STEINBERG PRESENTATIONS OF BLACK BOX CLASSICAL GROUPS IN SMALL CHARACTERISTICS

ALEXANDRE BOROVIK AND ŞÜKRÜ YALÇINKAYA

Abstract. The main component of (constructive) recognition algorithms for black box groups of Lie type in computational group theory is the construction of unipotent elements. In the existing algorithms unipotent elements are found by random search and therefore the running time of these algorithms is polynomial in the underlying field size q which makes them unfeasible for most practical applications [27]. Meanwhile, the input size of recognition algorithms involves only $\log q$. The present paper introduces a new approach to construction of unipotent elements in which the running time of the algorithm is quadratic in characteristic p of the underlying field and is polynomial in $\log q$; for small values of p (which make a vast and practically important class of problems), the complexity of these algorithms is polynomial in the input size.

For $\mathrm{PSL}_2(q)$, $q \equiv 1 \bmod 4$, we present a Monte-Carlo algorithm which constructs a root subgroup U, the maximal torus T normalizing U and a Weyl group element w which conjugates U to its opposite. Moreover, we extend this result and construct Steinberg generators for the black box untwisted classical groups defined over a field of odd size $q = p^k$ where $q \equiv 1 \bmod 4$. Our algorithms run in time quadratic in characteristic p of the underlying field and polynomial in $\log q$ and the Lie rank n of the group.

The case $q \equiv -1 \bmod 4$ requires the use of additional tools and is treated separately in our next paper [9]. Further, and much stronger results can be found in [6, 7].

1. Introduction and the principal results

1.1. **Black box groups.** The purpose of the present paper is to introduce an efficient algorithm which constructs the so-called Steinberg generators of black box classical groups in small odd characteristics; it will be used in subsequent papers [6, 7] for recovery of the structure of these groups.

Black box groups were introduced by Babai and Szemeredi [3] as an idealized setting for randomized algorithms for solving permutation and matrix group problems in computational group theory.

A black box group X is a black box (or an oracle, or a device, or an algorithm) operating with 0-1 strings of bounded length which encrypt (not necessarily in a unique way) elements of some finite group G (in various classes of black box problems the isomorphism type of G could be known in advance or unknown). The functionality of the black box is specified by the following axioms: the black box

BB1 produces strings encrypting random elements from G;

2000 *Mathematics Subject Classification.* Primary 20D06; Secondary 20P05.

BB2 computes a string encrypting the product of two group elements given by strings or a string encrypting the inverse of an element given by a string; and

BB3 compares whether two strings encrypt the same element in G—therefore we have a canonical map (not necessarily easily computable in practice) $\pi : X \to G$.

We shall say in this situation that X is a *black box over* G or that X *encrypts* G.

A typical example is provided by a group G generated in a big matrix group $\mathrm{GL}_n(r^k)$ by several matrices $g_1, \dots, g_l$. The product replacement algorithm [20] produces a sample of (almost) independent elements from a distribution on G which is close to the uniform distribution (see the discussion and further development in [1, 2, 11, 23, 32, 34, 36, 35, 37]). We can, of course, multiply, invert, compare matrices. Therefore the computer routines for these operations together with the sampling of the product replacement algorithm run on the tuple of generators $(g_1, \dots, g_l)$ can be viewed as a black box X encrypting the group G. The group G could be unknown—in which case we are interested in its isomorphism type—or it could be known, as it happens in a variety of other black box problems. For example, if we already know that G is isomorphic to, say, $\mathrm{SL}_{2m}(r^s)$, we may wish to construct in G subgroups $H_1 \cong \mathrm{Sp}_{2m}(r^s)$, $H_2 \cong \mathrm{SL}_{2m}(r)$ and $H_3 \cong \mathrm{Sp}_{2m}(r)$ in such a way that $H_1 \cap H_2 = H_3$. (This problem is actually solved in one of the subsequent papers in this series [9].) In our set-up, this means that we wish to construct black boxes Y_i, $i = 1, 2, 3$, over H_i and embeddings $Y_i \to X$. This formalism is further developed in [7, 8].

Notice that even in routine examples the number of elements of a matrix group G could be astronomical, thus making many natural questions about the black box X over G—for example, finding the isomorphism type or the order of G—inaccessible for all known deterministic methods. Even when G is cyclic and thus is characterized by its order, existing approaches to finding multiplicative orders of matrices over finite fields are conditional and involve oracles either for the discrete logarithm problem in finite fields or for prime factorization of integers.

Nevertheless black box problems for matrix groups have a feature which makes them more accessible:

BB4 We are given a *global exponent* of X, that is, a natural number E such that it is expected that $x^E = 1$ for all elements $x \in X$ while computation of x^E is computationally feasible.

Usually, for a black box group X arising from a subgroup in the ambient group $\mathrm{GL}_n(r^k)$, the exponent of $\mathrm{GL}_n(r^k)$ can be taken for a global exponent of X.

Abusing terminology, in this paper we shall frequently identify the black box X and the group G encrypted by X (as we have already done in formulation of Axiom BB4); this is relatively safe in simpler black box problems about matrix groups over finite fields. However, more sophisticated algorithms which we shall discuss in subsequent papers will require a certain level of hygiene which will make identification of black box groups with the groups which they encrypt inconvenient.

In this paper, we assume that all our black box groups satisfy assumptions BB1–BB4.

We emphasise that we do not assume that black box groups under consideration in this paper are given as subgroups of ambient matrix groups; thus our approach is wider than that of the computational matrix group project [30]. This makes us to be a more careful with basic terminology. In particular, given two black boxes X, Y encrypting groups G, H, correspondingly, we say that a map α which assigns strings from X to strings from Y is a morphism of black box groups, if there is a homomorphism $\beta : G \to H$ such that the following diagram is commutative:

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ \vdots\pi_X & & \vdots\pi_Y \\ \downarrow & & \downarrow \\ G & \xrightarrow{\beta} & H \end{array}$$

(here π_X and π_Y are canonical projections of X and Y onto G and H, correspondingly).

1.2. **Black box group problems.** We shall outline an hierarchy of typical black box group problems.

Verification Problem: Is the unknown group encrypted by a black box group X isomorphic to the given group G ("target group")?

Recognition Problem: Determine the isomorphism class of the group encrypted by X.

The Verification Problem frequently arises as a sub-problem within more complicated Recognition Problems. The two problems have dramatically different complexity. For example, the celebrated Miller-Rabin algorithm [39] for testing primality of the given odd natural number n in nothing else but a black box algorithm for solving the verification problem for the multiplicative group $\mathbb{Z}/n\mathbb{Z}^*$ of residues modulo n (given by a simple black box: take your favorite random numbers generator and generate random integers between 1 and n) and the cyclic group $\mathbb{Z}/(n-1)\mathbb{Z}$ of order $n-1$ as the target group. On the other hand, if $n = pq$ is the product of primes p and q, the recognition problem for the same black box group means finding the direct product decomposition

$$\mathbb{Z}/n\mathbb{Z}^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z}$$

which is equivalent to factorization of n into product of primes.

The next step after finding the isomorphism type of the black box group X is

Constructive Recognition: Suppose that a black box group X encrypts a concrete and explicitly given group G. Rewording a definition given in [15],

> The goal of a constructive recognition algorithm is to construct an effective isomorphism $\Psi : G \longrightarrow X$. That is, given $g \in G$, there is an efficient procedure to construct a string $\Psi(g)$ representing g in X and given a string x produced by X, there is an efficient procedure to construct the element $\Psi^{-1}(x) \in G$ represented by X.

However, there are still no really efficient constructive recognition algorithms for black box groups X of (known) Lie type over a finite field of large order $q = p^k$. The first computational obstacles for known algorithms [16, 13, 14, 17, 15, 19, 22, 31] are the need to construct unipotent elements in black box groups, [16, 13, 14, 17, 15, 19] or to solve discrete logarithm problem for matrix groups [21, 22, 31].

Unfortunately, the proportion of the unipotent elements in X is $O(1/q)$ [27]. Moreover the probability that the order of a random element is divisible by p is also $O(1/q)$, so one has to make $O(q)$ (that is, *exponentially many*, in terms of the input length $O(\log q)$ of the black boxes and the algorithms) random selections of elements in a given group to construct a unipotent element. However, this brute force approach is still working for small values of q, and Kantor and Seress [29] used it to develop an algorithm for recognition of black box classical groups. Later the algorithms of [29] were upgraded to polynomial time constructive recognition algorithms [14, 16, 17, 15] by assuming the availability of additional *oracles*:

- the *discrete logarithm oracle* in $\mathbb{F}_q^*$, and
- the $\mathrm{SL}_2(q)$-*oracle*.

The latter is a procedure for the constructive recognition of $\mathrm{SL}_2(q)$; see discussion in [15, Section 3].

Structure recovery: Suppose that a black box group X encrypts a concrete and explicitly given group G. A weaker, but frequently feasible and very useful version of constructive recognition is what we call *structure recovery*: construction of a probabilistic polynomial time morphism

$$\Psi : G \longrightarrow X.$$

That is, given $g \in G$, there is an efficient procedure to construct a string $\Psi(g)$ representing g in X—but we do not require that the map Ψ can be efficiently reversed.

Structure recovery of black box groups encrypting Chevalley groups in odd characteristic is the principal aim of papers [6, 7, 9, 10], the present paper prepares some scaffoldings for this work. A more detailed discussion of methodological issues could be found in [7, 8].

1.3. **Results of the paper.** This paper is the first in the series of works [6, 7, 8, 9, 10] directed at development of polynomial time methods of computing in black box groups without seeking help from any kind of oracles.

As we have already mentioned, for sake of compactness of exposition in this paper we do not make a notational distinction between a black box and the group encrypted by it. However, in view of the use of results of this paper in subsequent work we carefully underly this distinction in the statements of results.

As the first step, we find unipotent elements in black box groups of Lie type of small odd characteristic.

Theorem 1.1. *Let X be a black box group encrypting a quasi-simple group of Lie type of odd characteristic p over a field of size $q = p^k > 3$. If $p \neq 5$ or 7, then there exists a Las Vegas algorithm which constructs a string representing a unipotent element. This algorithm works in time polynomial in the Lie rank n of X and $\log q$, and is quadratic in p.*

The same result holds if $p = 5$ or 7 and k has a small divisor l, with the algorithm running in time polynomial in n and $\log q$, and quadratic in p^l.

Then we extend this result to present an algorithm that constructs the Steinberg generators of the classical groups. The groups $(\mathrm{P})\mathrm{SL}_2(q)$ can be viewed as the starting point of recursion and we first present an algorithm for $(\mathrm{P})\mathrm{SL}_2(q)$.

We need to recall the notion of Steinberg generators of $(\mathrm{P})\mathrm{SL}_2(q)$ as introduced by Steinberg [40, Theorem 8].

Let $G = \mathrm{SL}_2(q)$. Then, for $t \in \mathbb{F}(q)$, set

$$u(t) = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}, v(t) = \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}, h(t) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, n(t) = \begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$$

where $t \neq 0$ for $h(t)$ and $n(t)$. It is straightforward to check that

$$u(t)^{n(s)} = v(-s^{-2}t),\ u(1)^{h(t)} = u(-t^2) \text{ and } n(1)^{h(t)} = n(t^2). \tag{1}$$

Moreover,

$$n(t) = u(t)v(-t^{-1})u(t) \text{ and } h(t) = n(t)n(-1). \tag{2}$$

It is well-known that

$$G = \langle u(t), v(t) \mid t \in \mathbb{F}(q) \rangle,$$

see, for example, [18, Lemma 6.1.1]. Therefore, by (1) and (2),

$$G = \langle u(1), h(t), n(1) \mid t \in \mathbb{F}(q)^* \rangle;$$

notice that actually G is generated by three elements

$$G = \langle u(1), h(t), n(1) \rangle$$

where we can take for t an arbitrary primitive element of the field $\mathbb{F}_q$.

We prove the following.

Theorem 1.2. *Let X be a black box group encrypting $(\mathrm{P})\mathrm{SL}_2(q)$, where $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. Then there is a Monte-Carlo algorithm which constructs in X strings u, h, n such that there exists an isomorphism*

$$\Phi : X \longrightarrow (\mathrm{P})\mathrm{SL}_2(q)$$

with

$$\Phi(u) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \Phi(h) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \Phi(n) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

where t is some primitive element of the field $\mathbb{F}_q$.

The running time of the algorithm is $O(\xi(\log\log q + p^2) + \mu(k \log\log q \log q + \log q + p^2 \log p))$ where μ be an upper bound on the time requirement for each group operation in X and ξ an upper bound on the time requirement, per element, for the construction of random elements of X.

Theorem 1.2 deserves some discussion and comparison with the $\mathrm{SL}_2(q)$-oracle as described in [15, Section 3].

Notice that $\Phi(u)$, $\Phi(h)$, and $\Phi(n)$ are some Steinberg generators of $(\mathrm{P})\mathrm{SL}_2(q)$. However, not being oracles we do not have an efficient procedure for computing isomorphism Φ, but we exhibit its inverse Φ^{-1} in our next paper [7].

Still, Theorem 1.2 provides sufficient structural information about X to facilitate solution of a wide range of natural problems about $(\mathrm{P})\mathrm{SL}_2(q)$ and other black box groups of Lie type and odd characteristic; a detailed discussion of applications of Theorems 1.2 and its easy corollary, Theorem 1.3 below, can be found in our next paper [9].

Theorem 1.3. *Let X be a black box group encrypting the group $G \cong (\mathrm{P})\mathrm{SL}_2(q)$, where $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. Then there is a Monte-Carlo algorithm which constructs a triple (U, T, w) in X where U is (a black box for) a root subgroup in G, T is (a black box for) a maximal torus in G normalizing U and w is a representative in $N_X(T)$ of a Weyl group element in G which conjugates U to its opposite root subgroup.*

The running time of the algorithm is $O(\xi(\log\log q + p^2) + \mu(k \log\log q \log q + \log q + p^2 \log p))$.

The formulation of Theorem 1.3 reflects another aspect of our approach to black box groups: we prefer to manipulate with subgroups (defined in X by their own smaller black "subboxes") rather than with individual elements.

In our next result, we expand Theorem 1.3 to construction of Steinberg generators in the Curtis-Tits configurations of classical groups (for discussion of the latter, see Sections 2.2 and 2.3). We prove the following.

Theorem 1.4. *Let X be a black box classical group encrypting one of the groups* $(\mathrm{P})\mathrm{SL}_{n+1}(q)$, $(\mathrm{P})\mathrm{Sp}_{2n}(q)$, $\Omega_{2n+1}(q)$ *or* $(\mathrm{P})\Omega^+_{2n}(q)$, *where* $q \equiv 1 \bmod 4$ *and* $q > 5$. *Then there is an algorithm which constructs:*

- *black boxes for an extended Curtis-Tits configuration* $\{K_0, K_1, \dots, K_n\}$ *of* X;
- *black boxes for root subgroups* $U_\ell < K_\ell$;
- *a black box for a maximal torus* T *where* $T < N_X(U_\ell)$;
- *Weyl group elements* $w_\ell \in K_\ell$, *where* $U_\ell^{w_\ell}$ *is the opposite root subgroup of* U_ℓ *in* K_ℓ *for all* $\ell = 0, 1, \dots, n$.

The running time of the algorithm is quadratic in the characteristic p of the underlying field, and is polynomial in the Lie rank n of X and $\log q$.

The two families of classical groups, $(\mathrm{P})\mathrm{SU}_n(q)$ and $(\mathrm{P})\Omega^-_{2n}(q)$, are not covered by Theorem 1.4. They are twisted Chevalley groups whose Curtis-Tits presentations are more complicated than these of Chevalley groups, see [25, Section 2.4], and work within these groups requires additional technical tools. However, we know how to develop algorithms for $(\mathrm{P})\mathrm{SU}_n(q)$ and $(\mathrm{P})\Omega^-_{2n}(q)$ similar to those described in this paper, they will be published elsewhere. The corresponding algorithms for exceptional groups will be presented in our next paper [10].

Theorem 1.4 will be used in the subsequent paper [6] to prove a more precise result:

Theorem 1.5. *Let X be a black box classical group encrypting one of the groups* $G \simeq (\mathrm{P})\mathrm{SL}_{n+1}(q)$, $(\mathrm{P})\mathrm{Sp}_{2n}(q)$, $\Omega_{2n+1}(q)$ *or* $(\mathrm{P})\Omega^+_{2n}(q)$, *where* $q \equiv 1 \bmod 4$ *and* $q > 5$. *Then there is a Monte-Carlo algorithm which constructs a polynomial time (in p and* $\log q$*) morphism*

$$\Phi : G \to X.$$

The running time of the algorithm is polynomial in the characteristic p of the underlying field, in the Lie rank n of X, and and in $\log q$.

1.4. **Construction of centralizers of involutions in black box groups.** Our algorithms are based on the construction of involutions and their centralizers in black box groups. In this subsection we summarize these constructions following [4], see also [12].

Let X be a black box group having an exponent $E = 2^k m$ with m odd. To produce an involution from a random element in X, we need an element x of even order. Then the last non-identity element in the sequence

$$1 \neq x^m, x^{m2}, x^{m2^2}, \dots, x^{m2^{k-1}}, x^{m2^k} = 1$$

is an involution and denoted by $\mathrm{i}(x)$. Note that the proportion of elements of even order in classical groups of odd characteristic is at least $1/4$ [28].

Let i be an involution in X. Then, by [4, Section 6], there is a partial map $\zeta = \zeta_0 \sqcup \zeta_1$ defined by

$$\begin{array}{rcl} \zeta : X & \longrightarrow & C_X(i) \\ x & \mapsto & \begin{cases} \zeta_1(x) = (ii^x)^{(m+1)/2} \cdot x^{-1} & \text{if } o(ii^x) \text{ is odd} \\ \zeta_0(x) = \mathrm{i}(ii^x) & \text{if } o(ii^x) \text{ is even.} \end{cases} \end{array}$$

Here $o(x)$ is the order of the element $x \in X$. Notice that, with a given exponent E, we can construct $\zeta_0(x)$ and $\zeta_1(x)$ without knowing the exact order of ii^x.

The following theorem is the main tool in the construction of centralizers of involutions in black-box groups.

Theorem 1.6. ([4]) *Let X be a finite group and $i \in X$ be an involution. If the elements $x \in X$ are uniformly distributed and independent in X, then*

(1) *the elements $\zeta_1(x)$ are uniformly distributed and independent in $C_X(i)$ and*
(2) *the elements $\zeta_0(x)$ form a normal subset of involutions in $C_X(i)$.*

By Theorem 1.6, we shall use the map ζ_1 to produce uniformly distributed random elements in $C_X(i)$. For an arbitrary involution $i \in X$ where X is a finite simple classical group, the proportion of elements of the form ii^g which have odd order is bounded from below by c/n where c is an absolute constant and n is the Lie rank of X [38]. For the classical involutions in classical groups, such a proportion is proved to be bounded from below by an absolute constant [41, Theorem 8.1].

1.5. **GAP code and experiments.** All algorithms described in this paper have been implemented in GAP [26] and thoroughly tested. It is worth noting that our methodology of building internal structure of a black box group block-by-block, in an organized and directed way, allows us to write (and write quickly!) clean, transparent, compact GAP codes; not surprisingly, de-bugging is also much easier than in the "elementwise" approach.

For the efficiency in practice we want to note that the algorithm in Theorem 1.2 for the group $\mathrm{SL}_2(7^{30})$ constructs the unipotent, toral and Weyl group elements in around 20 seconds in 2008 model standard MacBook.

1.6. **Notation.** The notation is standard and mostly follows [25]. In particular,

- (P)$\mathrm{SL}_n(q)$ denotes any group $\mathrm{SL}_n(q)/N$ where N is a subgroup of the center of $\mathrm{SL}_n(q)$, with similar conventions for the remaining classical groups. In particular, (P)$\mathrm{SL}_2(q)$ denotes one of the group $\mathrm{PSL}_2(q)$ or $\mathrm{SL}_2(q)$;
- $\frac{1}{(2,n)}\mathrm{SL}_n(q)$ denotes the factor groups of $\mathrm{SL}_n(q)$ by the subgroup of order $(2, n)$ from its center.
- The groups $\Omega_{2n+1}(q)$, $q > 3$, $n \geqslant 3$ are simple, so we drop (P) in the notation for these groups.

2. Backgrounds

2.1. **The Curtis-Tits Theorem.** The main identification theorem used in the classification of the finite simple groups is so called the Curtis-Tits Theorem which shows that the essential relations in the Steinberg presentation are the ones involving Lie rank 2 subgroups corresponding to fundamental roots in Π, that is, edges and non-edges in the Dynkin diagram.

Theorem 2.1. (Curtis–Tits, [24, Theorem 27.3]) *Let G^* be a finite group of Lie type. Let Σ be the root system of G^* and X_α ($\alpha \in \Sigma$) the corresponding root subgroups. Let Π be a fundamental system in Σ and for each $\alpha \in \Pi$ set*

$$G^*_\alpha = \langle X_\alpha, X_{-\alpha} \rangle.$$

Assume that $|\Pi| \geqslant 3$.

If now G is any group generated by subgroups G_α ($\alpha \in \Pi$), and if there are homomorphisms

$$\phi_\alpha : G^*_\alpha \longrightarrow G_\alpha$$

and

$$\phi_{\alpha\beta} : \langle G^*_\alpha, G^*_\beta \rangle \longrightarrow \langle G_\alpha, G_\beta \rangle$$

for all $\alpha, \beta \in \Pi$, which are coherent in the sense that $\phi_{\alpha\beta} = \phi_{\beta\alpha}$ and

$$\phi_{\alpha\beta} \mid_{G^*_\alpha} = \phi_\alpha$$

for all α and β in Π, then $G/Z(G)$ is a homomorphic image of $G^*/Z(G^*)$.

The system of subgroups $\{G_\alpha \mid \alpha \in \Pi\}$ which satisfies conditions of Theorem 2.1 is usually called a *Curtis-Tits system* of the groups G.

2.2. **A Curtis-Tits configuration, the single bonds case.** In this series of papers [5, 6, 8, 9, 10, 41], we move beyond identification of a simple black box group to creation of tools for computing within these groups. For that purpose, we will use a modified concept of a Curtis-Tits system, more suitable for pin-pointing the internal structure of the given black box group X.

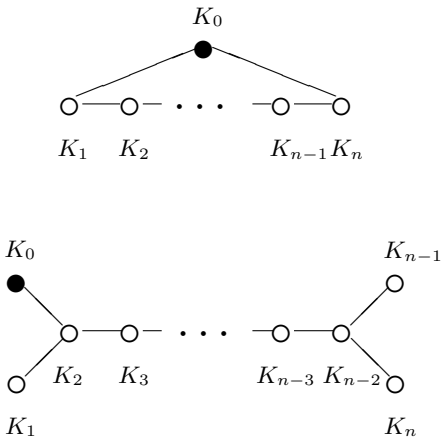


FIGURE 1. Extended Dynkin diagrams (and Curtis-Tits systems) of types A_n and D_n

Let Φ be an irreducible root system of rank at least 3 with fundamental system Π and with Dynkin diagram Δ of one of the types A_n for $n \geqslant 2$, D_n for $n \geqslant 3$, E_6, E_7, or E_8. Let $\Pi^* = \Pi \cup \{-\alpha_0\}$ where α_0 is the highest root in Π and Δ^* be the extended Dynkin diagram for Π^*.

Given a black box group X of type Δ over a finite field of odd prime power order $p^k = q > 3$, we have constructed in X [5] a *Curtis-Tits configuration*, that

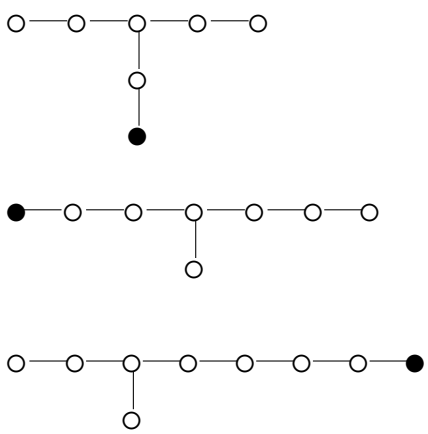


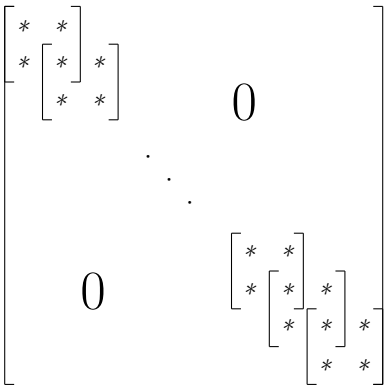
FIGURE 2. Extended Dynkin diagrams (and Curtis-Tits systems) of types E_6, E_7 and E_8

is, a system of subgroups $K_\alpha \cong \mathrm{SL}_2(q)$ labeled by nodes of Δ^* and satisfying the following conditions:

(a) $X = \langle K_\alpha \mid \alpha \in \Delta \rangle$;
(b) $[K_\alpha, K_\beta] = 1$ if α and β are not connected in Δ^*;
(c) $\langle K_\alpha, K_\beta \rangle \cong \mathrm{SL}_3(q)$ if α and β are connected with a single bond;
(d) if z_α is the involution in the center of K_α then $[z_\alpha, z_\beta] = 1$ for all $\alpha, \beta \in \Delta^*$;
(e) if we form the elementary abelian group $E = \langle z_\alpha \mid \alpha \in \Delta^* \rangle$, then $H = C_X(E)$ is an abelian p'-group;
(f) for all $\alpha \in \Delta^*$, the group $H_\alpha = H \cap K_\alpha$ is a maximal split torus in K_α and $\langle H_\alpha \mid \alpha \in \Delta \rangle = H$;
(g) the subgroup H normalizes each subgroup K_α for $\alpha \in \Delta^*$.

Definition 2.2. *The indexed set of subgroups* $\{K_\alpha \mid \alpha \in \Delta\}$ *which satisfies the conditions* (a)–(g) *above is called a* (single bond) Curtis-Tits configuration. *Similarly,* $\{K_\alpha \mid \alpha \in \Delta^*\}$ *is called a* (single bond) extended Curtis-Tits configuration *for* X.

Example 2.3. *The following* $n-1$ *subgroups* $\mathrm{SL}_2(q)$ *form a Curtis-Tits configuration in* $G = \mathrm{SL}_n(q)$.



The following result is an immediate consequence of [24, Corollary 27.4], which is, in its turn, a special case of Theorem 2.1.

Theorem 2.4. *Let G be a finite group with a single bond Curtis-Tits configuration $\{G_\alpha\}$ over a field of odd order $q > 5$ corresponding to one of the Dynkin diagrams A_n, $n \geqslant 2$, D_n, $n \geqslant 3$, E_6, E_7, or E_8. Then G is isomorphic to a quasi-simple group of Lie type over $\mathbb{F}(q)$ of the corresponding type and $\{G_\alpha\}$ is the system of root SL_2-subgroups for roots in a system of simple roots Π associated with some maximal split torus H of G.*

2.3. **A Curtis-Tits configuration for double bond Dynkin diagrams of rank at least 3.** Let now Δ^* be an extended Dynkin diagram of one of the types B_n or C_n for $n \geqslant 3$, see Figure 3; notice that the labelling of the nodes is chosen so that the nodes $1, 2, \ldots, n$ form the corresponding Dynkin diagram and the nodes $n-1$ and n are connected by a double bond.

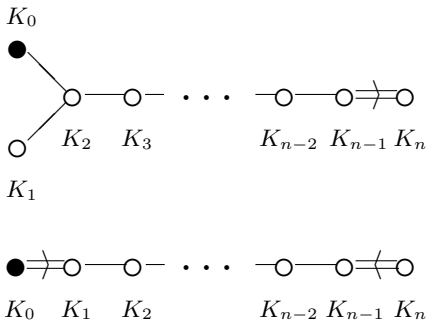


FIGURE 3. Extended Dynkin diagrams of type B_n and C_n

Given a black box group X of type B_n or C_n over a finite field of odd prime power order $p^k = q > 5$, *Curtis-Tits configuration*, that is, a system of subgroups $K_\alpha \cong (\mathrm{P})\mathrm{SL}_2(q)$ labeled by nodes of Δ^* and satisfying the following conditions:

(a) $X = \langle K_\alpha \mid \alpha \in \Delta \rangle$;
(b) $[K_\alpha, K_\beta] = 1$ if α and β are not connected in Δ^*;
(c) – $\langle K_\alpha, K_\beta \rangle \cong \mathrm{SL}_3(q)$ if α and β are connected with a single bond;
– $\langle K_\alpha, K_\beta \rangle \cong (\mathrm{P})\mathrm{Sp}_4(q)$ if α and β are connected with a double bond;
(d) if z_α and z_β are involution in the centers of $K_\alpha \cong K_\beta \cong \mathrm{SL}_2(q)$ then $[z_\alpha, z_\beta] = 1$. Moreover, there exits an element $t \in X$ of order $(q-1)/2$ such that $\langle K_1, \ldots, K_{n-1} \rangle \leq C_X(t)$ and $[z_0, t] = [z_n, t] = 1$.
(e) if we form the abelian group

$$E = \langle z_\alpha, t \mid \alpha \in \Delta^* \text{ and } K_\alpha \cong \mathrm{SL}_2(q) \rangle,$$

then $H = C_X(E)$ is an abelian p'-group.
(f) for all $\alpha \in \Delta^*$, the group $H_\alpha = H \cap K_\alpha$ is a maximal split torus in K_α and $\langle H_\alpha \mid \alpha \in \Delta \rangle = H$;
(g) the subgroup H normalizes each subgroup K_α for $\alpha \in \Delta^*$.

Remark 2.5. From the algorithmic point of view, we shall note here that if $X \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$ and $q \equiv 1 \bmod 4$, then the element $t \in X$ of order $(q-1)/2$ in (d) above can be chosen to be an involution (or a pseudo-involution – an element of order 4 whose square is a central involution when X is not simple). The restriction $q > 5$ is imposed due to the following fact for the groups of type B_n. Note first that if $X \cong \Omega_{2n+1}(q)$, then $C = C_X(z_0, z_1, \ldots, z_{n-1})$ is a subgroup of order $\frac{(q-1)^n}{2}.2^n$, which is not abelian. Here, the subgroup of order 2^n arises from the graph automorphisms and the inversions in the corresponding centralizers of involutions. Therefore, if $q = 5$, then the element t becomes an involution since its order is $(5-1)/2 = 2$ and it centralizes the subgroup of order 2^n. We shall also note that such an element t corresponds to an involution of type t_n, that is, $C_X(t)$ has a semisimple component isomorphic to $\Omega^+_{2n}(q)$, and if $q > 5$, then $C_X(t)$ has a semisimple component isomorphic to $\mathrm{SL}_n(q)$. Thus, if $q = 5$ then $C = C_X(z_0, z_1, \ldots, z_{n-1}, t)$ is not a maximal split torus. However, in the case of groups of type B_n, the black box group algorithm for the construction of a Curtis-Tits configuration does not depend on such an element $t \in X$. We also note here that the Curtis-Tits configuration above for the groups $(\mathrm{P})\mathrm{Sp}_{2n}(5)$ also holds. For $q = 3$, however, the methods used in the construction of Curtis-Tits configurations in [5] do not work as $\mathrm{SL}_2(3)$ is solvable. Hence it is enough to assume that $q > 3$ for the algorithmic applications. We refer the reader to [5, Section 8] for the details about the construction of Curtis-Tits configurations in black box classical groups.

Similarly to Theorem 2.4, the following result is an easy consequence of Theorem 2.1.

Theorem 2.6. *Let G be a finite group with an extended double bond Curtis-Tits configuration $\{G_\alpha\}$ over a field of odd order $q > 5$ corresponding to one of the extended Dynkin diagrams B_n or C_n $(n \geqslant 3)$.*

Then G is isomorphic to a quasi-simple group of Lie type over $\mathbb{F}(q)$ of the corresponding type and $\{G_\alpha \mid \alpha \in \Delta\}$ is the system of root SL_2-subgroups for roots in a system of simple roots Π associated with some maximal split torus H of G.

Perhaps it is time to comment on subtle differences between the Curtis-Tits configurations in groups $(\mathrm{P})\mathrm{Sp}_{2n}$ of type C_n and in groups Ω_{2n+1} and Spin_{2n+1} of type B_n. Indeed some confusion could be created by the fact that $\mathrm{PSp}_4(q) \cong \Omega_5(q)$ and $\mathrm{Sp}_4(q) \cong \mathrm{Spin}_5(q)$. However the root $(\mathrm{P})\mathrm{SL}_2$-subgroups K_{n-1} and K_n in $\langle K_{n-1}, K_n\rangle \cong (\mathrm{P})\mathrm{Sp}_4(q)$ correspond to roots of different length, and therefore correspond to homomorphisms $\mathrm{SL}_2(q) \longrightarrow (\mathrm{P})\mathrm{Sp}_4(q)$ which are *not* conjugate in $\mathrm{Aut}\,(\mathrm{P})\mathrm{Sp}_4(q)$.

In particular,

- If $K_n \cong \mathrm{PSL}_2(q)$ then $\langle K_{n-1}, K_n\rangle \cong \mathrm{PSp}_4(q) \cong \Omega_5(q)$ and $G \cong \Omega_{2n+1}(q)$;
- if $K_n \cong \mathrm{SL}_2(q)$ then $\langle K_{n-1}, K_n\rangle \cong \mathrm{Sp}_4(q) \cong \mathrm{Spin}_5(q)$ and $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$ or $\mathrm{Spin}_{2n+1}(q)$; in that case, further information comes from the behaviour of the involution $z_n \in Z(K_n)$:
  - if $z_n \in Z(G)$ then $G \cong \mathrm{Spin}_{2n+1}(q)$;
  - if $z_n \notin Z(G)$ then $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$.

Actually the distinctions between the cases of PSp_{2n}, Sp_{2n}, Ω_{2n+1} and Spin_{2n+1} become clear at early stages of construction of an extended Curtis-Tits configuration [41, 5] and therefore any potential confusion is easily avoidable.

Indeed, before we start constructing Curtis-Tits system for a classical group, we construct a long root $\mathrm{SL}_2(q)$-subgroup K and check whether, for a random element $g \in G$, $\langle K, K^g\rangle$ is

- $\mathrm{SL}_4(q)$,
- $\mathrm{Sp}_4(q)$,
- $\mathrm{SU}_4(q)$, or
- $\mathrm{SO}_8^+(q)$.

This is the case with probability at least $1 - O(1/q)$ provided that the rank is big enough if G is $\mathrm{SL}_n(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{SU}_n(q)$ or an orthogonal group, respectively. This is Theorem 7.1 in [5], and Theorem 7.2 of the same paper presents an algorithm which computes the type of the group (not distinguishing the groups of type B_n and D_n). The differences between $\mathrm{Sp}_{2n}(q)$ and $\mathrm{PSp}_{2n}(q)$, and $\Omega_{2n+1}(q)$ and $\mathrm{Spin}_{2n+1}(q)$ is quite clear as one of them has a central involution and the other does not have such an involution.

3. Steinberg generators of $(\mathrm{P})\mathrm{SL}_2(q)$

Let $G \cong \mathrm{PSL}_2(q)$ and $q \equiv 1 \bmod 4$. In this section we construct, in G, a unipotent element u, a Weyl group element w which conjugates u to its opposite and the split torus $T < G$ which normalizes the root subgroup U containing u. Note that all of this construction can be done in $\mathrm{SL}_2(q)$ with obvious modifications in the arguments.

Remark 3.1. It is well-known that the non-trivial elements of $G \cong \mathrm{PSL}_2(q)$ are either semisimple or unipotent. Moreover, any non-trivial semisimple (or unipotent) element belongs to a unique maximal torus (or root subgroup).

Lemma 3.2. *Let $G \cong \mathrm{PSL}_2(q)$, $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. If $i \in G$ is an involution, then there exists $g \in G$ such that ii^g has order p.*

Proof. Since $q \equiv 1 \bmod 4$, any involution in G belongs to a torus of order $(q-1)/2$. Assume that $i \in T$ for some torus $T < G$. By Remark 3.1, T is uniquely determined by the involution i. Moreover, there are exactly two Borel subgroups B_1 and B_2

which contain T. If $B_1 = T \ltimes U$ and $B_2 = T \ltimes V$, then U and V are opposite unipotent subgroups of G. Now observe that $u^i = u^{-1}$ for any $u \in U$ (or $u \in V$), which implies that the element ii^u has order p and the lemma follows. □

Lemma 3.3. *Let $G \cong \mathrm{PSL}_2(q)$, $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. For any involution $i \in G$, the probability that ii^g has order p for a random element $g \in G$ is at least $1/q$.*

Proof. Normalizers of unipotent subgroups of order q in G are Borel subgroups, and it is well known that any two distinct Borel subgroups intersect over a maximal torus of order $(q-1)/2$. Since $q \equiv 1 \bmod 4$, this torus contains an involution, uniquely determined by this involution and normalizes exactly two unipotent subgroups of order q—see proof of Lemma 3.2. Hence there are only two unipotent subgroups U, V of order q which are normalized by i.

Unipotent subgroups U and V are also normalized by the torus T containing i, and are the opposite unipotent subgroups of each other in the sense of the root system associated with the torus T. Since $C_G(U) = U$, all involutions of the form i^g, $g \in G$, which invert U lie in the coset Ui. By considering the opposite unipotent subgroup V, we have $2(q-1)$ involutions of the form i^g, $g \in G$, such that ii^g is an element of order p. Since $|G| = q(q^2-1)/2$, the proportion of the elements $g \in G$ such that ii^g is of order p is

$$\frac{2(q-1)}{q(q^2-1)/2} \cdot (q-1) = \frac{4(q-1)}{q(q+1)} > \frac{1}{q}.$$

□

Lemma 3.4. *Let $G \cong \mathrm{PSL}_2(q)$ and $q \equiv 1 \bmod 4$. Assume that $i \in G$ is an involution and $u = ii^g$ is a unipotent element for some $g \in G$. If $i \in T$ for some torus T and U is a root subgroup containing u, then $T < N_G(U)$.*

Proof. Since $u^i = u^{-1}$, we have $i \in N_G(\langle u \rangle)$. Moreover, since $N_G(U)$ contains a torus and $i \in T$, by Remark 3.1, we have $T < N_G(U)$ and the lemma follows. □

Lemma 3.5. *Let $G \cong \mathrm{PSL}_2(q)$ and $U < G$ be the root subgroup containing a unipotent element $u \in G$. Assume also that $T = \langle t \rangle$ is a maximal torus in $N_G(U)$. Then $\langle u, t \rangle = N_G(U)$. In particular, U is the derived subgroup of $\langle u, t \rangle$.*

Proof. It is well-known that U is a minimal normal subgroup of $N_G(U) = TU$. Hence the lemma follows. □

Remark 3.6. Let $G \cong \mathrm{PSL}_2(q)$ and $q \equiv 1 \bmod 4$. Let T be a torus of order $(q-1)/2$ containing an involution i. Then $C_G(i) = T \rtimes \langle j \rangle$ where $t^j = t^{-1}$ for all $t \in T$. Observe that if U is a root subgroup normalized by T, then U^j is the opposite root subgroup of U in G, that is, $G = \langle U, U^j \rangle$, see [18, Lemma 6.1.1 and 7.2.1]. We will call the element j a *Weyl group element*.

It is well-known that any two maximal tori of fixed order in $\mathrm{PSL}_2(q)$ are conjugate. The following lemma will be used to find a conjugating element for a given two tori of order $(q-1)/2$ in $\mathrm{PSL}_2(q)$.

Lemma 3.7. *Let $G \cong \mathrm{PSL}_2(q)$ and $q \equiv 1 \bmod 4$. Assume that T_1, T_2 be two tori of order $(q-1)/2$ in G, and i_1, i_2 are the involutions in T_1, T_2, respectively. Assume also that $|i_1 i_2| = m$ is odd. Then $T_1^z = T_2$ where $z = (i_1 i_2)^{(m+1)/2}$.*

Proof. Assume first that $q > 5$. Let $D = \langle i_1, i_2 \rangle$, then D is a dihedral group of order $2m$ and $i_1^z = i_2$. Since $C_G(i_1) = T_1 \rtimes \langle j_1 \rangle$ and $C_G(i_2) = T_2 \rtimes \langle j_2 \rangle$ where j_1 and j_2 are involutions inverting T_1 and T_2, respectively, we have

$$T_2 \rtimes \langle j_2 \rangle = C_G(i_2) = C_G(i_1^z) = C_G(i_1)^z = T_1^z \rtimes \langle j_1 \rangle^z.$$

Since there is only one cyclic group of order $(q-1)/2$ in $T_2 \rtimes \langle j_2 \rangle$, we have $T_2 = T_1^z$. If $q = 5$, then $T_1 = \langle i_1 \rangle$ and $T_2 = \langle i_2 \rangle$. Therefore, $T_1^z = T_2$ and the lemma follows. □

4. An algorithm for $\mathrm{PSL}_2(q)$

Let $G \cong \mathrm{PSL}_2(q)$ and $t \in G$ be an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even. Let $s \in \langle t \rangle$ be an involution, $r \in G$ an involution which inverts t, and $x \in G$ an element of order 3 which normalizes $\langle s, r \rangle$. The subgroup $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4$ plays a crucial role in our algorithm. Observe that the preimage of the elements s and r in $\widetilde{G} \cong \mathrm{SL}_2(q)$ generate the quaternion group Q of order 8 so the preimage of $L = \langle s, r, x \rangle$ is a subgroup of $N_{\widetilde{G}}(Q)$.

Lemma 4.1. *Assume that $G \cong \mathrm{PSL}_2(q)$, $q = p^k$ for some $k \geqslant 2$ and $t \in G$ is an element of order $(p \pm 1)/2$ where $(p \pm 1)/2$ is even. Let $s \in \langle t \rangle$ be an involution, $r \in G$ an involution which inverts t, and $x \in G$ an element of order 3 which normalizes $\langle s, r \rangle$. Then, except for $p = 5, 7$, we have $\langle t, x \rangle \cong \mathrm{PSL}_2(p)$. Moreover, if a divides k and t is of order $(p^a \pm 1)/2$ where $(p^a \pm 1)/2$ is even, then $\langle t, x \rangle \cong \mathrm{PSL}_2(p^a)$.*

Proof. Let $L = \langle s, r, x \rangle \cong \mathrm{Alt}_4 \cong \mathrm{PSL}_2(3)$. Observe that L is a subgroup of some $H \leqslant G$ where $H \cong \mathrm{PSL}_2(p)$. Since $s = t^m$ for some $m \geqslant 1$, $t \in C_G(s)$ and t is contained in a torus T of order $(q \pm 1)/2$ in $C_G(s)$. Now $T \cap H$ has order $(p \pm 1)/2$. Since T is cyclic, it has only one subgroup of order $(p \pm 1)/2$ so $t \in H$. Thus $\langle t, x \rangle \leqslant H$. By the subgroup structure of $\mathrm{PSL}_2(p)$, the subgroup L is either a maximal subgroup of H or it is contained in $\mathrm{Sym}_4 \leqslant H$. Hence, if $|t| \geqslant 5$, or equivalently, $p \geqslant 9$ then we have $\langle t, x \rangle = H$ since L does not contain elements of order bigger than 5. As we noted above, if $p = 3$, then $L \cong \mathrm{Alt}_4 \cong \mathrm{PSL}_2(3)$.

Observe that if a divides k and $|t| = (p^a \pm 1)/2$, then t belongs to a subgroup $H \cong \mathrm{PSL}_2(p^a)$. Assuming that $(p^a \pm 1)/2$ is even, the lemma follows from the arguments above. □

Remark 4.2. Following the notation of Lemma 4.1, observe that if $p = 5$, then $s = t$, and if $p = 7$, then $|t| = 4$ and $\langle t, x \rangle = \mathrm{Sym}_4$. Therefore, in these cases, we have $\langle t, x \rangle \ncong \mathrm{PSL}_2(p)$. It is clear that if $G \cong \mathrm{SL}_2(q)$, then, by considering the pseudo-involutions (whose squares are the central involution in G), the same result in Lemma 4.1 holds. Note that, in this case, we consider the elements $t \in G$ of order $p \pm 1$ where $(p \pm 1)/2$ is even. Similarly, following the notation in Lemma 4.1, if $p = 5$ or 7, then $\langle t, x \rangle \ncong \mathrm{SL}_2(p)$.

The following lemma is concerned with the construction of the element of order 3 in $\mathrm{Alt}_4 \leqslant \mathrm{PSL}_2(q)$. Let $V = \{1, i_1, i_2, i_3\}$ be a subgroup of G isomorphic to Klein 4-group. For any random element $g \in G$, denote $j_\ell = i_\ell^g$ for $\ell = 1, 2, 3$.

Lemma 4.3. *Together with the setting above, assume that $t_1 = i_1 j_2$ has odd order m_1. Set $u_1 = t_1^{\frac{m_1+1}{2}}$ and $k = i_3^{gu_1^{-1}}$. Assume also that $t_2 = i_2 k$ has odd order m_2 and $u_2 = t_2^{\frac{m_2+1}{2}}$. Then the element $x = g u_1^{-1} u_2^{-1}$ permutes i_1, i_2, i_3. In particular, $x \in N_G(V) \leqslant \mathrm{Sym}_4$ and x has order 3.*

Proof. Observe first that $i_1^{u_1} = j_2$ and $i_2^{u_2} = k$. Then, since $k = i_3^{gu_1^{-1}}$, we have $i_2^{u_2} = i_3^{gu_1^{-1}}$. Hence $i_2 = i_3^{gu_1^{-1}u_2^{-1}} = i_3^x$. Now, we prove that $i_2^x = i_1$. Since $i_2^g = j_2$ and $j_2^{u_1^{-1}} = i_1$, we have $i_2^x = i_2^{gu_1^{-1}u_2^{-1}} = i_1^{u_2^{-1}}$. We claim that $t_2 \in C_G(i_1)$, which implies that $u_2 \in C_G(i_1)$, so $i_2^x = i_1^{u_2^{-1}} = i_1$. Now, since $i_2 \in C_G(i_1)$, $t_2 = i_2k \in C_G(i_1)$ if and only if $k = i_3^{gu_1^{-1}} \in C_G(i_1)$. Recall that $i_1^{u_1} = j_2$. Therefore $k \in C_G(i_1)$ if and only if $i_3^g \in C_G(j_2) = C_G(i_2^g)$, equivalently, $i_3 \in C_G(i_2)$ and the claim follows. It is now clear that $i_1^x = i_3$ since $i_1i_2 = i_3$. □

Lemma 4.4. *Let t_1 and t_2 be as in Lemma 4.3. Then the probability that t_1 and t_2 have odd orders is bounded from below by $1/2 - 1/2q$.*

Proof. Notice that all involutions in $G \cong \mathrm{PSL}_2(q)$ are conjugate. Therefore the probability that t_1 and t_2 have odd orders is the same as the probability of the product of two random involutions from G to be of odd order.

We denote by a one of these numbers $(q \pm 1)/2$ which is odd and by b the other one. Then $|G| = q(q^2-1)/2 = 2abq$ and $|C_G(i)| = 2b$ for any involution $i \in G$. Hence the total number of involutions is

$$\frac{|G|}{|C_G(i)|} = \frac{2abq}{2b} = aq.$$

Now we shall compute the number of pairs of involutions (i, j) such that their product ij belongs to a torus of order a. Let T be a torus of order a. Then $N_G(T)$ is a dihedral group of order $2a$. Therefore the involutions in $N_G(T)$ form the coset $N_G(T)\backslash T$ since a is odd. Hence, for every torus of order a, we have a^2 pairs of involutions whose product belong to T. The number of tori of order a is $|G|/|N_G(T)| = 2abq/2a = bq$. Hence, there are bqa^2 pairs of involutions whose product belong to a torus of order a. Thus the desired probability is

$$\frac{bqa^2}{(aq)^2} = \frac{b}{q} \geqslant \frac{q-1}{2q} = \frac{1}{2} - \frac{1}{2q}.$$

□

Remark 4.5. An important part of our algorithm is to find a generator of a torus T of order $(q\pm1)/2$ in $\mathrm{PSL}_2(q)$. However, since finding the exact order of an element involves factorization of integers into primes, we consider the elements $t \in T$ where the order of t is divisible by some primitive prime divisor of $(q \pm 1)/2$. On the other hand, by [33, I.8], the proportion of the elements of order $(q \pm 1)/2$ in T is $O(1/\log\log q)$.

A prime number r is said to be a primitive prime divisor of $p^k - 1$ if r divides $p^k - 1$ but not $p^i - 1$ for $1 \leqslant i < k$. By [43], there exists a primitive prime divisor of $p^k - 1$ except when $(p, k) = (2, 6)$, or $k = 2$ and p is a Mersenne prime. Observe that the all of the primitive prime divisors of $p^{2k} - 1$ divide $p^k + 1$. Therefore the primitive prime divisors of $p^k + 1$ are defined to be the primitive prime divisors of $p^{2k} - 1$. Here, we shall note that the Mersenne primes which are less than 1000 are 3, 7, 31, 127.

For the practical purposes of our algorithms, we shall be dealing with small primes, for example the primes less than 1000. Assume that $q \equiv 1 \bmod 4$ and $q = p^k$ for some prime p. If $k = 1$, then we can assume that the factorization into primes is possible and we can check whether a given element has order $(p\pm1)/2$. If

$k \geqslant 2$ and q is big, then we can not use factorization of integers into primes to find exact orders of elements. In this case, if $p \equiv 1 \bmod 4$, then we look for an element $t \in T$ which satisfies

$$t^{p^k-1} = 1, \quad t^{\prod_{i=1}^{k-1}(p^i-1)} \neq 1.$$

Moreover, we also need that the element $t^{\frac{p^k-1}{p-1}}$ has order $(p-1)/2$. If $p \equiv -1 \bmod 4$, then we look for the elements $t \in T$ satisfying

$$t^{p^k+1} = 1, \quad t^{\prod_{i=1}^{2k-1}(p^i-1)} \neq 1$$

and the element $t^{\frac{p^k+1}{p+1}}$ has order $(p+1)/2$. Note that the prime factorization of $p \pm 1$ can be computed in $O(p)$ time. It follows from [29, Lemma 2.6] that there exists a primitive prime divisor of $p^k \pm 1$ which divides the order of t.

Proof of Theorem 1.1. Let G be a simple black box group of Lie type of odd characteristic p. Assume first that $p \neq 5, 7$. If $G \ncong \mathrm{PSL}_2(q)$ or ${}^2\mathrm{G}_2(q)$, then we construct a long root $\mathrm{SL}_2(q)$-subgroup L of G by [41, Theorem 1.1]. Now by Lemmas 4.1, 4.3, 4.4 and Remark 4.2, we construct a subgroup $K \leqslant L \cong \mathrm{SL}_2(q)$ where $K \cong \mathrm{SL}_2(p)$. By [27], the proportion of the unipotent elements in K is $O(1/p)$. Therefore, we can find a unipotent element from randomly chosen $O(p)$ elements in K. If $G \cong {}^2\mathrm{G}_2(q)$, then $C_G(i)' \cong \mathrm{PSL}_2(q^2)$ for any involution $i \in G$. Therefore, by the same arguments above, we can construct unipotent elements in ${}^2\mathrm{G}_2(q)$ and $\mathrm{PSL}_2(q)$.

Assume now that $p = 5$ or 7. If $q = p^k$ and k has small prime divisor r. Then, again by the arguments above, we can construct a subgroup isomorphic to $(\mathrm{P})\mathrm{SL}_2(p^r)$ and perform random search in this subgroup to construct a unipotent element. In this case the probability of finding a unipotent element is $O(1/p^r)$.

Note that the running time of the algorithm [41, Theorem 1.1] constructing a long root $\mathrm{SL}_2(q)$-subgroup is polynomial in the input length. Therefore the running time of this algorithm follows from the above computations □

Algorithm 4.6. *Let G be a black box group isomorphic to $\mathrm{PSL}_2(q)$ where $q \equiv 1 \bmod 4$ and $q = p^k$.*

Input:
- *A set of generators of G.*
- *The characteristic p of the underlying field.*
- *An exponent E for G.*

Output:
- *A root subgroup U;*
- *The maximal torus T normalizing U;*
- *A Weyl group element w where U^w is the opposite root subgroup of U.*

Outline of Algorithm 4.6 (a more detailed description follows below):

1. Find the size of the field q.
2. Construct a Klein 4-group $V = \langle i, j \rangle$ in G together with the torus T where $i \in T$ and j inverts T.
3. Construct an element of order 3 in $N_G(V)$.
4. Construct $H \cong \mathrm{PSL}_2(p)$ or $\mathrm{PSL}_2(p^2)$ if $p \equiv 1 \bmod 4$ or $p \equiv -1 \bmod 4$, respectively.
5. Construct a unipotent element $u \in H$ of the form $u = ii^h$ for $h \in H$ and conclude that the torus T which contains i is a subgroup of $N_G(U)$ where U is the root subgroup containing u and j is the corresponding Weyl group element.

Now we give a more detailed description of Algorithm 4.6.

Step 1: We compute the size q of the underlying field by Algorithm 5.5 in [42].

Step 2: Let $E = 2^k m$ where $(2, m) = 1$. Take an arbitrary element $g \in G$. If the order of g is even, then the last non-identity element in the following sequence is an involution

$$1 \neq g^m,\ g^{2m},\ g^{2^2 m}, \ldots, g^{2^k m} = 1.$$

Note that the probability of finding an element of even order in the groups of Lie type of odd characteristic is at least $1/4$ by [28, Corollary 5.3]. Let $i \in G$ be an involution constructed as above. Then, we construct $C_G(i)$ by the method described in [4, 12] together with the result in [38]. We have $C_G(i) = T \rtimes \langle w \rangle$ where T is a torus of order $(q-1)/2$ and w is an involution which inverts T. We follow the arguments in Remark 4.5 to find a toral element $t \in T$ where $|t|$ is divisible by $(p-1)r$ if $p \equiv 1 \bmod 4$, or $(p^2-1)r$ if $p \equiv -1 \bmod 4$ where r is a primitive prime divisor of $(q-1)$. Note that t has order $(q-1)/2$ with probability at least $O(1/\log\log q)$. Note also that the coset Tw consists of involutions inverting T. Hence we can find an involution $j \in C_G(i)$ which inverts T with probability at least $1/2$. Now it is clear by the construction that $V = \langle i, j \rangle$ is a Klein 4-group, $i \in T$ and j inverts T.

Step 3: Let $i_1 = i$, $i_2 = j$, $i_3 = i*j$. Then we search for an element $g \in G$ such that $t_1 := i_1 i_2^g$ has odd order m_1 and $t_2 := i_2 i_3^{gu_1^{-1}}$ has odd order m_2 where $u_1 = t_1^{\frac{m_1+1}{2}}$. By Lemma 4.4, we can find such element $g \in G$ with probability at least $1/2 - 1/2q$. Now, by Lemma 4.3, $x := g u_1^{-1} u_2^{-1} \in N_G(V)$ has order 3, where $u_2 = t_2^{\frac{m_2+1}{2}}$.

Step 4: Let $T = \langle t \rangle$ be the torus constructed in Step 2 and x the element of order 3 constructed in Step 3. By Lemma 4.1, if $p \equiv 1 \bmod 4$, then $H = \langle t', x \rangle \cong \mathrm{PSL}_2(p)$ where $t' \in T$, $|t'| = (p-1)/2$. If $p \equiv -1 \bmod 4$, then $H = \langle t', x \rangle \cong \mathrm{PSL}_2(p^2)$ where $t' \in T$ and $|t'| = (p^2-1)/2$.

Step 5: Notice first that $i \in H$. Assume that $H \cong \mathrm{PSL}_2(p)$ and $p \equiv 1 \bmod 4$. Then, by Lemma 3.3, we can find an element $g \in H$ with probability at least $1/p$ such that $u = ii^g$ is a unipotent element in H. Since $i \in T$ (see Step 2), by Lemma 3.4, $T < N_G(U)$ where U is the subgroup containing u. Note that we can construct the root subgroup U by Lemma 3.5. Moreover, by Remark 3.6, the element j constructed in Step 2 is the corresponding Weyl group element.

If $p \equiv -1 \bmod 4$, then, in Step 4, we construct $H \cong \mathrm{PSL}_2(p^2)$. Following the same arguments above, we construct a unipotent element of the form $u = ii^g$ for some $g \in H$ with probability at least $1/p^2$ and the rest of the construction is the same as above.

4.1. **Complexity.** Let μ be an upper bound on the time requirement for each group operation in X and ξ an upper bound on the time requirement, per element, for the construction of random elements of X.

We outline the running time for each step as presented above. For simplicity, we assume that $E = |X| = |\mathrm{SL}_2(q)| = q(q^2-1)$.

Step 1: First, random elements in X belong to a torus of order $q-1$ or $q+1$ with probability at least $1 - O(1/q)$ by [27]. Then, in each type of tori, by [33], we can find an elements of order $q-1$ and $q+1$ with probability $c/\log\log q$ for some constant c. Therefore, producing $m = O(\log\log q)$ elements $g_1, \ldots, g_m$, we assume that one of g_i has order $q-1$ and g_j has order $q+1$. Now, checking each $g_i^{p(p^{2\ell}-1)} = 1$ involves at most $\log p^{2\ell+1}$ computations making the overall cost to determine the exact power of p involving in $q = p^k$

$$\sum_{\ell=1}^{k} \log(p^{2\ell+1}) = \log p^{k^2+2k} = (k+2)\log q.$$

Hence the size of the field can be computed in time $O(k\mu \log\log q \log q + \xi \log\log q)$.

Step 2: By [28, Corollary 5.3], random elements in X have even order with probability at least $1/4$. Then, construction of an involution i from a random element and checking whether an element of the form ii^g has odd order for a random element involves $\log|X| \leq \log q^3$ computations by repeated square and multiply method. Again, by [33], we can find a generator for the torus $T \leq C_G(i)$ with probability $O(1/\log\log q)$ and hence we can construct $C_G(i)$ in time $O(\xi \log\log q + \mu \log\log q \log q)$.

Step 3: By Lemma 4.4 the elements $t_1 = i_1 i_2^g$ and $t_2 = i_2 i_3^{gu_1^{-1}}$ have odd orders m_1 and m_2 with probability $1/2 - 1/2q$. Checking both elements for having odd order and construction of elements $u_1 = t_1^{\frac{m_1+1}{2}}$ and $u_2 = t_2^{\frac{m_2+1}{2}}$ involves $\log|X|$ multiplications making overall cost $O(\xi + \mu \log q)$.

Step 4: Determination of $p \equiv 1 \bmod 4$ or $p \equiv -1 \bmod 4$ can be done by Euclidean algorithm in time $O(\log^2 4)$, and computing an element $t' \in T$ with $|t'| = p \pm 1$ involves $O(\log q)$ multiplications. Hence the running time for this step is $O(\mu \log q)$.

Step 5: An element of the form ii^g in $\mathrm{SL}_2(p^2)$ has order p with probability $O(1/p^2)$. Checking ii^g has order p costs $O(\log p)$ multiplications. Hence the running time for this step is $O(\xi p^2 + \mu p^2 \log p)$.

By the running times of each steps above, the overall running time of the algorithm is $O(\xi(\log\log q + p^2) + \mu(k \log\log q \log q + \log q + p^2 \log p))$.

Notice that algorithms described in this and previous section provide a proof of Theorems 1.2 and 1.3.

5. Construction of a maximal split torus

Let G be a quasi-simple classical black box group of odd characteristic isomorphic to $(\mathrm{P})\mathrm{SL}_{n+1}(q)$, $(\mathrm{P})\mathrm{Sp}_{2n}(q)$, $(\mathrm{P})\Omega_{2n+1}(q)$ or $(\mathrm{P})\Omega^+_{2n}(q)$. Assume that $\{K_0, K_1, \ldots, K_n\}$ is an extended Curtis-Tits configuration of G.

In this section, for any odd $q > 3$, we describe a method constructing the split tori $T_\ell < K_\ell$, $\ell = 0, 1, \ldots, n$, which all together generate a maximally split torus

$$T = \langle T_k \mid k = 1, 2, \ldots, n \rangle$$

in G normalizing K_ℓ for all $\ell \in \{0, 1, \dots, n\}$. We set that K_0 is the root $\mathrm{SL}_2(q)$-subgroup of G corresponding to the extra node in the extended Dynkin diagram of G.

Note that an extended Curtis-Tits configuration of G can be constructed by using the algorithm in [5] except that $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$ and $q \equiv -1 \bmod 4$. Therefore, we assume that $q \equiv 1 \bmod 4$ if $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$.

5.1. **Groups of type A_n.** Assume that $G \cong (\mathrm{P})\mathrm{SL}_{n+1}(q)$, $q > 3$, $n \geqslant 2$. Note that, for each $\ell = 0, 1, \dots, n$ (see Figure 1), $K_\ell \cong \mathrm{SL}_2(q)$. Assume that $i_\ell \in K_\ell$ is the unique involution for each $\ell = 0, 1, \dots, n$.

We set

- $T_0 = C_{K_0}(i_1) = C_{K_0}(i_n)$,
- $T_1 = C_{K_1}(i_2)$,
- $T_\ell = C_{K_\ell}(i_{\ell-1})$, $\ell = 2, \dots, n$.

Lemma 5.1. *We have $|T_\ell| = q - 1$ for each $\ell = 0, 1, 2, \dots, n$.*

Proof. Recall that the involutions i_ℓ, $\ell = 0, 1, \dots, n$, mutually commute with each other. Observe that $i_k \in N_G(K_\ell)$ for all $k, \ell = 0, 1, \dots, n$ and $i_{\ell-1}$ acts as an involution of type t_1 on K_ℓ for $\ell = 2, \dots, n$. Hence $|T_\ell| = |C_{K_\ell}(i_{\ell-1})| = q - 1$ for $\ell = 2, 3, \dots, n$. The other cases are analogous. □

Lemma 5.2. *The subgroup $\langle T_0, T_1, \dots, T_n\rangle$ is a maximally split torus normalizing K_ℓ for each $\ell = 0, 1, \dots, n$. In particular, $\langle T_0, T_1, \dots, T_n\rangle = \langle T_1, \dots, T_n\rangle$.*

Proof. By Lemma 5.1, we have $|T_\ell| = q - 1$ for each $\ell = 0, 1, \dots, n$. We shall prove that T_ℓ's are mutually commuting with each other. We prove that $[T_1, T_2] = 1$ and the other cases are treated similarly. Consider $L = \langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$. Then, by [25, Theorem 4.5.5 (c)], $C_L(i_2) = N_L(K_2)$. Therefore $T_1 = C_{K_1}(i_2)$ normalizes K_2. Thus $C_{K_2}(T_1)$ is a torus in K_2. Since $C_{K_2}(i_1)$ is also a torus in K_2 we must have $T_2 = C_{K_2}(i_1) = C_{K_2}(T_1)$. Thus $[T_1, T_2] = 1$. In a similar manner, we have $[T_k, T_\ell] = 1$ and $T_k \leqslant N_G(K_\ell)$ for each $k, \ell = 0, 1, \dots, n$ so $T = \langle T_1, \dots T_n\rangle$ is a maximally split torus normalizing K_ℓ for each $\ell = 0, 1, \dots, n$. Since T_0 commutes with T_ℓ for each $\ell = 1, \dots, n$, we have $T_0 \leqslant C_G(\langle T_1, \dots, T_n\rangle) = \langle T_1, \dots, T_n\rangle$. □

5.2. **Groups of type C_n.** Assume that $G \cong \mathrm{PSp}_{2n}(q)$, $n \geqslant 2$, $q \equiv 1 \bmod 4$. Let $\Sigma = \{K_0, K_1, \dots, K_n\}$ be an extended Curtis-Tits configuration of G. By Remark 2.5, we can take an involution $j \in G$ (necessarily of type t_n) such that $C_G(j) = LD$ where $L = \langle K_1, \dots, K_{n-1}\rangle = C_G(j)'' \cong \frac{1}{(2,n)}\mathrm{SL}_n(q)$ and D is a dihedral group of order $2(q-1)$. Note that if $G \cong \mathrm{Sp}_{2n}(q)$, then j is a pseudo-involution, $L \cong \mathrm{SL}_n(q)$ and D is a torus of order $q-1$. Note also that if $G \cong \mathrm{PSp}_4(q)$, then $K_1 \cong \mathrm{PSL}_2(q)$, $K_0 \cong K_2 \cong \mathrm{SL}_2(q)$ and in all the other cases $K_\ell \cong \mathrm{SL}_2(q)$ for each $\ell = 0, 1, \dots, n$.

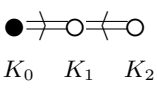


FIGURE 4. Extended Dynkin diagram of C_2

Remark 5.3. Since $\{K_0, K_1, \dots, K_n\}$ is a Curtis-Tits configuration of $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$, the element $j \in G$ chosen above has the property that $j \in N_G(K_i)$ for all $i = 0, 1, \dots, n$.

We set

- $T_0 = C_{K_0}(j)$ and $T_n = C_{K_n}(j)$ where j is as above.
- If $n = 2$, then T_1 is the cyclic subgroup of order $(q-1)/2$ in $C_{K_1}(i_0)$ where $i_0 \in Z(K_0)$.
- If $n \geq 3$, then $T_1, \dots, T_{n-1}$ are as described in Subsection 5.1.

Lemma 5.4. *Let $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$ and $q \equiv 1 \bmod 4$. Then $\langle T_0, T_1, \dots, T_2\rangle$ is a maximally split torus normalizing K_ℓ for each $\ell = 0, 1, \dots, n$. In particular, $\langle T_0, T_1, \dots T_n\rangle = \langle T_1, \dots T_n\rangle$*

Proof. We first assume that $G \cong \mathrm{PSp}_4(q)$. Then $K_0 \cong K_2 \cong \mathrm{SL}_2(q)$ and $K_1 \cong \mathrm{PSL}_2(q)$, (see Figure 4). We shall show that $T = \langle T_0, T_1, T_2\rangle$ is abelian. By the setting above, it is clear that $[T_0, T_2] = 1$. Moreover, $i_0 \in C_G(j)$ and $i_0 \in N_G(K_1)$ where $i_0 \in Z(K_0)$ since $\{K_0, K_1, K_2\}$ is a Curtis-Tits configuration of G. Now $T_1 \leqslant C_{K_1}(i_0) = C_{K_1}(T_0) = C_{K_1}(T_2)$ since T_0 and T_2 are cyclic groups and $i_0 \in T_0 \cap T_2$. Hence $[T_1, T_0] = [T_1, T_2] = 1$.

We have $T_0 = C_{K_0}(j) \leqslant C_G(j) = N_G(K_1)$. Similarly, we have $T_2 \leqslant N_G(K_1)$. Observe that $C_{K_1}(i_0)' \leqslant C_G(i_0)' = N_G(K_0) = N_G(K_2)$ and $|T_1 : C_{K_1}(i_0)'| = 2$ so $T_1 \leqslant N_G(K_0) = N_G(K_2)$. Thus, T_0, T_1 and T_2 normalize K_0, K_1 and K_2. Moreover, since T_0 commutes with T_1 and T_2, we have $T_0 \leqslant C_G(\langle T_1, T_2\rangle) = \langle T_1, T_2\rangle$.

Now we assume that $G \cong \mathrm{Sp}_4(q)$ or $(\mathrm{P})\mathrm{Sp}_{2n}(q)$, $n \geq 3$. We first show that $\langle T_0, T_1, \dots, T_n\rangle$ is abelian. By Lemma 5.2, observe that it is enough to show that $[T_0, T_1] = [T_{n-1}, T_n] = 1$. We show that $[T_0, T_1] = 1$ and the other case is analogous. Consider $L = \langle K_0, K_1\rangle \cong \mathrm{Sp}_4(q)$. Since $\{K_0, K_1, \dots, K_n\}$ is a Curtis-Tits configuration of G, we have $C_L(i_2) = C_L(i_0) = K_0 \times \widetilde{K}_0$ for some $\widetilde{K}_0 \cong \mathrm{SL}_2(q)$, and i_0, i_2 act as an involution of type t_1 on K_1. Therefore $C_{K_1}(i_0) = C_{K_1}(i_2) = T_1$. Now since j commutes with K_1 and T_0, we have $K_1T_0 \leqslant C_L(j)$. Therefore $i_0 \in T_0 \leqslant N_L(K_1)$. It follows that $T_1 = C_{K_1}(i_0) = C_{K_1}(T_0)$. Hence $[T_0, T_1] = 1$.

It is clear that T_0 commutes with K_ℓ for each $\ell = 2, \dots, n$. Therefore, since $T_0 \leqslant N_L(K_1)$, we have $T_0 \leqslant N_G(K_\ell)$ for each $\ell = 2, \dots, n$. Moreover, $T_1 = C_{K_1}(i_2) = C_{K_1}(i_0) \leqslant C_L(i_0) = N_L(K_0)$. By similar arguments, we conclude that $T_k \leqslant N_G(K_\ell)$ for all $k, \ell = 0, 1, \dots, n$.

Since T_0 commutes with T_ℓ for each $\ell = 1, 2, \dots, n$. We have

$$T_0 \leqslant C_G(\langle T_1, T_2, \dots, T_n\rangle) = \langle T_1, T_2, \dots, T_n\rangle.$$

Hence $\langle T_1, T_2, \dots, T_n\rangle = \langle T_0, T_1, T_2, \dots, T_n\rangle$ and the lemma follows. □

5.3. **Groups of type B_n.** Assume that $G \cong \Omega_{2n+1}(q)$, $q > 3$, $n \geqslant 3$. Let $\{K_0, K_1, \dots, K_n\}$ be an extended Curtis-Tits configuration for G where K_ℓ, $\ell = 0, 1, \dots, n-1$, correspond to long root $\mathrm{SL}_2(q)$-subgroups and K_n corresponds to the short root $\mathrm{SL}_2(q)$-subgroup in the extended Dynkin diagram of G (see Figure 3). Then $K_\ell \cong \mathrm{SL}_2(q)$ for $\ell = 0, 1, \dots, n-1$ and $K_n \cong \mathrm{PSL}_2(q)$. We set

- $T_0 = C_{K_0}(i_2)$, $T_1 = C_{K_1}(i_2)$,
- $T_\ell = C_{K_\ell}(i_{\ell-1})$, $\ell = 2, \dots, n-1$,
- $T_n < C_{K_n}(i_{n-1})$ where T_n is an abelian group of order $(q-1)/2$.

Lemma 5.5. *Let $G \cong \Omega_{2n+1}(q)$, $n \geqslant 3$. Then $\langle T_0, T_1, \dots, T_n\rangle$ is a maximally split torus normalizing each K_ℓ, $\ell = 0, 1, \dots, n$. In particular, $\langle T_0, T_1, \dots, T_n\rangle = \langle T_1, \dots, T_n\rangle$.*

Proof. It follows from the extended Dynkin diagram of G (see Figure 3 on page 10) that $\langle K_0, K_2, \dots, K_{n-1}\rangle \cong \langle K_1, K_2, \dots, K_{n-1}\rangle \cong \mathrm{SL}_n(q)$ and $\langle K_{n-1}, K_n\rangle \cong \mathrm{PSp}_4(q)$. Recall that $K_n \cong \mathrm{PSL}_2(q)$ and the involution $i_{n-1} \in K_{n-1}$ acts as an involution of type t_1 on K_n so $C_{K_n}(i_{n-1})$ is a dihedral group of order $q-1$. Taking T_n as the abelian group of order $(q-1)/2$ in $C_{K_n}(i_{n-1})$, the result follows from Lemmas 5.2 and 5.4. □

5.4. **Groups of type D_n.** Assume that $G \cong (\mathrm{P})\Omega^+_{2n}(q)$, $q > 3$, $n \geqslant 4$. Let $\{K_0, K_1, \dots, K_n\}$ be an extended Curtis-Tits configuration for G. Then, for each $\ell = 0, 1, \dots, n$ (see Figure 1), $K_\ell \cong \mathrm{SL}_2(q)$. Assume that $i_\ell \in K_\ell$ is the unique involution for each $\ell = 0, 1, \dots, n$.

We set

- $T_0 = C_{K_0}(i_2)$, $T_1 = C_{K_1}(i_2)$,
- $T_{n-1} = C_{K_{n-1}}(i_{n-2})$, $T_n = C_{K_n}(i_{n-2})$,
- $T_\ell = C_{K_\ell}(i_{\ell-1})$, $\ell = 2, \dots, n-2$.

Lemma 5.6. *Let $G \cong (\mathrm{P})\Omega^+_{2n}(q)$, $n \geqslant 4$. Then $\langle T_0, T_1, \dots, T_n\rangle$ is a maximally split torus normalizing each K_ℓ, $\ell = 0, 1, \dots, n$. In particular, $\langle T_0, T_1, \dots, T_n\rangle = \langle T_1, \dots, T_n\rangle$.*

Proof. It follows from the extended Dynkin diagram of G (see Figure 1 on page 8) that

$$(\mathrm{P})\mathrm{SL}_n(q) \cong \langle K_0, K_2, K_3, \dots, K_{n-2}, K_n\rangle \cong \langle K_1, K_2, K_3, \dots, K_{n-2}, K_{n-1}\rangle.$$

Hence the result follows from Lemma 5.2. □

6. Construction of the Weyl group

In this section, we construct the generators of the Weyl group of a quasi-simple classical group G, which correspond to the fundamental reflections in the root system of G.

We assume that $q \equiv 1 \bmod 4$ throughout this section. Let $\{K_0, K_1, \dots, K_n\}$ be an extended Curtis-Tits configuration of G. Assume also that $T_\ell < K_\ell$, $\ell = 0, 1, \dots, n$, be the corresponding tori constructed as in Section 5. We construct the Weyl group elements $w_\ell \in K_\ell$ as discussed in Remark 3.6 for each $\ell = 0, 1, \dots, n$.

Lemma 6.1. *Let $w_\ell \in K_\ell$ be Weyl group elements associated to T_ℓ, that is, w_ℓ inverts T_ℓ for each $\ell = 0, 1, \dots, n$. Then $w_\ell \in N_G(T)$ for each $\ell = 0, 1, \dots, n$ where $T = \langle T_0, T_1, \dots, T_n\rangle$. In particular,*

$$W = \langle w_0, w_1, \dots, w_n\rangle T/T = \langle w_1, \dots, w_n\rangle T/T$$

is the Weyl group of G.

Proof. We prove that $w_1 \in N_G(T)$ and the other cases are analogous. Assume first that $G \cong (\mathrm{P})\mathrm{SL}_n(q)$ and $L = \langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$. Since w_1 inverts T_1 and $[T_1, T_2] = 1$, we have $[T_1^{w_1}, T_2] = 1$ which implies that $T_2^{w_1} \leqslant C_L(T_1) = \langle T_1, T_2\rangle$. Hence $w_1 \in N_L(\langle T_1, T_2\rangle)$. Similarly, $w_1 \in N_L(\langle T_1, T_0\rangle)$. By the construction of $K_0, K_1, \dots, K_n$, it is clear that w_1 commutes with T_ℓ for $\ell \geqslant 3$. Thus $w_1 \in N_G(T)$.

If $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$, then it is enough to consider $L = \langle K_0, K_1\rangle \cong (\mathrm{P})\mathrm{Sp}_4(q)$. Then, following the same arguments above, we see that $w_1 \in N_G(T)$. The groups of type B_n and D_n are treated similarly.

Observe that, in all cases, we have $w_0 \in N_G(T)$ by the same arguments in the case $G \cong \mathrm{PSL}_n(q)$. Since $N_G(T) = \langle w_1, \dots, w_n\rangle T$, we have $w_0 \in \langle w_1, \dots, w_n\rangle T$ and the lemma follows. □

7. Construction of root elements in $(\mathrm{P})\mathrm{SL}_{n+1}(q)$

Let $G \cong (\mathrm{P})\mathrm{SL}_{n+1}(q)$ and $\{K_0, K_1, \dots, K_n\}$ be an extended Curtis-Tits configuration for G. In this section, we construct unipotent elements $u_0, u_1, \dots, u_n$ in $K_0, K_1, \dots, K_n$ where the maximal split torus $T = \langle T_0, T_1, \dots, T_n\rangle$ constructed in Section 5 normalizes the root subgroups $U_\ell < K_\ell$ containing u_ℓ for each $\ell = 0, 1, 2, \dots, n$. Note that $T_\ell < K_\ell$ for each $\ell = 0, 1, 2, \dots, n$.

By Algorithm 4.6, we can construct a triple (u, T, w) such that $u \in K_1 \cong \mathrm{SL}_2(q)$ is a unipotent element, $T < K_1$ is a torus of order $q - 1$ normalizing the root subgroup containing u and $w \in K_1$ is a Weyl group element. By Lemmas 3.7 and 4.4, we can find an element $g \in K_1$ such that $T^g = T_1$ with probability at least $1/2$. We set $u_1 = u^g$ and $w_1 = w^g$. Then, it is clear that T_1 is a maximal torus in K_1 normalizing the root subgroup U_1 containing u_1. Moreover w_1 inverts T_1 and U_1^w is the opposite root subgroup of U_1.

For each tori $T_0, T_1, \dots, T_n$, let $w_0, w_1, \dots, w_n$ be the corresponding Weyl group elements constructed as discussed in Remark 3.6, then, by Lemma 6.1,

$$W = \langle w_0, w_1, \dots, w_n\rangle T/T = \langle w_1, \dots, w_n\rangle T/T$$

is the Weyl group of G.

Lemma 7.1. *Let $G \cong (\mathrm{P})\mathrm{SL}_{n+1}(q)$. If $\{w_1, \dots, w_n\}$ is a set of fundamental reflections in the Weyl group W of G. Then*

$$\alpha_i = w_{i-1}w_i(\alpha_{i-1})$$

where α_i is the corresponding fundamental root in the root system of G and $i = 2, \dots, n$. Moreover,

$$\alpha_0 = w_0w_nw_0(\alpha_n).$$

Proof. The proof follows from a direct computation in the structure of the root system of type A_n. □

Corollary 7.2. *Let $G \cong (\mathrm{P})\mathrm{SL}_{n+1}(q)$. We have*

$$U_i = U_{i-1}^{w_{i-1}w_i}$$

for each $i = 2, \dots, n$ and

$$U_0 = U_n^{w_0w_nw_0}.$$

8. The algorithm

Algorithm 8.1. *Let $G \cong (\mathrm{P})\mathrm{SL}_{n+1}(q)$, $(\mathrm{P})\mathrm{Sp}_{2n}(q)$, $\Omega_{2n+1}(q)$, or $(\mathrm{P})\Omega^+_{2n}(q)$ where $q = p^k$ and $q \equiv 1 \bmod 4$.*

Input:
- *a set of generators for G;*
- *the characteristic p of the underlying field;*
- *an exponent for G.*

Output:
- *An extended Curtis-Tits system* $\{K_0, K_1, \ldots, K_n\}$ *for* G *together with*
  - *The root subgroups* $U_\ell < K_\ell$ *for each* $\ell = 0, 1, \ldots, n$*;*
  - *The maximally split torus*

$$T = \langle T_0, T_1, \ldots, T_n \rangle$$

where $T_k < N_G(U_\ell)$ *for all* $k, \ell = 0, 1, \ldots, n$*;*

  - *The Weyl group elements* $w_\ell \in K_\ell$*, where* $U_\ell^{w_\ell}$ *is the opposite root subgroup of* U_ℓ *for each* $\ell = 0, 1, \ldots, n$ *and*

$$\langle w_0, w_1, \ldots, w_n \rangle T/T = \langle w_1, \ldots, w_n \rangle T/T$$

is the Weyl group of G*.*

The details of Algorithm 8.1 are as follows:

1. Construct an extended Curtis-Tits configuration $\Sigma = \{K_0, K_1, \ldots, K_n\}$ of G and find the size q of the underlying field.
2. Construct a maximally split torus $T = \langle T_0, T_1, \ldots, T_n \rangle$ and Weyl group elements $w_0, w_1, \ldots, w_n$, where $T_\ell \leqslant K_\ell$ and T normalizes K_ℓ for each $\ell = 0, 1, \ldots, n$.
3. Construct a subgroup $H_1 \cong \mathrm{SL}_2(p)$ or $\mathrm{SL}_2(p^2)$ if $p \equiv 1 \bmod 4$ or $p \equiv -1 \bmod 4$, respectively, in K_1.
4. Construct (u, S, w) in H_1, where u is a unipotent element, S is a maximal torus normalizing the root subgroup containing u and w is a Weyl group element which inverts S.
5. Construct the maximal torus $T \leqslant K_1$ containing S.
6. Construct $z \in K_1$ such that $T^z = T_1$.
7. Construct the remaining unipotent elements in each K_ℓ, $\ell = 0, 2, 3, \ldots, n$.

And what follows is a more detailed descriptions of Steps 1–7.

Step 1: We use the algorithm in [5] to construct an extended Curtis-Tits configuration

$$\Sigma = \{K_0, K_1, \ldots, K_n\}$$

of G. We compute the size q of the underlying field by using [42, Algorithm 5.5].

Step 2: We construct a maximally split torus $T = \langle T_0, T_1, \ldots, T_n \rangle$ as described in Section 5 depending on the type of the group G. Here the construction of the tori T_k, $k = 0, 1, \ldots, n$, means that we find a toral element $t_k \in T_k$ as in Step 2 of Algorithm 4.6. Moreover, by Remark 3.6, we can construct the corresponding Weyl group elements $w_0, w_1, \ldots, w_n$ in $K_0, K_1 \ldots, K_n$, respectively. By Lemma 6.1,

$$W = \langle w_0, w_1, \ldots, w_n \rangle T/T$$

is the Weyl group of G.

Step 3: Assume that $K_1 \cong \mathrm{PSL}_2(q)$. Then this is Step 2, 3 and 4 of Algorithm 4.6. Observe that the same computations apply for $K_1 \cong \mathrm{SL}_2(q)$ with obvious modifications in the arguments as noted in the beginning of Section 3.

Step 4: This is Step 5 of Algorithm 4.6.

Step 5: We continue to assume that $K_1 \cong \mathrm{PSL}_2(q)$. If $i \in S$ is an involution, then $C_{K_1}(i)$ contains a torus T of order $(q-1)/2$ containing S. It is clear

that T normalizes the the root subgroup U_1 which contains u. We construct the root subgroup U_1 by using Lemma 3.5.

Step 6: Let T_1 and T be the tori constructed in Step 2 and Step 5, respectively. Then, by Lemmas 3.7 and 4.4, we can construct an element $z \in K_1$ such that $T^z = T_1$ with probability at least $1/2$.

Step 7: If $G \cong (\mathrm{P})\mathrm{SL}_{n+1}(q)$, then, by Corollary 7.2, we construct the remaining unipotent elements $u_\ell \in K_\ell$ for each $\ell = 0, 2, \ldots, n$.

If $G \cong (\mathrm{P})\mathrm{Sp}_{2n}(q)$, then, since

$$\langle K_1, \ldots, K_{n-1} \rangle \cong \frac{1}{(2,n)}\mathrm{SL}_n(q) \text{ or } \mathrm{SL}_n(q),$$

we can construct unipotent elements $u_2 \in K_2, \ldots, u_{n-1} \in K_{n-1}$ by Corollary 7.2. To construct u_0 and u_n, we repeat Steps 3, 4, 5, 6 for the groups K_0 and K_n. It is clear that the unipotent elements u_0 and u_n are aligned with the rest of the unipotent elements since T_0 and T_n are aligned with the rest of the root subgroups. However, we need to check whether u_0 and u_n commute with u_1 and u_{n-1}, respectively, since u_0 or u_n may correspond to opposite root subgroups in K_0 and K_n, respectively.

If $G \cong \Omega_{2n+1}(q)$, then the construction of the remaining unipotent elements is similar to the construction of unipotent elements for $\mathrm{PSp}_{2n}(q)$.

If $G \cong (\mathrm{P})\Omega^+_{2n}(q)$, then

$$\langle K_1, K_2, \ldots, K_{n-1} \rangle \cong \mathrm{SL}_n(q).$$

Therefore, we can construct unipotent elements $u_2 \in K_2, \ldots, u_{n-1} \in K_{n-1}$ by Corollary 7.2. We follow the same arguments in the case of $(\mathrm{P})\mathrm{Sp}_{2n}(q)$ to construct $u_0 \in K_0$ and $u_n \in K_n$.

Finally, by Lemma 3.5, we construct the root subgroups $U_0, U_1, \ldots, U_n$ for each type of the group G.

Note that the running time of the algorithm in [5] which constructs an extended Curtis-Tits configuration is polynomial in the input length. Therefore, together with the computations in Subsection 4.1, the running time of the algorithm constructing Steinberg generators for $(\mathrm{P})\mathrm{SL}_{n+1}(q), (\mathrm{P})\mathrm{Sp}_{2n}(q), \Omega_{2n+1}(q)$ and $(\mathrm{P})\Omega^+_{2n}(q)$, $q \equiv 1 \bmod 4$, is quadratic in p and is polynomial in the Lie rank n and $\log q$. Hence algorithms described in this section provide proof of Theorem 1.4.

Acknowledgements

This paper would have never been written if the authors did not enjoy the warm hospitality offered to them at the Nesin Mathematics Village (in Şirince, Izmir Province, Turkey) in August 2011 and August 2012; our thanks go to Ali Nesin and to all volunteers and staff who have made the Village a mathematical paradise.

We thank Adrien Deloro for many fruitful discussions, in Şirince and elsewhere. We also thank Bill Kantor for his invaluable comments.

The first author is grateful to Dr Douglas E Jeffrey for most helpful advice.

We gratefully acknowledge the use of Paul Taylor's Commutative Diagrams package, `http://www.paultaylor.eu/diagrams/`.

References

[1] L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000) (New York), ACM, 2000, pp. 627–635.

[2] L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, J. Algorithms **50** (2004), no. 2, 215–231, SODA 2000 special issue.

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

[4] A. V. Borovik, *Centralisers of involutions in black box groups*, Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 7–20.

[5] A.V. Borovik and Ş. Yalçınkaya, *Construction of Curtis-Phan-Tits system for black box classical groups*, Available at arXiv:1008.2823v1.

[6] A.V. Borovik and Ş. Yalçınkaya, *Classical black box groups in small odd characteristics*, in preparation.

[7] A.V. Borovik and Ş. Yalçınkaya, *Fifty shades of black*, in preparation.

[8] A.V. Borovik and Ş. Yalçınkaya, *Oracles and revelations*, in preparation.

[9] A.V. Borovik and Ş. Yalçınkaya, *Subgroup structure and automorphisms of black box classical groups*, in preparation.

[10] A.V. Borovik and Ş. Yalçınkaya, *Subgroup structure and automorphisms of black box groups of exceptional groups of odd characteristic*, in preparation.

[11] S. Bratus and I. Pak, *On sampling generating sets of finite groups and product replacement algorithm (extended abstract)*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 91–96.

[12] J. N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245.

[13] P. A. Brooksbank, *A constructive recognition algorithm for the matrix group* $\Omega(d, q)$, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 79–93.

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

[15] P. A. Brooksbank, *Fast constructive recognition of black box symplectic groups*, J. Algebra **320** (2008), no. 2, 885–909.

[16] P. A. Brooksbank and W. M. Kantor, *On constructive recognition of a black box* $\mathrm{PSL}(d, q)$, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 95–111.

[17] P. A. Brooksbank and W. M. Kantor, *Fast constructive recognition of black box orthogonal groups*, J. Algebra **300** (2006), no. 1, 256–288.

[18] R. W. Carter, *Simple Groups of Lie Type*, John Wiley & Sons, London, 1972.

[19] F. Celler and C. R. Leedham-Green, *A constructive recognition algorithm for the special linear group*, The atlas of finite groups: ten years on (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, Cambridge, 1998, pp. 11–26.

[20] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), no. 13, 4931–4948.

[21] M. D. E. Conder and C. R. Leedham-Green, *Fast recognition of classical groups over large fields*, Groups and Computation III (Berlin) (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, 2001, pp. 113–121.

[22] M. D. E. Conder, C. R. Leedham-Green, and E. A. O'Brien, *Constructive recognition of* $\mathrm{PSL}(2, q)$, Trans. Amer. Math. Soc. **358** (2006), no. 3, 1203–1221.

[23] A. Gamburd and I. Pak, *Expansion of product replacement graphs*, Combinatorica **26** (2006), no. 4, 411–429.

[24] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups. Number 1*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1994.

[25] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1998.

[26] The GAP Group, *Gap—groups, algorithms, and programming, version 4.4*, Aachen, St Andrews (`http://www-gap.dcs.st-and.ac.uk/ gap`) (2004).
[27] R. M. Guralnick and F. Lübeck, *On p-singular elements in Chevalley groups in characteristic p*, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 169–182.
[28] I. M. Isaacs, W. M. Kantor, and N. Spaltenstein, *On the probability that a group element is p-singular*, J. Algebra **176** (1995), no. 1, 139–181.
[29] W. M. Kantor and Á. Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708, viii+168.
[30] C. R. Leedham-Green, *The computational matrix group project*, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 229–247.
[31] C. R. Leedham-Green and E. A. O'Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881.
[32] A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363.
[33] D. S. Mitrinović, J. Sándor, and B. Crstici, *Handbook of number theory*, Mathematics and its Applications, vol. 351, Kluwer Academic Publishers Group, Dordrecht, 1996.
[34] I. Pak, *The product replacement algorithm is polynomial*, 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), IEEE Comput. Soc. Press, Los Alamitos, CA, 2000, pp. 476–485.
[35] I. Pak, *The product replacement algorithm is polynomial*, Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci. (2001), 476–485.
[36] I. Pak, *What do we know about the product replacement algorithm?*, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 301–347.
[37] I. Pak and A. Żuk, *On Kazhdan constants and mixing of random walks*, Int. Math. Res. Not. (2002), no. 36, 1891–1905.
[38] C. W. Parker and R. A. Wilson, *Recognising simplicity of black-box groups by constructing involutions and their centralisers*, J. Algebra **324** (2010), no. 5, 885–915.
[39] M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.
[40] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968, Notes prepared by John Faulkner and Robert Wilson.
[41] Ş. Yalçınkaya, *Construction of long root $SL_2(q)$-subgroups in black-box groups*, Available at arXiv, math.GR/1001.3184v1.
[42] Ş. Yalçınkaya, *Black box groups*, Turkish J. Math. **31** (2007), no. suppl., 171–210.
[43] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), no. 1, 265–284.

School of Mathematics, University of Manchester, UK
E-mail address: `alexandre.borovik@gmail.com`

Bilgi University, Istanbul, Turkey
E-mail address: `sukru.yalcinkaya@gmail.com`