We provide a simple reduction to [KM, Sec. 3]. Let $\epsilon = 1$ for $G_2(q)$ and 3 for ${}^3D_4(q)$.

Choose up to 40 elements $x \in G$ in order to find one of even order. Let t be the involution in $\langle x \rangle$.

Choose up to $4 \cdot 10^7$ pairs $g, h \in G$, and for each test whether $|tt^g|$ and $|tt^h|$ are odd, in which case let $C := \langle \tilde{g}, \tilde{h} \rangle \leq \mathrm{C}_G(t)$ (cf. (2.5)). For some g, h we will probably have $C \trianglerighteq R \circ L$ with R a long root $\mathrm{SL}(2,q)$ subgroup and L a short root $\mathrm{SL}(2,q^\epsilon)$ subgroup; find R and L as in [KS, Sec. 3.6.2]. Use the hypothesized oracles to obtain constructive isomorphisms $\Psi_R \colon \mathrm{SL}(2,q) \to R$ and $\Psi_L \colon \mathrm{SL}(2,q^\epsilon) \to L$.

Time: $O(\chi + \mu \log q)$.

Reliability: $> 1 - 1/2^9$. For, some x has even order with probability $> 1 - 1/2^{10}$ in view of [IKS, Thm. 5.2]. By [PW, Thm. 1], with probability $> (1/10^3)^2$ both $|tt^g|$ and $|tt^h|$ are odd, in which case C is as stated with probability $> (1/5)^2$ (as in [KS, Lemma 3.8]); and find R and L (and then also Ψ_R and Ψ_L) with probability $> 3/4$ [KS, Sec. 3.6.2]. Hence, none of the $4 \cdot 10^7$ choices for g, h produce R and L with probability $< (1 - \{(1/10^3)^2(1/5)^2(3/4)\})^{4 \cdot 10^7} < 1/2^{10}$, so that the procedure succeeds with probability $> 1 - 1/2^9$.

Given R, L, Ψ_R and Ψ_L, we can repeat [KM, Sec. 3] in order to complete the proof.

6. Characteristic 2 and rank 2

In this section we only consider the case $G \cong G_2(2^e)$, $e > 2$.

6.1. **Preliminaries.** Let $q \equiv \delta \equiv \delta' \pmod 3$, where $\delta = \pm 1$, and $\delta' \in \{1, 2\}$.

Lemma 6.1. *With probability $\geq 5/18$, an element $g \in G$ has order $3\mathrm{ppd}^\sharp(p; 3\delta' e)$. In that case the element of order 3 in $\langle g \rangle$ lies in a short root $\mathrm{SL}(2,q)$ subgroup.*

Proof. Let J be a long root $\mathrm{SL}^\delta(3,q)$ subgroup of G, so that $\mathrm{Z}(J) = \langle y \rangle$ has order 3 in view of $q \pmod 3$. Then $\mathrm{C}_G(y)$ contains a long root $\mathrm{SL}(2,q)$ subgroup whose centralizer is a short root $\mathrm{SL}(2,q)$ subgroup containing y. Thus, G contains elements g of the required sort.

The probability of choosing an element g of the stated order is at least $(1/3)(1 - 1/6)$ (as in [KM, Lemma 2.24]). Moreover, in that case, by Sylow's Theorem g lies in a conjugate J_1 of J and $\mathrm{C}_{J_1}(g)$ is a maximal torus of both G and J_1. In particular, $\mathrm{Z}(J_1) \leq \langle g \rangle$ and $\mathrm{Z}(J_1)$ is conjugate to $\mathrm{Z}(J)$. Then $\mathrm{Z}(J_1)$ lies in a short root $\mathrm{SL}(2,q)$ subgroup. $\square$

Lemma 6.2. *With probability $> 1/10$, two different subgroups of order 3 each lying in a short root $\mathrm{SL}(2,q)$ subgroup both lie in such a subgroup.*

Proof. All such subgroups Y of order 3 are conjugate in G. We have seen that $\mathrm{C}_G(Y)$ is a long root $\mathrm{SL}^\delta(3,q)$ subgroup and Y lies in a short root $\mathrm{SL}(2,q)$ subgroup D. There are $a := |G \colon \mathrm{SL}^\delta(3,q) \cdot 2| \left(|G \colon \mathrm{SL}^\delta(3,q) \cdot 2| - 1 \right)$ ordered pairs of distinct conjugates of Y, and $b := |G \colon \mathrm{N}_G(D)| \cdot \frac{1}{2} q(q+\delta) \left(\frac{1}{2} q(q+\delta) - 1 \right)$ such pairs lying in conjugates of D. (Here $\mathrm{N}_G(D) \cong \mathrm{SL}(2,q) \times \mathrm{SL}(2,q)$.) Thus, two distinct conjugates of Y lie in a conjugate of D with probability $\geq b/a > 1/10$. (This is where the magic of G_2 is visible: there is no analogous result for ${}^3D_4$.)

We still need to verify that distinct Y, Y^g lie in at most one short root $\mathrm{SL}(2,q)$ subgroup. For otherwise, $\mathrm{C}_G(\langle Y, Y^g \rangle)$ contains distinct long root $\mathrm{SL}(2,q)$ subgroups R_1, R_2 that lie in $\mathrm{C}_G(\langle Y \rangle) = \mathrm{SL}^\delta(3,q)$. Then either $\langle R_1, R_2 \rangle = \mathrm{SL}^\delta(3,q)$ has center

$Y = Y^g$, or $\delta = +$ and $\langle R_1, R_2\rangle$ has the form $q^2\mathrm{SL}(2,q)$. Since $Y, Y^g < \mathrm{SL}(2,q)$, some conjugate $Y^{g'}$ satisfies $\langle Y, Y^{g'}\rangle \cong \mathrm{SL}(2,q')$ for some q'. Now $\mathrm{N}_G(\langle Y, Y^{g'}\rangle)$ has a subgroup $q^2\mathrm{SL}(2,q)\times\mathrm{SL}(2,q')$, and this must lie inside a parabolic subgroup of G. A parabolic subgroup containing $q^2\mathrm{SL}(2,q)$ has the shape $q^{2+3}\mathrm{GL}(2,q)$ and hence contains no subgroup $q^2\mathrm{SL}(2,q)\times\mathrm{SL}(2,q')$, producing the desired contradiction. □

6.2. **Algorithm.** Choose up to 36 elements $g \in G$ in order to find one of order $3\mathrm{ppd}^\sharp(p; 3\delta' e)$, in which case let y be an element of order 3 in $\langle g\rangle$. Choose up to 100 conjugates $y' \neq y^{\pm 1}$ of y, and for each test whether $t := [y', y'^y]$ or $(y'y'^y)^m y'$ is an involution, where $2m+1 = q^2-1$ [KK, Prop. 4]. Then t is a long root element or G.

Choose up to 10^8 pairs $g, h \in G$, and for each test whether $|tt^g|$ and $|tt^h|$ are both odd, in which case let $C := \langle \tilde{g}, \tilde{h}\rangle \leq \mathrm{C}_G(t)$ (cf. (2.5)); this is probably of the form $R\times X$, with X the short root group containing t and R a long root $\mathrm{SL}(2,q)$ subgroup. Find R (e.g., using ppds as in Lemma 3.1, or the fact that $R = \langle \tilde{g}^2, \tilde{h}^2\rangle$ with very high probability). Find a constructive isomorphism $\Psi_R \colon \hat{R} \to R$ using [KK].

Find a long root group Z of R and hence of G. Let $1 \neq z \in Z$.

As above, find $\mathrm{C}_G(z)$ (testing the same 10^8 pairs $g, h \in G$), which has the form $Z \times L$ for a short root $\mathrm{SL}(2,q)$ subgroup L; and then find L and a constructive isomorphism $\Psi_L \colon \hat{L} \to L$.

Time: $O(\xi + \chi)$, with $\chi = \mu \log^3 q \log\log q$ by [KK].

Reliability: $> 1 - 1/2^8$ using Lemmas 6.1 and 6.2 and imitating Section 5.

As in Section 5, we can now repeat the remainder of [KM, Sec. 3] in order to complete the proof.

Acknowledgement: We are grateful to Rob Wilson for helpful conversations at the start of this research.

References

[AB] C. Altseimer and A. V. Borovik, Probabilistic recognition of orthogonal and symplectic groups, pp. 1–20 in: Groups and Computation III (eds. W. M. Kantor and Á. Seress), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001.

[Ba] L. Babai, Local expansion of vertex-transitive graphs and random generation in finite groups, pp. 164–174 in: Proc. 1991 ACM Symp. on Theory of Computing.

[BBS] L. Babai, R. Beals and À. Seress, Polynomial-time theory of matrix groups, pp. 55–64 in: Proceedings of the 2009 ACM International Symposium on Theory of Computing. ACM, New York 2009.

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

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

[BKL] L. Babai, W. M. Kantor and A. Lubotzky, Small diameter Cayley graphs for finite simple groups. European J. Combinatorics 10 (1989) 507–522.

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

[Bo] 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, AMS, Providence 2002.

[BY] A. Borovik and S. Yalçinkaya, Fifty shades of black (preprint) arXiv:1308.2487v1.

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

[Br1] P. A. Brooksbank, Constructive recognition of classical groups in their natural representation. J. Symbolic Computation 35 (2003) 195–239.

[Br2] P. A. Brooksbank, Fast constructive recognition of black box unitary groups. LMS J. Comput. Math. 6 (2003) 162–197.

[Br3] P. A. Brooksbank, Fast constructive recognition of black box symplectic groups. J. Algebra 320 (2008) 885–909.

[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.

[BrK2] P. A. Brooksbank and W. M. Kantor, Fast constructive recognition of black box orthogonal groups. J. Algebra 300 (2006) 256–288.

[Ca] R. W. Carter, Simple groups of Lie type. Wiley, London–New York–Sydney 1972.

[CLG] 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.

[Di] J. D. Dixon, Generating random elements in finite groups. Electronic J. Combinatorics 13 (2008), ♯R94.

[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. AMS, Providence 1998.

[HM1] G. Hiss and G. Malle, Low-dimensional representations of quasi-simple groups. LMS J. Comput. Math. 4 (2001) 22–63.

[HM2] G. Hiss and G. Malle, Corrigenda: "Low-dimensional representations of quasi-simple groups". LMS J. Comput. Math. 5 (2002) 95–126.

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

[KK] W. M. Kantor and M. Kassabov, Black box groups isomorphic to $\mathrm{PGL}(2,2^e)$ (to appear in J. Algebra).

[Ka1] W. M. Kantor, Some topics in asymptotic group theory, pp. 403-421 in: Groups, Combinatorics and Geometry (eds. M. W. Liebeck and J. Saxl), LMS Lecture Notes 165, 1992.

[Ka2] W. M. Kantor, Simple groups in computational group theory, pp. 77–86 in: Proc. International Congress of Mathematicians, Vol. II, Documenta Math., Berlin 1998.

[KL] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group. Geom. Ded. 36 (1990) 67–87.

[KM] W. M. Kantor and K. Magaard, Black box exceptional groups of Lie type. TAMS 365 (2013) 4895–4931.

[KS] W. M. Kantor and Á. Seress, Black box classical groups. Mem. AMS 149 (2001), No. 708.

[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.

[LGO] C. R. Leedham–Green and E. A. O'Brien, Constructive recognition of $SL(2,q)$. TAMS 358 (2006) 1203–1221.

[LO] M. W. Liebeck and E. A. O'Brien, Recognition of finite exceptional groups of Lie type (preprint) arXiv:1310.2978v1.

[LSe] M. W. Liebeck and G. M. Seitz, Maximal subgroups of large rank in exceptional groups of Lie type. JLMS 71 (2005) 345–361.

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

[Lu] F. Lübeck, Small degree representations of finite Chevalley groups in defining characteristic. LMS J. Comput. Math. 4 (2001) 135–169.

[LMO] F. Lübeck, K. Magaard and E. A. O'Brien, Constructive recognition of $\mathrm{SL}(3,q)$. J. Algebra 316 (2007) 619–633.

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

[Se1] Á. Seress, Permutation group algorithms, Cambridge U. Press, Cambridge 2002.

[Se2] Á. Seress, A unified approach to computations with permutation and matrix groups, pp. 245–258, in: Proc. International Congress of Mathematicians, Vol. II, Eur. Math. Soc., Zürich 2006.

University of Oregon, Eugene, OR 97403 and Northeastern University, Boston, MA 02115
E-mail address: kantor@uoregon.edu

University of Birmingham, Edgbaston, Birmingham B15 2TT
E-mail address: k.magaard@bham.ac.uk