Turkish Journal of Mathematics

Volume 31
Number 5 *Suppl.*

Article 12

1-1-2007

Black Box Groups

ŞÜKRÜ YALÇINKAYA

Turk J Math
31 (2007) , Suppl, 171 – 210.

Black Box Groups

Şükrü Yalçınkaya

Abstract

We propose a uniform approach for recognizing all black box groups of Lie type which is based on the analysis of the structure of the centralizers of involutions. Our approach can be viewed as a computational version of the classification of the finite simple groups. We present an algorithm which constructs a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple group of Lie type of odd characteristic, then we use the Aschbacher's "Classical Involution Theorem" as a model in the recognition algorithm and we construct all root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes in the extended Dynkin diagram, that is, we construct the extended Curtis - Phan - Tits system of the finite simple groups of Lie type of odd characteristic. In particular, we construct all subsystem subgroups which can be read from the extended Dynkin diagram. We also present an algorithm which determines whether the p-core (or "unipotent radical") $O_p(G)$ of a black box group G is trivial or not, where $G/O_p(G)$ is a finite simple classical group of odd characteristic p, answering a well-known question of Babai and Shalev.

1. Introduction

A *black box group* X is a device or an algorithm (*'oracle'* or *'black box'*) which produces (nearly) uniformly distributed independent random elements from some finite group X. These elements are encoded as 0–1 strings of uniform length N; given strings representing $x, y \in X$, the black box can compute strings representing xy and x^{-1}, and decide whether $x = y$ in time bounded from above by a constant. In this setting, one is usually interested in finding probabilistic algorithms which allow us to determine, with probability of error ϵ, the isomorphism type of X in time $O(\log(1/\varepsilon) \cdot (\log |X|)^c)$. Note that we have an upper

2000 *AMS Mathematics Subject Classification:* 20G40, 20F69

bound for the order of the group $|X| \leqslant 2^N$. See [12, 6] for thorough discussion of the subject.

A *Monte–Carlo algorithm* is a randomized algorithm which gives a correct output to a decision problem with probability strictly bigger than 1/2. The probability of having incorrect output can be made arbitrarily small by running the algorithm sufficiently many times. A Monte–Carlo algorithm with outputs "yes" and "no" is called *one-sided* if the output "yes" is always correct. A *polynomial time* algorithm is an algorithm whose running time is polynomial in the input length. A Monte–Carlo algorithm which runs in polynomial time in the input length is called a *Monte–Carlo polynomial time algorithm*. A special subclass of Monte–Carlo algorithm is a *Las Vegas algorithm* which either outputs a correct answer or reports failure. A detailed comparison of Monte–Carlo and Las Vegas algorithms, both from practical and theoretical point, can be found in [5].

In this paper our goal is to present a structural approach to the recognition of black box groups. Our methods develops a remarkable analogy between the classification of the finite simple groups and the recognition of black box groups (Section 2). The conjugacy classes of involutions and their centralizers, which played a prominent role in the classification of the finite simple groups, are the main focus of our methods.

Isomorphisms and homomorphisms of black box groups are understood as isomorphisms and homomorphisms of their underlying groups. However we reserve the term *black box subgroup* for a subgroup of a black box group endowed with its own black box oracle.

The important examples of black box groups are permutation groups and matrix groups over finite fields. Practically, the recognition problem is interesting when the input group is big. For example, given two square matrices x and y of size 100×100 over a finite field, it is unrealistic to list all elements in the group X generated by x and y and determine the isomorphism class of X by inspection. But this can often be done, with an arbitrarily small probability of error, by studying a sample of random products of the generators x and y. The algorithms are implemented in the software packages GAP [44] and MAGMA [19].

If the group representation is known, for example, generators of a group may be given as permutations on some set or matrices over finite fields, the algorithms, in many cases, depend on the representation of the given group. For example, there is a huge library of permutation group algorithms in literature running in *nearly* linear polynomial time in the input length (for example, constructing centralizers of elements, center of the group

etc.), see the book by Seress [70] for an exposition of such algorithms. In the matrix group setting, there is an ambitious on-going project called "computational matrix group project" which is focused on the construction of composition series of a given matrix group over finite fields. Leedham–Green outlined in [53] how a composition series for a matrix group $X \leqslant \mathrm{GL}_n(q)$ can be computed by using Aschbacher's classification theorem on the structure of maximal subgroups of $\mathrm{GL}_n(q)$ [3], for the recent advances see [63].

1.1. Order oracle

Almost nothing can be said about a black box group without access to additional information. In some cases (for example, when our black box is given as a permutation group of computationally feasible degree) we can use the *order oracle*, that is, we can determine the orders of elements $x \in X$. Note that the order of an element can be easily computed from its cycle structure in a permutation group. We can also determine the order of an element when we are given a reasonably small superset π of prime integers dividing the order $|X|$ of X as well as reasonable bounds for $|X|$. In this case we can make the list of all divisors d of $|X|$ and try all of them by checking whether $x^d = 1$; the minimal such d is, of course, the order of x. In the case of matrix groups $X \leqslant GL_n(\mathbb{F}_q)$ this means that we have to factorize $|GL_n(\mathbb{F}_q)|$ into primes, which is as hard as the general factorization problem [6].

In the present paper we do not need to find the exact orders of the elements. Instead, we work with a milder assumption that a computationally feasible global exponent E for X, that is, a reasonably sized natural number E such that $x^E = 1$ for all $x \in X$ is given as an input. We do not assume that we know the exact factorization of E into primes since then the orders of the elements can be computed. Note that having such an exponent for a black box group X, we can immediately determine, in certain cases, whether X is isomorphic to a known finite group G, for example, if we find an element $x \in X$ satisfying $x^{|G|} \neq 1$ then, clearly, $X \ncong G$. To check whether $x^{|G|} \neq 1$, we use square-and-multiply method, which involves only $O(\log |G|)$ multiplications in the group.

1.2. Random elements and product replacement algorithm

One of the biggest problems about black box groups is to construct uniformly distributed random elements in the group. The commonly used solution is the "the product replacement algorithm" [30]. Let $\Gamma_k(G)$ be the graph whose vertices are generating k-tuples of

elements in G and edges are given by the following transformations:

$$\begin{aligned}(g_1,\dots,g_i,\dots,g_k) &\rightarrow (g_1,\dots,g_i\cdot g_j^{\pm 1},\dots,g_k)\\ (g_1,\dots,g_i,\dots,g_k) &\rightarrow (g_1,\dots,g_j^{\pm 1}\cdot g_i,\dots,g_k)\end{aligned}$$

Note that $i \neq j$ above, and therefore these transformations map a generating k-tuple to generating k-tuple. A 'random' element in G can be produced by applying these transformations randomly and returning a random component of the resulting generating k-tuple. The connectivity of the graph $\Gamma_k(G)$ and the mixing time of this algorithm are the central issues to construct random elements in this way, see [65] for a detailed discussion.

The mixing time for a random walk on a graph Γ is, basically, the minimal number of steps such that after these steps the distribution of the end points of the random walk on Γ is close to the uniform distribution. It is proved in [64] that the mixing time for a random walk on $\Gamma_k(G)$ is polynomial in k and $\log|G|$ when k is sufficiently large. Indeed, when $k = \Theta(\log|G|\log\log|G|)$ the mixing time of the walk is $O(\log^9|G|(\log\log|G|)^5)$. An important observation by Lubotzky and Pak on the free groups F_k gives a much better bound for the mixing time.

Theorem 1.1 [59] *If $Aut(F_k)$ has Kazhdan's property (T), then for every finite group G generated by k elements the mixing time of a random walk on $\Gamma_k(G)$ is bounded by $c(k)\log|G|$ where $c(k)$ is a constant depending only on k.*

Hence the problem is reduced to the following conjecture.

Conjecture 1.2 *$Aut(F_k)$ satisfies Kazhdan's (T) property for $k \geqslant 4$.*

A topological group G is said to have Kazhdan's (T) property, if there is a compact subset $Q \subset G$ such that

$$\inf_{\rho}\inf_{v\neq 0}\max_{q\in Q}\frac{||\rho(q)(v)-v||}{||v||} > 0$$

where ρ runs over all unitary representations of G without fixed non-zero vectors. In the case of $Aut(F_k)$, we have discrete topology and compact subsets of $Aut(F_k)$ are precisely the finite subsets.

Observe that the graph $\Gamma_k(G)$ is not always connected, for example, if $G = \mathbb{Z}_p\times\cdots\times\mathbb{Z}_p$ (k-times), then $\Gamma_k(G)$ has $p-1$ components of equal size, see [35]. Although $\Gamma_k(G)$ is

not always connected, there are positive answers when k is big enough, for example, it is easy to see that if we take $k \geqslant d(G) + \bar{d}(G)$, where $d(G)$ is the minimal number of generators for G and $\bar{d}(G)$ is the maximal size of the minimal generating set for G, then $\Gamma_k(G)$ becomes a connected graph, see [65, Proposition 2.2.2]. However, it is still unknown for a finite simple group G, whether $\Gamma_k(G)$ is connected for $k \geqslant 3$ or not. Note that $d(G) \leqslant 2$ for finite simple groups. Pak proved in [65] that, for a fixed $k \geqslant 3$, there are large connected components for large simple groups G, that is, there exist connected components $\Gamma'_k(G) \subset \Gamma_k(G)$ such that

$$\frac{|\Gamma'_k(G)|}{|\Gamma_k(G)|} \to 1 \quad \text{as} \quad |G| \to \infty.$$

The product replacement algorithm was implemented in GAP and it has very successful practical performance, see [30] for more details.

On the theoretical side, Babai proposed an algorithm which constructs *nearly* uniformly distributed elements [4]. This algorithm first constructs a new generating set of $O(\log|G|)$ elements in $O(\log^5|G|)$ multiplications and then uses this set to produce sequence of nearly uniformly distributed elements in $O(\log|G|)$ multiplications for each element. The main drawback of this algorithm is that $O(\log^5|G|)$ number of steps needed in the preprocessing step which is not suitable for practical purposes. Here an algorithm outputs nearly uniformly distributed elements if it produces each group element with probability $(1 \pm \varepsilon)/|G|$ where $\varepsilon \leqslant 1/2$.

1.3. Three types of problems

There are basically three types of recognition algorithms for a given black box group X:

- *Verification problem:* Determine whether $X \cong G$ for a known finite group G.
- *Probabilistic recognition:* Determine the isomorphism type of X with given degree of certainty.
- *Constructive recognition:* Constructs an isomorphism $X \to G$ to a known group G.

1.3.1. Verification problem

One of the simplest ways to test whether a black box group X is isomorphic to a given group G is to look for an element of order not present in G. If such an element is found,

then we definitely know that $X \ncong G$. These computations can be carried out, in general, by working with global exponents, that is, if we can find an element $x \in X$ such that $x^E \neq 1$ where E be a global exponent for G, then we deduce that $X \ncong G$. This type of computations will be used frequently to determine the isomorphism type of a given classical group, see Section 5.3.

As pointed out in [18, Section 1.3] we shall discuss the similarity between the use of involutions in the verification problems and the classical Miller–Rabin primality test [68], see also [52, Section V.1], which is based on the fact that a number n is prime if and only if $(\mathbb{Z}/n\mathbb{Z})^*$ is the cyclic group of order $n-1$. Let $X = (\mathbb{Z}/n\mathbb{Z})^*$ be a black box group. To produce random uniformly distributed independent elements from X we use standard random number generators. Now we want to determine whether $X \cong \mathbb{Z}_{n-1}$. Notice that the group $\mathbb{Z}_{n-1}$ contains only one involution. On the other hand, if $n = p_1^{l_1} \cdots p_k^{l_k}$ is the prime factorisation of n then

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p_1^{l_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{l_k}\mathbb{Z})^*,$$

and by using the Chinese Remainder Theorem we can lift the involutions $-1 \bmod p_i^{l_i}$ to involutions in $(\mathbb{Z}/n\mathbb{Z})^*$ which shows that the involutions in $(\mathbb{Z}/n\mathbb{Z})^*$ generate an elementary abelian subgroup of order 2^k.

By using $E = n-1$ as a global exponent for X we can easily compute involutions in $\mathbb{Z}_{n-1}$. Indeed, we can factorise $n-1$ into a power of 2 and an odd factor: $n-1 = 2^l \cdot m$, m odd. Obviously, at least half of the elements in $\mathbb{Z}_{n-1}$ are of even order, so, with probability at least $1/2$, x^m is a non-trivial 2-element. The last non-identity element in the sequence of squares

$$x^m, (x^m)^2, \ldots, (x^m)^{2^l}$$

has order 2; we denote it $\mathrm{i}(x)$ and call the *involution produced by* x. For the sake of completeness of this definition, we set $\mathrm{i}(x) = 1$ if x is of odd order.

If $(\mathbb{Z}/n\mathbb{Z})^* \ncong \mathbb{Z}_{n-1}$, this procedure is likely to fail due to the fact that, for most integers n, $(x^m)^{2^l} \neq 1 \bmod n$ with probability at least $1/2$. In the worst case scenario, that is, when n is a so-called *Carmichael* number, the probability of producing ± 1 can be shown to be less than $\frac{1}{2^{k-1}} \leqslant \frac{1}{2}$. Hence we come to the following formulation of the Miller-Rabin primality test.

REPEAT for random $x \in (\mathbb{Z}/n\mathbb{Z})^*$:

- COMPUTE $\mathrm{i}(x)$.
- IF the computation of $\mathrm{i}(x)$ fails or $\mathrm{i}(x) \neq \pm 1$, RETURN

  n is not prime
- IF $\mathrm{i}(x) = \pm 1$ for l random values of x, RETURN

  n is prime with probability of error $\leqslant \frac{1}{2^l}$.

1.3.2. Probabilistic recognition

The major breakthrough result in recognition algorithms for matrix groups was presented by Neumann and Praeger in [61]. Their algorithm decides whether given a set of invertible $n \times n$ matrices over $\mathbb{F}_q$ generates a subgroup containing $\mathrm{SL}_n(q)$. The algorithm seeks elements having certain special properties where $\mathrm{SL}_n(q)$ has large proportion of such elements. By using the classification of the maximal subgroups of $\mathrm{GL}_n(q)$ [3], it can be deduced that few subgroups of $\mathrm{GL}_n(q)$ which do not contain $\mathrm{SL}_n(q)$ have such elements and these subgroups can be recognized by special routines. This is a Monte-Carlo algorithm and the answer "X contains $\mathrm{SL}_n(q)$" is always correct. Later, this idea is extended to all classical groups in their natural representation [28, 62]. A uniform approach in recognition of all black box finite simple groups of Lie type is given in [9] by using an order oracle. This algorithm produces sufficiently many uniformly distributed elements and examines the divisibility of the orders of these elements by certain prime divisors. This idea allows to identify all Lie type groups except for the groups $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$, q odd, since these two groups have virtually the same statistics of elements orders especially over large fields. The algorithm distinguishing $\mathrm{PSp}_{2n}(q)$ from $\Omega_{2n+1}(q)$, $n \geqslant 3$, is given in [1], and its idea is based on the structure of centralizers of involutions and the conjugacy classes of involutions in these groups. Hence

Theorem 1.3 [1, 9] *There is a polynomial-time Monte Carlo algorithm which, when given a black-box group $X = \langle S \rangle$ known to be isomorphic to a finite simple group of Lie type in given characteristic p, finds the standard name of X.*

The assumption that we know the characteristic of the underlying field can be avoided by using the algorithm in [50], see also [56].

A natural next step is to identify a black box group which is not known to be simple or not in advance, in other words, to determine whether the input group X is simple or not. Babai and Shalev developed an algorithm for black box groups of characteristic p which reduces the problem in Monte–Carlo polynomial time to the determination of whether the maximal normal p-subgroup $O_p(X)$ (or "p-core") is trivial or not [11]. They also present an algorithm solving this problem in the class of groups X where $X/O_p(X)$ is a *unisingular simple groups of Lie type of characteristic p.* A group X is called *unisingular* in characteristic p if every non-trivial module M of characteristic p has the property that every element of X has a non-zero fixed point in its action on M. It turns out that random search works pretty well to find a p-element in the class of groups X where $X/O_p(X)$ is a unisingular group of Lie type of characteristic p [11]. The simple unisingular groups of Lie type are classified in [46].

Let $\varepsilon = \pm 1$ and (P)$\mathrm{SL}_n^{\varepsilon}(q)$ denote the groups $\mathrm{PSL}_n(q)$ if $\varepsilon = +1$, and (P)$\mathrm{SU}_n(q)$ if $\varepsilon = -1$. Similarly, let $E_6^{\varepsilon}(q)$ denote $E_6(q)$ if $\varepsilon = +1$, and ${}^2E_6(q)$ if $\varepsilon = -1$.

Theorem 1.4 [46] *Let G be a finite simple group of Lie type of characteristic p defined over the field $GF(q)$, where $q = p^k$ for some $k \geqslant 1$. Then G is unisingular if and only if G is one of the following:*

1. $\mathrm{PSL}_n^{\varepsilon}(p)$ *with* $n|(p-\varepsilon)$;
2. $\Omega_{2n+1}(p)$, $\mathrm{PSp}_{2n}(p)$ *with p odd;*
3. $\mathrm{P}\Omega_{2n}^{\varepsilon}(p)$ *with p odd and* $\varepsilon = (-1)^{n(p-1)/2}$;
4. ${}^2G_2(q)$, $F_4(q)$, ${}^2F_4(q)$, $E_8(q)$ *with q arbitrary;*
5. $G_2(q)$ *with q odd;*
6. $E_6^{\varepsilon}(p)$ *with* $3|(p-\varepsilon)$;
7. $E_7(p)$ *with p odd.*

A polynomial time algorithm for the determination of $O_p(X) \neq 1$ for the groups of Lie type of odd characteristic is announced independently by Borovik [18], and Parker and Wilson [66]. We present this algorithm for classical groups of odd characteristic in this paper.

1.3.3. Constructive recognition

The constructive recognition algorithms for the simple groups are essential in the matrix group recognition project. A simple black box group $X = \langle S \rangle$ is said to be *constructively recognizable* if there exists an algorithm (Monte–Carlo or Las Vegas) for the following tasks:

1. Find the isomorphism type of X.
2. Find a new set S^* such that $X = \langle S^* \rangle$ and an explicit isomorhism $\varphi : X \to G$ specified by the image of S^* where G is the standard copy of X.
3. For any $x \in X$, express x as a word in S^*.
4. Given $g \in G$, express g as word in $\varphi(S^*)$.

An example of a constructive recognition algorithm for the group $G = \mathrm{SL}_n(q)$ is presented in [29] where the algorithm uses the fact that group is given in its natural representation, that is, generators of the group are given as invertable $n \times n$ matrices of determinant 1 over a field of size q. Its main idea follows the argument that $\mathrm{SL}_n(q)$ is generated by transvections, (or "unipotent elements"), and the algorithm first constructs a transvection and then conjugating it suitably to obtain a set of transvections which generate G. A black box group algorithm which recognizes $\mathrm{GL}_n(2)$ constructively is presented in [33]. Following this algorithm Kantor and Seress developed constructive black-box group algorithms of all classical groups [49], but these algorithms are not polynomial time algorithms in the input length, they are polynomial in q but the input size involves only $\log q$. They depend on the construction of unipotent elements found after a random search in the group. However the share of p'-elements (or "semisimple elements") in a simple group of Lie type defined over a field $\mathbb{F}_q$ is $1-O(1/q)$ [45]. Therefore the probability of a random element to be semisimple is close to 1 when the order of the field is *large*, in other words, it is unrealistic to expect producing unipotent elements over large fields by random search. Later the algorithms in [49] were upgraded to polynomial time constructive recognition algorithms [22, 23, 24] by assuming additional oracles: discrete logarithm oracle in $\mathbb{F}_q^*$ and $\mathrm{SL}_2(q)$-oracle. An $\mathrm{SL}_2(q)$-*oracle* is a deterministic algorithm which computes an explicit isomorphism between $\mathrm{SL}_2(q)$ and a black box group isomorphic to $\mathrm{SL}_2(q)$, in other words, it is a procedure for the constructive recognition of $\mathrm{SL}_2(q)$. Hence the constructive recognition algorithm for a finite simple group of Lie

type is reduced to the constructive recognition of (P)$\mathrm{SL}_2(q)$. In the matrix group case, there is a polynomial time constructive recognition algorithm for $\mathrm{SL}_2(q)$ based on discrete logarithm oracle for $\mathbb{F}_q^*$ [31, 32] which completes the constructive recognition of classical groups. In the case of a black box group, the polynomial-time constructive recognition algorithm for classical groups still represents a hard problem.

The first constructive recognition algorithm for the black box groups Sym_n and Alt_n appeared in [20] where the case $X \cong \mathrm{Sym}_n$ is described and the modifications for the case $X \cong \mathrm{Alt}_n$ is sketched. The algorithm presented in [14] completes the above procedures, in full details, for the constructive recognition of Sym_n and Alt_n. As it is quite elementary, we present a constructive recognition algorithm for $X \cong \mathrm{Sym}_k$ in [20] as an example, where $k = 2n$ for some n, the case $k = 2n + 1$ is similar. The algorithm uses Goldbach Conjecture which has been confirmed for the numbers $\leqslant 10^{14}$.

1. Find an element $x \in X$ of order p_1p_2 where $p_1 + p_2 = n$ and p_1, p_2 are distinct primes. Then we can assume that $y_1 = x^{p_2} = (1, 2, \ldots, p_1)$ and $y_2 = x^{p_1} = (p_1 + 1, p_1 + 2, \ldots, n)$.

2. Find an element $y \in X$ of order $2q_1q_2$ where q_1 and q_2 are odd primes, and $q_1 + q_2 = n - 2$. Then $t = y^{q_1 q_2}$ is a transposition.

3. Check whether $ty_1 \neq y_1t$ and $ty_2 \neq y_2t$. If not, repeat Step 2. Such a transposition interchanges a point from the cycle y_1 and a point from the cycle y_2, so we can assume that $t = (p_1, p_1 + 1)$.

4. Notice that the element $s = y_1ty_2$ is an n-cylce, and we compute the transposition $t_1 = t^{s^{p_1-1}}$. Hence there is a homomorhism $\varphi : X \to \mathrm{Sym}_n$ sending $s \mapsto (1, 2, \ldots, n)$ and $t_1 \mapsto (1, 2)$.

5. Compute $t_j = t_{j-1}^s$, $j = 2, 3, \ldots, n - 1$ and $t_n = t_{n-1}^s$. We have $\varphi(t_j) = (j, j + 1)$, $j = 2, 3, \ldots n - 1$ and $\varphi(t_n) = (n, 1)$.

6. Identifying $t_1 \sim (1, 2)$ and $s \sim (1, 2, \ldots, n)$ under φ, determine the action of an arbitrary element $x \in X$ on the set $\{1, 2, \ldots, n\}$ in the following way: Compute $t_1^x = (x(1), x(2))$ and determine which of the elements t_j commutes with the set $\{x(1), x(2)\}$. Similarly, compute

$$\{x(2), x(3)\}, \{x(3), x(4)\}, \ldots, \{x(n), x(1)\}.$$

Notice that each two consecutive sets above have a common element. Hence $x(j)$ is determined for all $j = 1, 2, \ldots, n$.

2. A uniform approach to recognition of black box groups of odd characteristic

As discussed in the previous section, the existing constructive recognition algorithms for black box classical groups depend on the discrete logarithm problem and the consructive recognition of $\mathrm{SL}_2(q)$ which is based on a construction of a unipotent element. The distribution of unipotent elements is close to 0 over large fields and it is not known a way to construct a unipotent element over large fields except from random search. Following this observation, we will present an alternative uniform approach for recognizing the simple groups of Lie type of odd characteristic which follows the computational version of the classification of the finite simple groups. Similar to the inductive argument on centralizers of involutions which plays a crucial role in the classification project, our approach is based on a recursive construction of the centralizers of involutions in black box groups [18, 21].

We propose the following plan for the recognition of the black box finite simple groups of Lie type of known odd characteristic.

- Construct all root $\mathrm{SL}_2(q)$-subgroups in a given simple black box group of Lie type of odd characteristic G corresponding to the nodes in the extended Dynkin diagram of the corresponding algebraic group.

Observe that this procedure determines the isomorphism type of G uniquely, indeed these groups are the root $\mathrm{SL}_2(q)$-subgroups in the Curtis–Phan–Tits presentation [34, 67, 73]. Fixing a Dynkin diagram of a simple algebraic group, the root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes of the Dynkin diagram in the untwisted groups of Lie type form the Curtis–Tits system while in the twisted case they form the Phan's system. For example, in the case of the Dynkin diagram of type A_{n-1}, the corresponding untwisted and twisted simple groups of Lie types are $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$ respectively and the root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes of the Dynkin diagram are $K_i = \mathrm{SL}_2(q)$, $i = 1, 2, \ldots, n-1$. In the Curtis-Tits system for $\mathrm{PSL}_n(q)$, the subgroups K_i satisfy $\langle K_i, K_{i+1}\rangle = \mathrm{SL}_3(q)$ and K_i commutes elementwise with K_j for $|i-j| \geqslant 2$ whereas in the Phan system for $\mathrm{PSU}_n(q)$ we have $\langle K_i, K_{i+1}\rangle = \mathrm{SU}_3(q)$ and again K_i commutes

elementwise with K_j for $|i-j| \geqslant 2$, see Section 3.3 for the precise formulization.

Although this procedure is not a constructive recognition of G, it allows us to construct all *subsystem subgroups* of G which can be read from the extended Dynkin diagram. To define a subsystem subgroup for the finite groups of Lie type and make the arguments uniform, we introduce the following definition. Let G be a untwisted group of Lie type of rank n, then we call a maximal split torus, which is of order $(q-1)^n$, a *maximal standard torus*. For the twisted groups, except for $\mathrm{P}\Omega^-_{2n}(q)$, n even, and ${}^3D_4(q)$, we define a maximal standard torus as a maximal torus of order $(q+1)^n$ where n is the Lie rank of the corresponding simple algebraic group. For $G = \mathrm{P}\Omega^-_{2n}(q)$, n even, or ${}^3D_4(q)$, tori of orders $(q+1)^{n-1}(q-1)$ or $(q-1)(q^3-1)$ will be called maximal standard tori of G respectively. Except for Suzuki-Ree groups, a "subsystem subgroup" of a finite simple group G of Lie type is a quasi-simple subgroup of G normalized by a maximal standard torus. In this setting, the long root $\mathrm{SL}_2(q)$-subgroups are subsystem subgroups of finite simple groups of Lie type of odd characteristic.

Note that this procedure is a computational version of Aschbacher's "Classical Involution Theorem" [2]. Aschbacher's characterization of Chevalley groups over fields of odd order is based on the study of "2-components" in the centralizers of involutions. Recall that a 2-*component* of a group G is a perfect subnormal subgroup L such that $L/O(L)$ is quasi-simple where $O(L)$ is the maximal normal subgroup of L of odd order and *solvable* 2-*component* of G is a subnormal subgroup L of G with $O(L) = O(G)$ and $L/O(L) = (\mathrm{P})\mathrm{SL}_2(3)$. Aschbacher's Classical Involution Theorem reads:

> *Let G be a finite group the generalized Fitting subgroup $F^*(G)$ simple. Let z be an involution in G and K a 2-component or solvable 2-component of $C_G(z)$ of 2-rank 1 containing z. Then $F^*(G)$ is a Chevalley group of odd characteristic or the Mathieu group M_{11}.*

The involutions satisfying the hypothesis of the above theorem are called *classical involutions*. It turns out that the classical involutions in a finite quasi-simple group of Lie type of odd characteristic are the involutions which belong to the long root $\mathrm{SL}_2(q)$-subgroups (see Theroem 3.3). Taking the "Classical Involution Theorem" as a model, we extend our setting to the black box groups X where $X/O_p(X)$ is a finite simple group of Lie type of odd characteristic p. Observe that an involution $i \in X$ belongs to a 2-component or solvable 2-component of $C_X(i)$ of 2-rank 1 if and only if $\bar{i} \in X/O_p(X)$ belongs to a 2-component or solvable 2-component of $C_{X/O_p(X)}(\bar{i})$ of 2-rank 1 since p is odd. Hence

Aschbacher's characterization fits into this setting, and we propose the following project for the recognition of black box group X where $X/O_p(X)$ is a finite simple group of Lie type of known odd characteristic p.

Procedure 1: Construct a subgroup K where $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$.

Procedure 2: Determine whether $O_p(X) \neq 1$.

Procedure 3: Construct all subgroups K where $K/O_p(K)$ are root $\mathrm{SL}_2(q)$-subgroups in $X/O_p(X)$ corresponding to the nodes in the extended Dynkin diagram of the corresponding algebraic group.

3. Structure of groups of Lie type

In this section we summarize the basic properties of the finite groups of Lie type which are needed in our algorithms, standard references are [26, 27, 71]. We use the following notation. Let $\bar{G}$ denote a connected simple algebraic group over an algebrically closed field of characteristic p, $\bar{T}$ a maximal torus of $\bar{G}$, $\bar{\Sigma}$ a $\bar{T}$-root system, $\bar{B}$ a Borel subgroup containing $\bar{T}$, $\bar{N} = N_{\bar{G}}(\bar{T})$ and $W = \bar{N}/\bar{T}$ the Weyl group of $\bar{G}$. Let σ be a Frobenious endomorphism of $\bar{G}$, then the fixed point set, $\bar{G}_\sigma$, is finite and let $G = O^{p'}(\bar{G}_\sigma)$, normal subgroup of $\bar{G}_\sigma$ generated by the p-elements of $\bar{G}_\sigma$. We also assume that the characteristic p of the underlying field is odd.

If G is untwisted, then we denote G by $\mathrm{PSL}_n(q)$, $\mathrm{P\Omega}_{2n+1}(q)$, $\mathrm{PSp}_{2n}(q)$, $\mathrm{P\Omega}^+_{2n}(q)$, $G_2(q)$, $F_4(q)$ and $E_n(q)$ for $n = 6, 7, 8$ where q is the order of the underlying field. For the twisted groups, we write $\mathrm{PSU}_n(q)$, $\mathrm{P\Omega}^-_{2n}(q)$, ${}^2E_6(q)$ where the Frobenious endomorphism of the corresponding simple algebraic group induces a field automorphism of order 2 on $\mathbb{F}_{q^2}$ and similarly we write $G = {}^3D_4(q)$ where we have a field automorphism of order 3 on $\mathbb{F}_{q^3}$. We say that G is defined over a field of order q. It turns out that, except for the Suzuki-Ree groups ${}^2B_2(2^{a+1/2})$, ${}^2F_4(2^{a+1/2})$, ${}^2G_2(3^{a+1/2})$, q is the order of the center of a long root subgroup.

3.1. Maximal Tori

It is well known that there exist a maximal torus $\bar{T}$ and Borel subgroup $\bar{B}$ of $\bar{G}$ which are σ-invariant and $\bar{T} \leqslant \bar{B}$. Moreover $\bar{G}_\sigma$ permutes transitively the set of all such pairs

$(\bar{T}, \bar{B})$. The subgroups of the form $G \cap \bar{T}$ for some σ-invariant maximal torus $\bar{T}$ of $\bar{G}$ is called a *maximal torus* of G.

Recall that $H^1(\sigma, G)$ is the set of equivalence classes of G under the relation $\sim_\sigma$ defined by

$$x \sim_\sigma y \text{ if and only if } y = gxg^{-\sigma} \text{ for some } g \in G. \tag{3.1}$$

If $x \sim_\sigma y$, then x and y are called σ-conjugate.

Theorem 3.1 ([27, Proposition 3.3.3]) *The set of G-orbits on the set of σ-invariant maximal tori of $\bar{G}$ is in bijective correspondence with $H^1(\sigma, W)$.*

Note that if σ fixes each element of W, which is the case if G is untwisted, then $H^1(\sigma, W)$ corresponds to the set of conjugacy classes of W.

Let S be the set of representatives of G-orbits on the set of σ-invariant maximal tori of $\bar{G}$. Then $S \cap G$ is the set of representatives of maximal tori of G whose elements correspond to elements $w \in W$ and they will be denoted by T_w. We will call these tori maximal tori of G *twisted* by w. Note that if $w \sim_\sigma w'$ in the sense of Equation 3.1, then T_w and $T_{w'}$ are G-conjugate.

The following lemma is crucial in our algorithms.

Theorem 3.2 ([27, Proposition 3.3.5, 3.3.6]) *Let $\bar{G}$ be a simple algebraic group and $\bar{T}$ be a σ-invariant maximal torus of $\bar{G}$ such that $\bar{T}_\sigma$ corresponds to an element $w \in W$. If q is the number of elements of the base field on which G is defined, then the characteristic polynomial of w evaluated at q gives the order of $\bar{T}_\sigma$. Moreover $|\bar{N}_\sigma / \bar{T}_\sigma| \cong |C_W(w)|$ where $\bar{N} = N_{\bar{G}}(\bar{T})$.*

The characteristic polynomials of $w \in W$ are given in [25] (see also Section 8 in [33]) and we give here the orders of maximal tori in classical groups.

- $G = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$: Provided that $l_1 + \cdots + l_k = n$, the orders of the maximal tori in G are of the form

$$(q^{l_1} - \varepsilon^{l_1})(q^{l_2} - \varepsilon^{l_2}) \cdots (q^{l_k} - \varepsilon^{l_k})/(q - \varepsilon).$$

  Here $\varepsilon = 1$ if $G = \mathrm{SL}_{n+1}(q)$ and $\varepsilon = -1$ if $G = \mathrm{SU}_{n+1}(q)$.

- $G = \mathrm{Spin}_{2n+1}(q)$ or $\mathrm{Sp}_{2n}(q)$: The orders of the tori in G are of the form

$$(q^{l_1} - 1) \cdots (q^{l_r} - 1)(q^{m_1} + 1) \cdots (q^{m_s} + 1)$$

  where $(l_1 + \cdots + l_r) + (m_1 + \cdots + m_s) = n$.

- $G = \mathrm{Spin}^{\pm}_{2n}(q)$: The orders of the tori in G are of the form

$$(q^{l_1} - 1) \cdots (q^{l_r} - 1)(q^{m_1} + 1) \cdots (q^{m_s} + 1)$$

  where $(l_1 + \cdots + l_r) + (m_1 + \cdots + m_s) = n$. If $G = \mathrm{Spin}^{+}_{2n}(q)$ then s is an even integer and if $G = \mathrm{Spin}^{-}_{2n}(q)$ then s is an odd integer.

In the case of $\mathrm{SL}_n(q)$, the Weyl group W is isomorphic to Sym_n and a maximal torus of order $(q^{l_1}-1)\cdots(q^{l_k}-1)/(q-1)$ corresponds to an element $w \in W$ where $w = w_1 \cdots w_k$ is the cycle decomposition of w and the cycles w_i have lengths l_i for each $i = 1, \ldots, k$. In particular, if a maximal torus T corresponds to a n-cycle in W, then T is a cyclic group of order $q^n - 1/q - 1$ and the probability of producing a semisimple element in G which is conjugate to an element in T is at least

$$\frac{|G|}{|N_G(T)|}\frac{|T|}{|G|} = \frac{1}{|C_W(w)|} = \frac{1}{n}.$$

3.2. Properties of root $\mathrm{SL}_2(q)$-subgroups

Let T be a maximal torus of G where $T = \bar{T}_\sigma$. For each root $r \in \bar{\Sigma}$, there exists a $\bar{T}$-root subgroup U_r of $\bar{G}$ and these root subgroups are permuted by σ. Let Δ be a $\langle\sigma\rangle$-orbit of a root subgroup of $\bar{G}$, then the subgroup $O^{p'}(\langle\Delta\rangle_\sigma)$ is called a T-root subgroup of G. The properties of T-root subgroups are studied thoroughly in [69]. Here we take a torus $\bar{T}$ which is a σ-invariant maximal torus contained in a σ-invariant Borel subgroup of $\bar{G}$. These T-root subgroups of G correspond to the roots in the root system Σ of G, see [38, Section 2.3] for the construction of root systems for the finite groups of Lie type, and G is generated by these root subgroups X_r, $r \in \Sigma$. A root subgroup is called a long or short root subgroup if the corresponding root is long or short respectively. The structure of root subgroups in G is summarized in Table 1.

In this setting the root subgroups are not always abelian in finite simple groups of Lie type. Let $M_i = \langle X_{r_i}, X_{-r_i}\rangle$, $Z_i = Z(X_{r_i})$ and $K_i = \langle Z_i, Z_{-i}\rangle$ where $r_i \in \Sigma$. Then X_{r_i} is

Table 1. The structure of root subgroups in G [38, Table 2.4]. Here E_{q^i} is an elementary abelian p-group of order q^i.

Type	r	Remarks
Untwisted	both	$X_r \cong E_q$
Twisted except $\mathrm{PSU}_{2n+1}(q)$	long	$X_r \cong E_q$
Twisted except ${}^3D_4(q)$	short	$X_r \cong E_{q^2}$
${}^3D_4(q)$	short	$X_r \cong E_{q^3}$
$\mathrm{PSU}_{2n+1}(q)$	long	$\lvert X_r\rvert = q^3$ and $Z(X_r) \cong E_q$
${}^2G_2(q)$		$\lvert X_r\rvert = q^6$ and $Z(X_r) \cong E_{q^2}$

a Sylow p-subgroup of M_i and Z_i is a Sylow p-subgroup of K_i. Moreover $X_{r_i} \cong Z_i \cong E_q$ and $K_i \cong M_i \cong \mathrm{SL}_2(q)$ except for the groups given in Table 2.

The subgroup K_i is called long or short root $\mathrm{SL}_2(q)$-subgroup if the corresponding root $r_i \in \Sigma$ is a long or short root respectively.

Table 2. Short root $\mathrm{SL}_2(q)$-subgroups in G [2, Table 14.4].

	$G(q)$	r	K_r	M_r
	$\mathrm{PSU}_{2n+1}(q)$	long	$\mathrm{SL}_2(q)$	$\mathrm{PSU}_3(q)$
	$\mathrm{PSU}_n(q)$	short	$\mathrm{PSL}_2(q^2)$	$\mathrm{PSL}_2(q^2)$
r	$\Omega_{2n+1}(q)$	short	$\mathrm{PSL}_2(q)$	$\mathrm{PSL}_2(q)$
	$\mathrm{P}\Omega^-_{2n}(q)$	short	$\mathrm{PSL}_2(q^2)$	$\mathrm{PSL}_2(q^2)$
	${}^2E_6(q)$	short	$\mathrm{SL}_2(q^2)$	$\mathrm{SL}_2(q^2)$
	${}^3D_4(q)$	short	$\mathrm{SL}_2(q^3)$	$\mathrm{SL}_2(q^3)$

We have the following fundamental theorem for long root $\mathrm{SL}_2(q)$-subgroups in simple groups of Lie type of odd characteristic.

Theorem 3.3 ([2, Theorem 14.5]) *Let G be a finite simple group of Lie type defined over a field of odd order q. With the notation as above, let r_i be a long root, $K = K_i$, and*

$\langle z \rangle = Z(K)$. *Then*

(1) $K \cong \mathrm{SL}_2(q)$.

(2) $O^{p'}(N_G(K)) = KL$ *where* $[K, L] = 1$ *and* L *is the Levi factor of the parabolic subgroup* $N_G(Z_i)$.

The following two lemmas are the key results to test whether a given subgroup isomorphic to $\mathrm{SL}_2(q)$ is a long root $\mathrm{SL}_2(q)$-subgroup in G.

Lemma 3.4 *Let* K *be a long root* $\mathrm{SL}_2(q)$*-subgroup of* G *and* $z \in Z(K)$. *Then* $K = K^g$ *for any* $g \in C_G(z)''$.

Lemma 3.5 [75] *Let* G *be a finite simple group of Lie type defined over a field of order* q *different from* ${}^3D_4(q)$ *and* $G_2(q)$. *Let* K *be a short root* $\mathrm{SL}_2(q)$*-subgroup of* G *and* $z \in K$ *be an involution. Then there exists* $g \in C_G(z)''$ *such that* $K \neq K^g$.

3.3. Curtis-Phan-Tits presentation

Finite groups of Lie type have a special presentation called the *Steinberg-presentation* [71] which is based on the relations on their root subgroups. Steinberg proved that if G is a finite group generated by the set $\{x_r(t) \mid r \in \Sigma,\, t \in \mathbb{F}_q\}$, where Σ is an irreducible root system of rank at least 2, subject to the relations

$$x_r(t+u) = x_r(t)x_r(u), \tag{3.2}$$

$$[x_r(t), x_s(u)] = \prod_{\substack{\gamma = ir + js,\ i,j \in \mathbb{N}^* \\ r,s \in \Sigma,\ r \neq \pm s}} x_\gamma(c_{i,j,r,s}t^i u^j), \tag{3.3}$$

$$h_r(t)h_r(u) = h_r(tu) \quad tu \neq 0, \tag{3.4}$$

where

$$h_r(t) = n_r(t)n_r(-1),$$
$$n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t),$$

then $G/Z(G)$ is a finite simple group of Lie type with root system Σ.

The analogue of the Steinberg presentation holds also for twisted groups of Lie type where the defining relations are much more sophisticated, a detailed discussion can be found in [38, Section 2.4, 2.9].

The following theorem (known as the Curtis-Tits presentation) shows that the essential relations in the Steinberg presentation are the ones involving rank 1-subgroups corresponding to fundamental roots in Σ. Note that, if G is untwisted, then we have

$$\langle X_r, X_{-r} \rangle \cong (\mathrm{P})\mathrm{SL}_2(q)$$

where $X_r = \langle x_r(t) \mid t \in \mathbb{F}_q \rangle$ for any $r \in \Sigma$. Note also that the nodes in the Dynkin diagram are labelled by the elements in Π. Therefore the Curtis-Tits presentation involves the pairs of fundamental roots which are edges or nonedges in the Dynkin diagram. More precisely;

Theorem 3.6 [72, Theorem 2] *Let Σ be an irreducible root system of rank at least 3 with fundamental system Π and Dynkin diagram Δ. Let G be a finite group and assume that the following are satisfied*

1. $G = \langle K_r \mid r \in \Pi \rangle$, $K_r = \langle X_r, X_{-r} \rangle = (\mathrm{P})\mathrm{SL}_2(q)$, *for all* $r \in \Pi$.
2. $H_r = N_{K_r}(X_r) \cap N_{K_r}(X_{-r}) \leqslant N_G(X_s)$ *for all* $r, s \in \Pi$.
3. $[K_r, K_s] = 1$ *if r and s are not connnected in Δ.*
4. $\langle K_r, K_s \rangle \cong (\mathrm{P})\mathrm{SL}_3(q)$ *if r and s are connected with a single bond.*
5. $\langle K_r, K_s \rangle \cong (\mathrm{P})\mathrm{Sp}_4(q)$ *if r and s are connected with a double bond.*

Then there exists a group of Lie type $\widetilde{G}$ with a root system Σ and a fundamental system Π, and a surjective homomorphism $\varphi : G \to \widetilde{G}$ mapping the $X_{\pm r}$ onto the corresponding fundamental root subgroups of $\widetilde{G}$. Moreover $\ker\varphi \leqslant Z(G) \cap H$ *where* $H = \langle H_r \mid r \in \Pi \rangle$.

Example 3.7 [71, p. 72] Let $G = \mathrm{SL}_n(q)$, $n \geqslant 3$ and $x_{ij}(t) = I + tE_{ij}$ where E_{ij} is the matrix whose (i, j)-entry is 1 and the others are 0. Then Steinberg-presentation of G is

$$G = \langle x_{ij}(t) \mid 1 \leqslant i, j \leqslant n,\ i \neq j,\ t \in \mathbb{F}_q \rangle$$

subject to the following relations

1. $x_{ij}(t+u) = x_{ij}(t)x_{ij}(u)$,
2. $[x_{ij}(t), x_{jk}(u)] = [x_{ik}(tu)]$ if i, j, k are different,
3. $[x_{ij}(t), x_{kl}(u)] = 1$ if $j \neq k$, $i \neq l$.

In the Curtis-Tits presentation of G we use only the generators $x_{ij}(t)$ where $\mid i-j \mid \leqslant 2$. Hence the number of relations is considerably less than the number of relations in Steinberg-presentation.

Phan proved similar results for the twisted groups of Lie type in [67]. Bennet and Shpectorov proved Phan's theorem with weaker assumptions for the groups $G = \mathrm{SU}_n(q)$:

Theorem 3.8 [17] *Let G be a finite group containing subgroups $K_i \cong \mathrm{SU}_2(q)$, $i = 1, 2, \ldots, n$ and $K_{i,j}$, $1 \leqslant i < j \leqslant n$, such that the following hold:*

1. *If $\mid i - j \mid > 1$ then $K_{i,j}$ is a central product of K_i and K_j.*
2. *For $i = 1, 2, \ldots, n-1$, K_i and K_{i+1} are contained in $K_{i,i+1}$ which is isomorphic to $\mathrm{SU}_3(q)$ or $\mathrm{PSU}_3(q)$. Moreover K_i and K_{i+1} are the stabilizers of a non-singular vector in $K_{i,i+1}$.*
3. *The subgroups $K_{i,j}$, $1 \leqslant i < j \leqslant n$, generate G.*

If $q > 3$, then G is isomorphic to a factor group of $\mathrm{SU}_{n+1}(q)$.

It is easy to see that the subgroups K_i, $i = 1, 2, \ldots, n$ in Theorem 3.8 play the role of the subgroups corresponding to the nodes in the Dynkin diagram of $\mathrm{PSL}_{n+1}(q)$ as in the Curtis-Tits presentation. Moreover each subgroup K_i is normalized by a maximal standard torus in G.

The relation between the Curtis-Tits theorem and Phan's theorems are discussed thoroughly in [16] and new Phan type presentation for the untwisted groups of Lie type has been constructed [39, 40, 41, 42].

Besides involving less relations than Steinberg presentation, the main advantage of Curtis-Tits presentation from the computational point of view is to allow us to work with the root $\mathrm{SL}_2(q)$-subgroups instead of unipotent elements. Recall that the existing constructive recognition of black box group algorithms are using either unipotent elements or the constructive recognition of the subgroups isomorphic to $\mathrm{SL}_2(q)$ which is only possible if one can construct unipotent elements. Recall also that the construction of

the unipotent elements over big fields is almost impossible by random search. Therefore the natural approach in the recognition of black box groups is to construct root $\mathrm{SL}_2(q)$-subgroups and check the relations between them, that is, the relations in the Curtis-Tits presentation.

3.4. The structure of the centralizers of involutions

The fundamental result on the structure of centralizers of involutions in Lie type groups of odd characteristic is the following result, see [38, Chapter 4] for a complete description.

Theorem 3.9 [38, Theorem 4.2.2] *Let G be a simple group of Lie type of odd characteristic p, $i \in G$ an involution, $C = C_G(i)$ and $L = O^{p'}(C)$. Then there exist a subgroup $T \leqslant C$ such that the following conditions satisfied.*

1. *L is a central product $L = L_1 \cdots L_s$ where $s \geqslant 0$ and L_k is a (quasi-)simple group of Lie type of characteristic p for each $k = 1, \ldots, s$.*
2. *T is an abelian p'-subgroup normalizing each L_k.*
3. *Setting $C^\circ = LT$, we have C/C° is an elementary abelian 2-subgroup.*

The subgroup $L = O^{p'}(C)$ will be called *semisimple socle* of $C_G(i)$. It follows immediately from Theorem 3.9 that the second derived subgroup $C_G(i)''$ is the semisimple socle of $C_G(i)$. Passsing to the groups with a non-trivial p-core we have the following.

Lemma 3.10 *Let X be a finite group where $X/O_p(X)$ is a finite simple group of Lie type over a field of odd size $q > 3$ and let $i \in X$ be an involution. Then $(C_X(i)/O_p(C_X(i)))''$ is the semisimple socle of $C_X(i)/O_p(C_X(i))$.*

It is worth to give the list of classical involutions and their centralizers, see Theorem 3.3; In Table 3, we write $G_1 \circ_n G_2$ which is meant to be $(G_1 \times G_2)/N$ for some cyclic group N of order n intersecting with G_1 and G_2 trivially. We write $\frac{1}{m}G$ to denote the quotient group G/Y where $Y \leqslant Z(G)$, $|Y| = m$ and $Z(G)$ is cyclic. Note that the center of $G = \mathrm{Spin}^+_{2n}(q)$, n even, is an elementary abelian group of order 4. Therefore $\frac{1}{2}\mathrm{Spin}^+_{2n}(q)$ is not uniquely defined for n even and we define it as follows. There is an involution $z \in Z(G)$ such that $G/\langle z\rangle \cong \mathrm{SO}^+_{2n}(q)$. For the other involutions z_1, $z_2 \in Z(G)\backslash\{z\}$, we have $G/\langle z_1\rangle \cong G/\langle z_2\rangle$ which is not isomorphic to $\mathrm{SO}^+_{2n}(q)$ and we denote these quotient

Table 3. The semisimple socles of the centralizers of the classical involutions.

G	$L = O^{p'}(C_G(i))$
$\mathrm{PSL}_n^{\varepsilon}(q)$	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_{n-2}^{\varepsilon}(q)$
$\mathrm{PSp}_{2n}(q)$	$\mathrm{SL}_2(q) \circ_2 \mathrm{Sp}_{2n-2}(q)$
$\Omega_{2n+1}(q)$	$(\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)) \circ_2 \Omega_{2n-3}(q)$
$\mathrm{P}\Omega_{2n}^{\varepsilon}(q)$	$(\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)) \circ_2 \Omega_{2n-4}^{\varepsilon}(q)$
$G_2(q)$	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$
${}^3D_4(q)$	$\mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$
$F_4(q)$	$\mathrm{SL}_2(q) \circ_2 \mathrm{Sp}_6(q)$
$E_6^{\varepsilon}(q)$	$\mathrm{SL}_2(q) \circ_2 \frac{1}{(q-\varepsilon,3)}\mathrm{SL}_6^{\varepsilon}(q)$
$E_7(q)$	$\mathrm{SL}_2(q) \circ_2 \frac{1}{2}\mathrm{Spin}_{12}^{+}(q)$
$E_8(q)$	$\mathrm{SL}_2(q) \circ_2 E_7(q)$

groups as $\frac{1}{2}\mathrm{Spin}_{2n}^{+}(q)$. Notice that $\frac{1}{2}\mathrm{Spin}_{12}^{+}(q)$ appears as the component in the centralizer of a classical involution in the groups $E_7(q)$.

4. Centralizers of involutions in black box groups

4.1. Construction of $C_G(i)$ in a black box group

Let X be a black box finite group and $E = 2^k m$ be an exponent for X with m odd. We shall first produce an involution from a random element $x \in X$. For this task, we need an element of even order and we follow the same argument as in Section 1.3.1.

A precise lower bound for the share of elements of even order in the groups of Lie type of odd characteristic is given by the following theorem:

Theorem 4.1 [47] *Let G be a finite group having a simple homomorphic image that is neither cyclic nor Lie type of characteristic 2. Then the share of elements having an even order is at least $1/4$.*

Let t be an involution and x a random element in X. Set $z = tt^x$.

- If the order m of z is odd, then consider $y = z^{(m+1)/2}$. Now observe that $yx^{-1} \in C_X(t)$ and denote $\zeta_1^t(x) = yx^{-1}$.

- If z is of even order, then $\mathrm{i}(z) \in C_X(i)$ where $\mathrm{i}(z)$ is the involution produced from z. Denote $\zeta_0^t(x) = \mathrm{i}(z)$.

Here the superscript ^{t} indicates the dependence of the map ζ_k, $k = 0, 1$, on the involution t.

Thus we have a map $\zeta^t = \zeta_0^t \sqcup \zeta_1^t$ defined by

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

Here $o(x)$ is the order of the element $x \in X$. Note that one can test whether an element $x \in X$ has odd or even order by raising it to the odd part m of the exponent E and compare it with 1. Moreover, if $o(x)$ is odd then $x^{(m+1)/2} = x^{(o(x)+1)/2}$. Therefore we can construct $\zeta_0^t(x)$ and $\zeta_1^t(x)$ without knowing the exact order of tt^x.

Observe that if $c \in C_X(t)$, then

$$\begin{array}{rcl} \zeta_1^t(cx) & = & (tt^{cx})^{(m+1)/2} \cdot x^{-1}c^{-1} = (tt^x)^{(m+1)/2} \cdot x^{-1}c^{-1} \\ & = & \zeta_1^t(x) \cdot c^{-1}, \\ \zeta_0^t(xc) & = & \mathrm{i}(t \cdot t^{xc}) = \mathrm{i}(t^c \cdot t^{xc}) = \mathrm{i}((t \cdot t^x)^c) = \mathrm{i}(tt^x)^c \\ & = & \zeta_0^t(x)^c. \end{array}$$

Therefore if the elements $x \in X$ are uniformly distributed and independent in X, then

- the distribution of the elements $\zeta_1^t(x)$ in $C_X(t)$ is invariant under the right multiplication of the elements in $C_X(t)$, in other words, if $S \subset C_X(t)$ and $c \in C_X(t)$, then
$$P(\zeta_1^t(x) \in S) = P(\zeta_1^t(x) \in Sc).$$

- the distribution of the elements $\zeta_0^t(x)$ in $C_X(t)$ is invariant under the conjugation action of $C_X(t)$ on itself, in other words
$$P(\zeta_0^t(x) \in S) = P(\zeta_0^t(x) \in S^c).$$

Hence we have the following important result for the construction of the centralizers of involutions in black box groups.

Theorem 4.2 [18] *Let X be a finite group and $t \in X$ be an involution. If the elements $x \in X$ are uniformly distributed and independent in X, then*

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

We will use both of the functions ζ_0^t and ζ_1^t in the recursive steps to generate $C_X(t)$. It follows directly from Theorem 4.2 that the image of the function ζ_1^t is $C_X(t)$ and the image of ζ_0^t generates a normal subgroup in $C_X(t)$.

4.2. The use of the maps ζ_0^i and ζ_1^i

If there is a good proportion of elements in a group G for which the map ζ_1^i is defined, then, following Theorem 4.2, the map ζ_1^i is an ideal black box in the construction of $C_G(i)$. The generation of finite (quasi)simple groups by random elements is studied in [36, 48, 57] and combining the results we have that randomly chosen two elements in a finite simple group G generate G with probability tends to 1 as the order of G tends to infinity.

In a finite simple group G of Lie type of odd characteristic, an estimate for the distribution of the elements $g \in G$ where ii^g has odd order for an involution $i \in G$ is announced indepently by Borovik [18] and Parker and Wilson [66].

Theorem 4.3 [18, 66] *Let G be a finite simple group of Lie type of odd characteristic and Lie rank n. If i is an involution in G, then the product ii^g has odd order with probability c/n for some positive constant c.*

It may happen, in some cases, that the map ζ_1 is not efficient to generate the centralizers of involutions. For example, let $Y = \mathrm{PSL}_2(q)$ and q is a big odd prime power, then random elements are regular semisimple with probability very close to 1, and hence belong to a cyclic torus of order $(q \pm 1)/2$. Note that one of the tori has even order and at least half of its elements have even order. Therefore the probability that the elements having even order in Y is close to $1/4$, see also Theorem 4.1. All involutions in Y are conjugate and the product of two random involutions is regular semisimple.

Therefore the product of two random involutions in Y has even order with probability close to $1/4$. Now let t be an involution in $X = Y \times \cdots \times Y$ (n times) acting non-trivially on each component, then one has to do these computations componentwise and therefore the product of two random involutions has odd order with probability close to $1/4^n$. This shows that when n is a big number, then the map ζ_1 is rarely defined for such involutions in which case the map ζ_0 is defined for almost all $x \in X$ and we use the map ζ_0. It turns out that, in a group of Lie type of odd characteristic, the image of the map ζ_0 generates sufficiently big subgroup for most of the purposes.

Let $i \in G$ be any fixed involution. We define

$$\heartsuit_i(G) = \langle \zeta_0^i(g) \mid g \in G \rangle.$$

We use here the convention that $\zeta_0^i(g) = 1$ if ii^g has odd order.

Theorem 4.4 [75] *Let G be a finite quasi-simple group of Lie type over a field of odd characteristic p and $i \in G$ be an involution.*

1. *If G is classical then $\heartsuit_i(G)$ contains the semisimple socle of $C_G(i)$ except for the groups $(\mathrm{P})\mathrm{Sp}_{2n}(q)$ and the classical involutions.*
2. *If G is exceptional then $\heartsuit_i(G)$ contains at least one component in $C_G(i)$.*

In the symplectic groups the description is as follows:

Lemma 4.5 [75] *Let $G = (\mathrm{P})\mathrm{Sp}_{2n}(q)$, $q > 3$ and i be a classical involution.*

1. *If $n \geqslant 3$, then $\heartsuit_i(G)' \cong \mathrm{Sp}_{2n-2}(q)$.*
2. *If $G = \mathrm{Sp}_4(q)$, then $\heartsuit_i(G) = Z(G)$.*
3. *If $G = \mathrm{PSp}_4(q)$, then $\heartsuit_i(G) \geqslant E(C_G(i))$ where $E(C_G(i))$ is the semisimple socle of $C_G(i)$.*

The proof of Theorem 4.4 follows mainly from the famous Glauberman Z^*-theorem [37]. We illustrate this result in the easiest case where the rest of the proof follows the same idea. Let $G = \mathrm{SL}_n(q)$ and $i = (-1, -1, 1, \ldots, 1) \in G$ be an involution. Then $C_G(i)' = \mathrm{SL}_2(q) \times \mathrm{SL}_{n-2}(q)$. It is easy to see that the involution $j = (1, -1, -1, 1, \ldots, 1)$ is conjugate to i, say $j = i^g$ for some $g \in G$, and $j \in C_G(i)$. Now $\zeta_0^i(g) = ii^g$ does

not centralize neither of the components in $C_G(i)'$ and hence $C_G(i)' \leqslant \heartsuit_i(G)$ since $\heartsuit_i(G) \trianglelefteq C_G(i)$.

The values of the map ζ_0^i belong to the union of the conjugacy classes of involutions in $C_G(i)$:

$$S = i_1^{\heartsuit_i(G)} \cup \cdots \cup i_k^{\heartsuit_i(G)}$$

with the probability distribution invariant under the conjugation from the elements in $C_G(i)$. If G is a finite simple group and S is a normal subset then a result of Liebeck and Shalev [58, Theorem 1.1] asserts that there exists a constant c such that $S^n = G$ for any $n \geqslant c \log |G| / \log |S|$. If G is a direct product of simple groups, then one has to take a normal subset which is a direct product of normal subsets in the components, and, by Theorem 4.4, we have a similar estimate for direct product of simple groups of Lie type of odd charactersitic.

5. The algorithms

In this section we present black box group algorithms for the groups X where $X/O_p(X)$ are simple groups of Lie type of odd characteristic p. If $X/O_p(X)$ is a quasi-simple group of Lie type with non-trivial center, then we can find $Z(X)$ by a Monte–Carlo polynomial time algorithm in [11]. Therefore our algorithms can be extended to the quasi-simple groups of Lie type over a field of odd order $q > 3$.

We first present an algorithm which constructs a long root $\mathrm{SL}_2(q)$-subgroup in a finite simple groups of Lie type of odd characteristic in Section 5.1. This algorithm can be easily extended to an algorithm for the groups with non-trivial p-core which constructs a subgroup $K \leqslant X$ such that $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$. Once we constructed such a subgroup, we reduce the problem of determining whether $O_p(X) \neq 1$ to this subgroup, and by using recursive arguments on the centralizers of classical involutions we decide whether $O_p(X) \neq 1$ in Section 5.2. The construction of a long root $\mathrm{SL}_2(q)$-subgroup in simple groups of Lie type of odd characteristic gives rise to a probabilistic recognition of classical groups and we present this algorithm in Section 5.3. Finally we discuss the construction of the Curtis-Tits system in simple groups of Lie type of odd characteristic in Section 5.4.

5.1. Construction of a long root $\mathrm{SL}_2(q)$-subgroup in simple groups of Lie type

In this section let G denote a finite simple group of Lie type of odd characteristic. Our aim is to present the following algorithm.

Algorithm 5.1 *"Construction of a long root* $\mathrm{SL}_2(q)$*-subgroup in a finite simple group of Lie type"*

> *Input: A black box group isomorphic to a finite simple group G of Lie type defined over a field of odd size $q > 3$ except* $\mathrm{PSL}_2(q)$ *and* ${}^2G_2(q)$.
>
> *Output: A black box subgroup $K \leqslant G$ which is a long root* $\mathrm{SL}_2(q)$*-subgroup in G.*

Note that if G is isomorphic to $\mathrm{PSL}_2(q)$ or ${}^2G_2(q)$, then there is no subgroup in G isomorphic to $\mathrm{SL}_2(q)$. Therefore it is natural to exclude these groups in Algorithm 5.1.

Let G be a group and $G_i \leqslant G$, $i = 1, \ldots, n$. Assume that

$$G = \langle G_i \mid i = 1, \ldots, n \rangle$$

and G_k commutes with G_l elementwise for any $k \neq l$. Then we say that G is *commuting products* of G_i for $i = 1, \ldots, n$.

We split Algorithm 5.1 into four pieces:

1. Construct commuting products of (P)$\mathrm{SL}_2(q)$ in G, say L.
2. Construct a component $K = \mathrm{SL}_2(q)$ in L. If $\mathrm{SL}_2(q)$ does not appear as a component in L, return to Step 1.
3. Find the size of the underlying field in K found in the previous step.
4. Check whether K is a long root $\mathrm{SL}_2(q)$ or not.

Note that the long root $\mathrm{SL}_2(q)$-subgroups in simple groups of Lie type of odd characteristic are indeedisomorphic to $\mathrm{SL}_2(q)$ by Theorem 3.3. Therefore if we have commuting products of $\mathrm{PSL}_2(q)$ in Step 2, then we conclude that the commuting products of $\mathrm{PSL}_2(q)$ do not contain a long root $\mathrm{SL}_2(q)$-subgroup as a component and we return to Step 1 for the construction of new commuting products of (P)$\mathrm{SL}_2(q)$.

In the case of black box groups X where $X/O_p(X)$ is isomorphic to a finite simple group over a field of odd size $q > 3$, the algorithm is as follows.

Algorithm 5.2 *"Main Algorithm"*

Input: A black box group X where $X/O_p(X)$ is isomorphic to a finite simple group over a field of odd size $q > 3$.

Output: A black box group K where $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$.

The structure of Algorithm 5.2 is exactly the same as the structure of Algorithm 5.1.

5.1.1. Constructing commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$

In this section we apply the results and the observations in Section 4.2 to present the following algorithm.

Algorithm 5.3 *"Construction of a commuting product of $(\mathrm{P})\mathrm{SL}_2(q)$-subgroups"*

Input: A black box group isomorphic to a finite simple group G of Lie type defined over a field of odd size q except $\mathrm{PSL}_2(q)$ and ${}^2G_2(q)$.

Output: A black box group which is commuting products of $(\mathrm{P})\mathrm{SL}_2(q^k)$ for various $k \geqslant 1$.

Observe that recursive construction of the semisimple socles of the centralizers of involutions in G ends with a commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ where q may vary. The computation goes as follows. We first produce a non-trivial involution $i = \mathrm{i}(g)$ from a random element $g \in G$ by using the arguments in Section 1.3.1. Then we construct a sufficiently large subset $S \subset G$ consisting of random elements and generate a subgroup of $C_G(i)$ by using the image of the map $\zeta^i = \zeta_0^i \sqcup \zeta_1^i$ on S. Note that if ζ_1^i is rarely defined for the subset S, then ζ_0^i is defined for almost all elements in S. The image of ζ_0^i generate a subgroup containing component(s) in the semisimple socle of $C_G(i)$ by Theorem 4.4 and the arguments in Section 4.2 except that $G = \mathrm{Sp}_4(q)$ in which case the involution $i \in G$ is a classical involution and we can assume that the map ζ_1^i is defined for most of the elements of S by Theorem 5.7. Hence we can construct a subgroup in $C_G(i)$ containing a quasi-simple subgroup. Note that the second derived subgroup $C_G(i)''$ is the semisimple socle of $C_G(i)$, see the remark after Theorem 3.9, and we compute derived subgroups of black box groups in polynomial time by an algorithm in [7]. Hence we have subgroup L which is a commuting product of quasi-simple groups of Lie type of characteristic p by

Theorem 3.9. Now we search for a non-central involution $j \in L$. If we can not construct a non-central involution in L in reasonable number of times, then we conclude that L is a direct product of $\mathrm{SL}_2(q)$ by a result in [43] and we return this subgroup. If a non-central involution $j \in L$ is found, then we construct $C_L(j)$ by using the same arguments.

Note that if $C_G(j)$ is solvable of length at most 2, that is, $C_G(j)'' = 1$, for a pseudo-involution (resp. an involution) $j \in G$ in a quasi-simple (resp. simple) group G of Lie type over a field of odd size $q > 3$, then $G \cong \mathrm{SL}_2(q)$ (resp. $\mathrm{PSL}_2(q)$).

Now we have two cases: Either $C_L(j)'' = 1$ or $\neq 1$. If $C_L(j)'' = 1$, which is the case if L is a central product of several $\mathrm{SL}_2(q)$ or direct product of $\mathrm{PSL}_2(q)$ and j acts as a pseudo-involution or an involution in all components respectively, then we return the subgroup $\langle j^L \rangle'$. If $C_L(j)'' \neq 1$, then we conclude that $C_L(j)''$ is the semisimple socle of $C_L(j)$ and we set $G := C_L(j)''$ and repeat the process for this subgroup.

It is clear that a centralizer of an involution contains a maximal torus T of G, and the semisimple socle is normalized by T, see Theorem 3.9. Hence the commuting products of $(\mathrm{P})\mathrm{SL}_2(q)$ obtained by the recursive construction of centralizers of involutions is normalized by a maximal torus of G.

5.1.2. Constructing $\mathrm{SL}_2(q)$

We continue Algorithm 5.3 with the following algorithm.

Algorithm 5.4 *" Construction of* $\mathrm{SL}_2(q)$*"*

> *Input: A black box group L which is isomorphic to commuting products of* $(\mathrm{P})\mathrm{SL}_2(q^l)$ *for various l.*
>
> *Output: A black box group isomorphic to* $\mathrm{SL}_2(q^k)$ *for some k appearing as a factor in the commuting product or return the statement "L is a direct product of* $\mathrm{PSL}_2(q)$*".*

As the involution in $\mathrm{SL}_2(q)$ is central, we are going to use pseudo-involutions to construct a component in L. We will call an element j a *pseudo-involution* in a quasimple group G if $j^2 \neq 1$ but $j^2 \in Z(G)$. We define the maps ζ_0 and ζ_1 in the same way for the pseudo-involutions and by a direct computation, we have $\langle \zeta_1^j(G) \rangle'' = 1$ for $G = \mathrm{SL}_2(q)$.

We define the 2-*height* of an integer n as the integer which is the maximum power of 2 dividing n. The 2-*height* of a group element is defined to be the 2-height of its order.

It is easy to see that random elements in L have different 2-heights with high probability. Therefore a pseudo-involution $j \in L$ constructed from a random element acts

non-trivially on fewer number of components with high probability. Hence $\langle j^L\rangle'$ contains fewer number of components and $\langle\zeta_1^j(L)\rangle''$ contains the complement in L. If we can not find a pseudo-involution, we conclude that L is direct products of $\mathrm{PSL}_2(q)$ in which case we return to Algorithm 5.3 to construct new commuting products of (P)$\mathrm{SL}_2(q)$. Now we set $L = \langle j^L\rangle'$ and continue in this way until we get $\langle\zeta_1^j(L)\rangle'' = 1$. If we always have $\langle\zeta_1^j(L)\rangle'' = 1$ for different pseudo-involutions after reasonable number of times, then we conclude that $L = \mathrm{SL}_2(q)$.

5.1.3. Finding the order of the field

Algorithm 5.5 "Finding field order"

Input: A black box group K isomorphic to $\mathrm{SL}_2(q)$.

Output: The order q of the underlying field.

Let K be a black box group isomorphic to $\mathrm{SL}_2(q)$. The elements of K have order dividing either $q-1$, $q+1$ or $2p$ where p is the characteristic of the field. The semisimple elements belong to tori of order $q\pm1$. The probability of finding a generator in these tori is

$$\frac{\Phi(q\pm1)}{q\pm1} \geqslant \frac{1}{e^\gamma \log\log(q\pm1)}$$

where Φ is Euler function, e is the base of the natural logarithm and γ is Euler constant [60]. Therefore we can find an element of order $q\pm1$ with probability at least $1/e^\gamma \log\log(q-1)$.

Let $E = p^n m$, $(p,m) = 1$, be a global exponent for the group G. We produce a set $S \subset K$ consisting of random elements. It is clear that $g^{p(p^n-1)} = 1$ for each $g \in S$. Starting from $k = 1$, we check whether $g^{p(p^{2k}-1)} = 1$ for each $g \in S$. When we find the smallest number k, $1 \leqslant k \leqslant n$ such that $g^{p(p^k-1)} = 1$ for each $g \in S$, we deduce that the order of the undelying field is $q = p^k$. The probability of error is at most $(1 - 1/e^\gamma \log\log(q\pm1))^{|S|}$.

Note that the order of the field found by Algorithm 5.5 is not necessarily the order of the field on which G is defined, for example, let $G = \mathrm{PSL}_4(q)$ and $q \equiv -1$ mod4, then there exists an involution $i \in G$ such that $K = C_G(i)'' = \mathrm{PSL}_2(q^2)$ and Algorithm 5.5 returns q^2.

5.1.4. A long root $\mathrm{SL}_2(q)$

Algorithm 5.6 "Checking whether a given $\mathrm{SL}_2(q)$ is a long root $\mathrm{SL}_2(q)$"

Input: A black box subgroup $K \leqslant G$ which is known to be isomorphic to $\mathrm{SL}_2(q)$.

Output: The truth value of the statement: "K is a long root $\mathrm{SL}_2(q)$-subgroup in G".

If K is a long root $\mathrm{SL}_2(q)$-subgroup, then $K = K^g$ for any $g \in C_G(i)''$ by Lemma 3.4.

Assume that $G \neq G_2(q)$ or ${}^3D_4(q)$. If $K \leqslant G$ is not a long root $\mathrm{SL}_2(q)$-subgroup but isomorphic to $\mathrm{SL}_2(q)$, then we can find with high probability $g \in C_G(i)''$ such that $K \neq K^g$ and again with high probability we can find an element $h \in \langle K, K^g \rangle$ whose order does not divide $|K|$, in other words, we are in the setting of verification problem, see Lemma 3.5. For example, let $G = \mathrm{SL}_n(q)$, $K = \mathrm{SL}_2(q^2)$ and $i \in K$ be the involution. Then $C_G(i)' \cong \mathrm{SL}_4(q) \times \mathrm{SL}_{n-4}(q)$, and $\langle K, K^g \rangle = \mathrm{SL}_4(q)$ with probability $1 - O(1/q)$ for random $g \in C_G(i)'$, and there are sufficiently many elements in $\mathrm{SL}_4(q)$ whose orders do not divide $|K|$.

If $G = G_2(q)$ or ${}^3D_4(q)$, then we need to have a special procedure to conclude that a given subgroup isomorphic to $\mathrm{SL}_2(q)$ indeed corresponds to a long root $\mathrm{SL}_2(q)$-subgroup in G. Note that there is only one conjugacy class of involutions in G. Let $G =^3 D_4(q)$, then $C_G(i) \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q^3)$ and $\mathrm{SL}_2(q^3)$ corresponds to a short root while $\mathrm{SL}_2(q)$ corresponds to a long root $\mathrm{SL}_2(q)$-subgroup. If $G = G_2(q)$ then $C_G(i) = \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ and one of the $\mathrm{SL}_2(q)$'s corresponds to a short root and the other corresponds to a long root $\mathrm{SL}_2(q)$-subgroup. We refer to Algorithm 4.17 in [74] for the rest of the technical details of the construction of a long root $\mathrm{SL}_2(q)$-subgroup.

Notice that the output "K is not a long root $\mathrm{SL}_2(q)$-subgroup" is always true.

Note that the long root $\mathrm{SL}_2(q)$-subgroups are normalized by a maximal standard torus of G.

5.2. Recognition of the p-core

In the recognition algorithm for the p-core, we are going to use classical involutions and the map ζ_1. The distribution of the elements for which the map ζ_1 is defined is given by the following theorem.

Theorem 5.7 [75] *Let G be a finite simple classical group of odd characteristic and $i \in G$ be a classical involution, then the product $i \cdot i^g$ has odd order with probability bounded from*

below by constant.

Parker and Wilson obtained a similar estimate in their preprint [66] for the exceptional groups of Lie type of odd characteristic.

Algorithm 5.8 *"Recognition of the p-core"*

> *Input: A black box group X with the property that $X/O_p(X)$ is a finite simple group of Lie type of odd characteristic p.*
>
> *Output: If $O_p(X) \neq 1$, then the algorithm finds a non-trivial p-element in $O_p(X)$ with probability bounded from below by a constant. Otherwise it returns the statement "Possibly, the p-core is trivial".*

Let $X/O_p(X) \cong \mathrm{PSL}_2(q)$ and $i \in X$ be an involution. Assume that $Q = O_p(X) \neq 1$. It is easy to see that $C_Q(i) \neq 1$ and therefore $Q_1 = O_p(C_X(i)) \neq 1$. Now $C_X(i)/Q_1$ is isomorphic to a dihedral group of order $q \pm 1$. If $O_p(C_X(i)') = 1$, then random elements in $C_X(i)$ have orders which are multiple of p and we can find a p-element in Q_1 by raising a random element in $C_X(i)$ to the power $q \pm 1$. Hence we can assume that $O_p(C_X(i)') \neq 1$. Now $C_X(i)'/O_p(C_X(i)')$ is isomorphic to a cyclic group of order $(q \pm 1)/2$. Hence when we take the power $(q \pm 1)/2$ of random elements in $C_X(i)'$ we can produce p-elements in $O_p(C_x(i)')$. Our approach in the general case is to reduce to problem to this case in all finite simple groups of Lie type of odd characteristic p.

If $X/O_p(X) \cong {}^2G_2(q)$ and $\bar{i} \in X/O_p(X)$ is an involution, then $C_{X/O_p(X)}(\bar{i}) \cong \langle \bar{i} \rangle \times \mathrm{PSL}_2(q^2)$ and hence we use the above method to determine whether $O_p(X) \neq 1$.

We first construct a subgroup K where $K/O_p(K)$ is a long root $\mathrm{SL}_2(q)$-subgroup in $X/O_p(X)$ by using Algorithm 5.2. Then we construct $C_X(i)$ by using the map ζ_1^i where i is a classical involution in K. The efficiency of the map ζ_1^i for classical involutions is given by Theorem 5.7. We know that $(C_X(i)/O_p(C_X(i)))''$ is the semisimple socle of $C_X(i)/O_p(C_X(i))$ by Lemma 3.10 and we construct 2-components K and L of $C_X(i)$. We can determine whether $O_p(K) \neq 1$ by using the argument above. If we find that $O_p(K) = 1$, and if $O_p(X) \neq 1$ then $O_p(L) \neq 1$. Therefore we set $X := L$ and repeat this procedure. If we always have $O_p(K) = 1$ for all K constructed in this way, we deduce that $O_p(X) = 1$.

5.3. Probabilistic recognition of classical groups

In this section we present an algorithm which determines the type (linear, symplectic, unitary, orthogonal) of a given black box classical group which is based on properties of long root $\mathrm{SL}_2(q)$-subgroups in classical groups. In particular, we present a black box group algorithm distinguishing symplectic groups $\mathrm{PSp}_{2n}(q)$ from othogonal groups $\mathrm{P}\Omega_{2n+1}(q)$ with given degree of certainty where such an algorithm was first presented by Altseimer and Borovik [1].

Theorem 5.9 *Let G be a finite simple classical group, K a long root $\mathrm{SL}_2(q)$-subgroup and $g \in G$. Then, with probability $1 - O(1/q)$, if*

- $G = \mathrm{PSL}_n(q)$ *and* $n > 4$, *then* $\langle K, K^g \rangle = \mathrm{SL}_4(q)$;
- $G = \mathrm{PSU}_n(q)$ *and* $n > 4$, *then* $\langle K, K^g \rangle = \mathrm{SU}_4(q)$;
- $G = \mathrm{PSp}_{2n}(q)$ *and* $n > 2$, *then* $\langle K, K^g \rangle = \mathrm{Sp}_4(q)$;
- $G = \mathrm{P}\Omega^{\varepsilon}_n(q)$ *and* $n > 8$, *then* $\langle K, K^g \rangle = \Omega^+_8(q)$.

If the rank of the group is smaller in the above cases, then we have $\langle K, K^g \rangle = G$ with probability $1 - O(1/q)$.

The algorithm is as follows.

Algorithm 5.10 "Determination of the type"

> *Input: A black box group G isomorphic to a finite simple classical group of odd characteristic p.*
>
> *Output: It finds the size of the underlying field, q, and returns one of the following statements: "G is isomorphic to $\mathrm{PSL}_n(q)$ for some n", "G is isomorphic to $\mathrm{PSU}_n(q)$ for some n", "G is isomorphic to $\mathrm{PSp}_{2n}(q)$ for some n", "G is isomorphic to $\mathrm{P}\Omega^{\varepsilon}_n(q)$ for some n".*

The groups $\mathrm{SL}_4(q)$, $\mathrm{SU}_4(q)$, $\mathrm{Sp}_4(q)$ and $\Omega^+_8(q)$ can be easily distinguished from each other by the analysis on the orders of elements, hence the type of the group G is determined by Theorem 5.9.

5.4. Construction of Curtis-Phan-Tits system

In this section we present an algorithm which constructs all long root $\mathrm{SL}_2(q)$-subgroups in a black box group G isomorphic to $\mathrm{PSL}_n(q)$, $n \geqslant 3$, $q \geqslant 5$ which correspond to the nodes in the extended Dynkin diagram of $\mathrm{PSL}_n(q)$. The algorithm for $\mathrm{PSU}_n(q)$ can be read along the same steps by changing the notation SL to SU.

Algorithm 5.11 "Curtis-Tits system for $\mathrm{PSL}_n(q)$"

Input: A black box group G isomorphic to $\mathrm{PSL}_n(q)$, $q \geqslant 5$ odd and $n \geqslant 3$.

Output: Some generators for long root $\mathrm{SL}_2(q)$-subgroups of G which correspond to the nodes in the extended Dynkin diagram of G.

Assume that $n \geqslant 4$. We first construct a long root $\mathrm{SL}_2(q)$-subgroup $K_1 \leqslant G$. The main task here is to construct a long root $\mathrm{SL}_2(q)$-subgroup $K_2 \leqslant G$ which together with K_1 generate $\mathrm{SL}_3(q)$. Recall that the long root $\mathrm{SL}_2(q)$-subgroups are normalized by a maximal standard torus of G. Recall also that two random long root $\mathrm{SL}_2(q)$-subgroups generate a subgroup isomorphic to $\mathrm{SL}_4(q)$ with probability $1 - O(1/q)$ by Theorem 5.9. Let $i_1 \in K_1$ be the involution. Then $C_G(i_1)'' = K_1L_1$ where $L_1 \cong \mathrm{SL}_{n-2}(q)$. We know by Theorem 4.4 that $C_G(i_1)'' \leqslant \heartsuit_{i_1}(G)$, which means that the map $\zeta_0^{i_1}$ produces involutions with the property that they do not centralize K_1 and L_1. It turns out that the distribution of the elements $g \in G$ such that $\zeta_0^{i_1}(g)$ is an involution which does not centralize K_1 is bounded from below by constant and such an involution is necessarily a classical involution [74]. Hence we can construct a classical involution $i_2 \in C_G(i_1)$ which does not centralize K_1. The long root $\mathrm{SL}_2(q)$-subgroup K_2 can be easily constructed from $C_G(i_2)'' = K_2L_2$ and it is easy to see that $\langle K_1, K_2\rangle = \mathrm{SL}_3(q)$.

Let $T_1 < K_1$ be a torus of order $q-1$, then there is a torus $T_2 < K_2$ of order $q-1$ such that $[T_1, T_2] = 1$ and $T_i < N_G(K_j)$ for $i, j = 1, 2$.

Now we will construct a long root $\mathrm{SL}_2(q)$-subgroup $K_3 \leqslant L_1$ in the same way. Note that $[K_1, L_1] = 1$, therefore we have $[K_1, K_3] = 1$. Hence we have constructed three long root $\mathrm{SL}_2(q)$-subgroups K_1, K_2, K_3 such that

- $[K_1, K_3] = 1$,
- $\langle K_1, K_2\rangle = \langle K_2, L_2\rangle = \mathrm{SL}_3(q)$.
- $T_i < N_G(K_j)$ for $i, j = 1, 2, 3$.

Continuing in this way, we will construct long root $\mathrm{SL}_2(q)$-subgroups $K_1, \ldots, K_{n-1}$ where

- $[K_i, K_j] = 1$ if $|i-j| \geqslant 2$,
- $\langle K_i, K_j \rangle = \mathrm{SL}_3(q)$ if $|i-j| = 1$.
- $T_i < N_G(K_j)$ for $i, j = 1, \ldots, n-1$

Notice that these subgroups correspond to the root $\mathrm{SL}_2(q)$-subgroups in the Curtis-Tits presentation and hence they correspond to the nodes in the Dynkin diagram. The maximal standard torus T normalizing each K_j is $T = \langle T_i \mid i = 1, \ldots, n-1 \rangle$. In order to construct the long root $\mathrm{SL}_2(q)$-subgroup $K_n \leqslant G$ which corresponds to the extra node in the extended Dynkin diagram, we first compute the involution $i_n = i_1 \cdots i_{n-1}$. It is easy to see that i_n is a classical involution and it does not centralize K_1 and K_{n-1}. Hence the subgroup K_n, which can be constructed from $C_G(i_n)'' = K_n L_n$, is a long root $\mathrm{SL}_2(q)$-subgroup corresponding to the extra node in the extended Dynkin diagram.

Acknowledgement

I am very grateful to Alexandre Borovik for many stimulating conversations and invaluable comments during the preparation of this work which would not have appeared without him. I would like to thank to Ayse Berkman for her useful suggestions. This work is supported in part by The Scientific and Technological Research Council of Turkey (TÜBİTAK).

References

[1] Altseimer, C., Borovik, A. V.: Probabilistic recognition of orthogonal and symplectic groups. In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 1–20, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

[2] Aschbacher, M.: A characterization of Chevalley groups over fields of odd order I, II. Ann. of Math. 106, 353–468 (1977).

[3] Aschbacher, M.: On the maximal subgroups of the finite classical groups. Invent. Math. 76, 469–514 (1984).

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

[5] Babai, L.: Randomization in group algorithms: conceptual questions. In: Groups and Computation II (Eds.: L. Finkelstein and W. M. Kantor) 1–17, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 28 (1997).

[6] Babai, L., Beals, R.: A polynomial-time theory of black box groups I. In: Groups St. Andrews 1997 in Bath I. 30–64, London Math. Soc. Lecture Note Ser. 260, Cambridge Univ. Press, Cambridge (1999).

[7] Babai, L., Cooperman, G., Finkelstein, L., Luks, E. M., Seress, Á.: Fast Monte Carlo algorithms for permutation groups. J. Comput. System Sci. 50, 296–308 (1995).

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

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

[10] Babai, L., Pak, I.: Strong bias of group generators: an obstacle to the "product replacement algorithm". J. Algorithms 50, 215–231 (2004).

[11] Babai, L., Shalev, A.: Recognizing simplicity of black-box groups and the frequency of p-singular elements in affine groups. In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 39–62, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

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

[13] Beals, R.: Towards polynomial time algorithms for matrix groups. In: Groups and Computation II (Eds.: L. Finkelstein and W. M. Kantor) 31–54, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 28 (1997).

[14] Beals,R., Leedham-Green, C. R., Niemeyer, A. C., Praeger, C. E., Seress, Á.: A black-box group algorithm for recognizing finite symmetric and alternating groups I. Trans. Amer. Math. Soc. 355, 2097–2113 (2003).

[15] Beals, R., Leedham-Green, C. R., Niemeyer, A. C., Praeger, C. E., Seress, Á.: Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules. J. Algebra 292, 4–46 (2005).

[16] Bennett, C. D., Gramlich, R., Hoffman, C., Shpectorov, S.: Curtis-Phan-Tits theory. In: Groups, combinatorics & geometry 13–29, World Sci. Publ. (2003).

[17] Bennett, C. D., Shpectorov, S.: A new proof of a theorem of Phan. J. Group Theory 7, 287–310 (2004).

[18] Borovik, A. V.: Centralisers of involutions in black box groups. In: Computational and statistical group theory 7–20, Contemp. Math. 298 (2002).

[19] Bosma, W., Cannon, J., Playoust, C.: The magma algebra system. J. Symbolic Computation 24, 235–265 (1997).

[20] Bratus, S., Pak, I.: Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's conjecture. J. Symbolic Comput. 29, 33–57 (2000).

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

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

[23] Brooksbank, P. A., Kantor, W. M.: On constructive recognition of a black box $\mathrm{PSL}(d, q)$. In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 95–111, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

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

[25] Carter, R.: Conjugacy classes in the Weyl group. In: Seminar on Algebraic Groups and Related Finite Groups 297–318, Lecture Notes in Mathematics 131, Springer, Berlin, 1970.

[26] Carter, R.: Simple groups of Lie type. London-New York-Sydney. John Wiley & Sons. 1972.

[27] Carter, R.: Finite groups of Lie type: Conjugacy classes and complex characters. New York. Wiley-Interscience. 1985.

[28] Celler, F., Leedham-Green, C. R.: A non-constructive recognition algorithm for the special linear and other classical groups. In: Groups and Computation II (Eds.: L. Finkelstein and W. M. Kantor) 61–67, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 28 (1997).

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

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

[31] Conder, M., Leedham-Green, C. R.: Fast recognition of classical goups over large fields. In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 113-121, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

[32] Conder, M., Leedham-Green, C. R., O'Brien, E. A.: Constructive recognition of PSL$(2, q)$. Trans. Amer. Math. Soc. 358, 1203–1221 (2006).

[33] Cooperman, G., Finkelstein, L., Linton, S.: Constructive recognition of a black box group isomorphic to GL$(n, 2)$. In: Groups and Computation II (Eds.: L. Finkelstein and W. M. Kantor) 85–100, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 28 (1997).

[34] Curtis, C. W.: Central extensions of groups of Lie type. J. Reine Angew. Math. 220, 174–185 (1965).

[35] Diaconis, P., Graham, R.: The graph of generating sets of an abelian group. Colloq. Math. 80, 31–38 (1999).

[36] Dixon, J. D.: The probability of generating the symmetric group. Math. Z. 110, 199–205 (1969).

[37] Glauberman, G.: Central elements in core-free groups. J. Algebra 4, 403–420 (1966).

[38] Gorenstein, D., Lyons, R., Solomon, R.: The classification of the finite simple groups. Number 3. Mathematical Surveys and Monographs 40, American Mathematical Society, Providence, RI (1998).

[39] Gramlich, R.: Weak Phan systems of type C_n. J. Algebra 280, 1–19 (2004).

[40] Gramlich,R., Hoffman, C., Nickel, W., Shpectorov, S.: Even-dimensional orthogonal groups as amalgams of unitary groups. J. Algebra 284, 141–173 (2005).

[41] Gramlich, R., Hoffman, C., Shpectorov, S.: A Phan-type theorem for Sp$(2n, q)$. J. Algebra 264, 358–384 (2003).

[42] Gramlich, R., Horn, M., Nickel, W.: The complete Phan-type theorem for Sp$(2n, q)$. J. Group Theory 9, 603–626 (2006).

[43] Griess, Jr. R. L.: Finite groups whose involutions lie in the center. Quart. J. Math. Oxford Ser. (2) 29, 241–247 (1978).

[44] The GAP Group. Gap - groups, algorithms, and programming, version 4.2. Aachen, St Andrews, (`http://www-gap.dcs.st-and.ac.uk/ gap`) 2000.

[45] Guralnick, R. M., Lübeck, F.: On p-singular elements in Chevalley groups in characteristic p. In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 169–182, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

[46] Guralnick, R. M., Tiep, P. H.: Finite simple unisingular groups of Lie type. J. Group Theory 6, 271–310 (2003).

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

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

[49] Kantor, W. M., Seress, Á.: Black box classical groups. Mem. Amer. Math. Soc. 149 (2001).

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

[51] Kantor, W. M., Seress, Á.: Computing with matrix groups. In: Groups, combinatorics & geometry 123–137, World Sci. Publ. (2003).

[52] Koblitz, N.: A course in Number Theory and Cryptography. Springer-Verlag 1994.

[53] Leedham-Green, C. R.: The computational matrix group project. In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 229–247, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

[54] Leedham-Green, C. R., O'Brien, E. A.: Recognising tensor products of matrix groups. Internat. J. Algebra Comput. 7, 541–559 (1997).

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

[56] Liebeck, M. W., O'Brien, E. A.: Finding the characteristic of a group of Lie type. to appear in J. London Math. Soc.

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

[58] Liebeck, M. W., Shalev, A.: Diameters of finite simple groups: sharp bounds and applications. Ann. of Math. 154, 383–406 (2001).

[59] Lubotzky, A., Pak, I.: The product replacement algorithm and Kazhdan's property (T). J. Amer. Math. Soc. 14, 347–363 (2001).

[60] Mitrinović, D. S., Sándor, J., Crstici, B.: Handbook of number theory, Mathematics and its Applications 351. Kluwer Academic Publishers Group, Dordrecht 1996.

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

[62] Niemeyer, A. C., Praeger, C. E.: A recognition algorithm for classical groups over finite fields. Proc. London Math. Soc. 77, 117–169 (1998).

[63] O'Brien, E. A.: Towards effective algorithms for linear groups. In: Finite Geometries, Groups and Computation 163–190, de Gruyter, Colorado (2006).

[64] Pak, I.: The product replacement algorithm is polynomial. Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci. 476–485 (2001).

[65] Pak, I.: What do we know about the product replacement algorithm? In: Groups and Computation III (Eds.: W. M. Kantor and Á. Seress) 301–347, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001).

[66] Parker, C., Wilson, R.: Recognising simplicity of black box groups, preprint.

[67] Phan, K. W.: On groups generated by three-dimensional special unitary groups I, II. J. Austral. Math. Soc. Ser. A 23, 67–77, 129–146 (1977).

[68] Rabin, M. O.: Probabilistic algorithms for testing primality. J. Number Theory 12, 128–138 (1980).

[69] Seitz, G. M.: The root subgroups for maximal tori in finite groups of Lie type. Pacific J. Math. 106, 153–244 (1983).

[70] Seress, Á.: Permutation group algorithms, Cambridge Tracts in Mathematics 152. Cambridge University Press, Cambridge 2003.

[71] Steinberg, R.: Lectures on Chevalley groups. Yale University, New Haven, Conn. 1968.

[72] Timmesfeld, F. G.: The Curtis-Tits presentation. Adv. Math. 189, 38–67 (2004).

[73] Tits, J.: Groupes semi-simples isotropes. In: Colloq. Théorie des Groupes Algébriques 137–147, Librairie Universitaire, Louvain (1962).

[74] Yalçınkaya, Ş.: Black box groups and related group theoretic constructions. PhD. Thesis. METU (2007).

[75] Yalçınkaya, Ş.: Construction of long root $SL_2(q)$-subgroups in black box groups, in preparation.

[76] Zsigmondy, K.: Zur Theorie der Potenzreste. Monatsh. Math. Phys. 3, 265–284 (1892).

Şükrü YALÇINKAYA
Department of Mathematics
Middle East Technical University
Ankara-TURKEY
e-mail: sukru.yalcinkaya@gmail.com

Received 17.10.2007