Construction of Curtis-Phan-Tits system in black box classical groups

Borovik, Alexandre and Yalcinkaya, Sukru

2010

MIMS EPrint: **2010.72**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Construction of Curtis-Phan-Tits system in black box classical groups

Alexandre Borovik* and Şükrü Yalçınkaya†

May 10, 2010

Abstract

We present a polynomial time Monte-Carlo algorithm for finite simple black box classical groups of odd characteristic which constructs all root $\mathrm{SL}_2(q)$-subgroups associated with the nodes of the extended Dynkin diagram of the corresponding algebraic group.

Contents

1 Introduction **2**

2 Root $\mathrm{SL}_2(q)$-subgroups in finite groups of Lie type **4**

3 Involutions in classical groups **5**

4 Curtis-Phan-Tits presentation **6**

5 Construction of $C_G(i)$ in black box groups **9**

6 Probabilistic estimates and other results **11**
6.1 Groups of type A_{n-1} . . . 12
6.2 Groups of type B_n and D_n . . . 15
6.3 Groups of type C_n . . . 18

7 Preliminary algorithms **20**
7.1 Probabilistic recognition of classical groups . . . 20
7.2 Recognising classical involutions in black box groups . . . 22

8 Construction of Curtis-Phan-Tits system **23**
8.1 Groups of type A_{n-1} . . . 23
8.2 Groups of type B_n and D_n . . . 26
8.3 Groups of type C_n . . . 29
8.3.1 A small case: $\mathrm{PSp}_4(q)$ . . . 29
8.3.2 General case: $\mathrm{PSp}_{2n}(q)$, $n \geqslant 3$ . . . 30

*School of Mathematics, University of Manchetser, UK; alexandre.borovik@manchester.ac.uk

†Corresponding author: School of Mathematics and Statistics, University of Western Australia; sukru@maths.uwa.edu.au

1 Introduction

Babai and Szemeredi [6] introduced *black box groups* as an ideal setting for an abstraction of the permutation and matrix group problems in computational group theory. A black box group is a group whose elements are represented by $0-1$ strings of uniform length and the tasks: multiplying group elements, taking inverse and checking whether a string represents a trivial element or not are done by an oracle (or 'black box'). A black box group algorithm is an algorithm which does not depend on specific properties of the representation of the given group or how the group operations are performed [42].

A black box group X is specified as $X = \langle S \rangle$ for some set S of elements of X and to construct a black box subgroup means to construct some generators for this subgroup. We have $|X| \leqslant 2^N$ where N is the encoding length. Therefore, if X is a classical group of rank n defined over a field of size q, then $|X| > q^{n^2}$, and so $O(N) = n^2 \log q$.

An important component of black-box group algorithms is the construction of uniformly distributed random elements. In [4], Babai proved that there is a polynomial time Monte-Carlo algorithm producing "nearly" uniformly distributed random elements in black box groups. However, this algorithm is not convenient for practical purposes, especially for matrix groups, as its cost is $O(N^5)$ where N is the input length. A more practical solution is the "product replacement algorithm" [19], see also [35, 36].

In this paper, we complete the black box recognition of a finite group X where $X/O_p(X)$ is a simple classical group of odd characteristic p via the approach introduced in [46]. By the availability of a black box oracle for the construction of a centraliser of an involution in black box groups [1, 10, 13], a uniform approach is proposed in [46] to recognise a black box group X where $X/O_p(X)$ is a simple group of Lie type of odd characteristic p by utilizing the ideas from the classification of the finite simple groups. The structure of this approach is as follows.

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

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

3. Construct all subgroups $K \leqslant X$ where $K/O_p(K)$ corresponds to root $\mathrm{SL}_2(q)$-subgroups associated with the extended Dynkin diagram of the corresponding algebraic group.

The task (1) is completed in [46], and (2) is announced independently in [37] and [46]. The present paper completes the task (3) for classical groups, that is, we prove the following.

Theorem 1.1 *Let X be a black box group where $X/O_p(X)$ is isomorphic to a finite simple classical group over a field of odd size $q = p^k > 3$. Then there is*

a Monte-Carlo polynomial time algorithm which constructs all subgroups corresponding to root $\mathrm{SL}_2(q)$*-subgroups of* $X/O_p(X)$ *associated with the nodes in the extended Dynkin diagram of the corresponding algebraic group.*

In a subsequent paper [11], we extend Theorem 1.1 to all black box groups of Lie type of odd characteristic proving an analogous result for the exceptional groups of Lie type of odd characteristic. We shall note here that this approach can be viewed as a black box analogue of Aschbacher's Classical Involution Theorem [2] which is the main identification theorem in the classification of the finite simple groups, see [46] for a discussion of the analogy between our approach and the Classical Involution Theorem. Besides building an analogy between recognition of black box groups and the classification of the finite simple groups, our approach also answers some interesting questions in computational group theory. For example, it immediately follows from Theorem 1.1 that we can construct representatives of all conjugacy classes of involutions in a classical group G of odd characteristic. Moreover, we can also construct all subsystem subgroups of G which can be read from the extended Dynkin diagram and normalised by some maximally split torus, if G is not a twisted group. In the twisted case, such a torus is of order $(q+1)^n$ where n is the Lie rank of the corresponding algebraic group. A *subsystem subgroup* of a simple group G of Lie type is defined to be a subgroup which is normalised by some maximal torus of G.

There are mainly two types of black box algorithms to recognise a finite group: probabilistic and constructive recognition algorithms. The probabilistic recognition algorithms are designed to determine the isomorphism type of the groups with a user prescribed probability of error, for example, the standard name of a given simple group of Lie type can be computed in Monte-Carlo polynomial time [1, 5] by assuming an order oracle with which one can compute the order of elements. If successful, the constructive recognition algorithms establish isomorphism between a given black box group and its standard copy. The constructive recognition of black box classical groups is presented in [29]. However, they are not polynomial time algorithms in the input length. They are polynomial in q whereas the input size involves only $\log q$. The size of the field q appears in the running time of the algorithm because unipotent elements (or p-elements where p is the characteristic of the underlying field) are needed to construct an isomorphism and the proportion of unipotent elements or, more generally, p-singular elements (whose orders are multiple of p) is $O(1/q)$ [26]. At the present time, it is still not known how to construct a unipotent element except for random search in a black box group. Later, these algorithms are extended to polynomial time algorithms in a series of papers [14, 15, 16, 17] by assuming a constructive recognition of $\mathrm{SL}_2(q)$. We shall note here that our approach is not a constructive recognition algorithm.

Following our setting in [47], we assume that the characteristic p of the underlying field is given as an input. However, this assumption can be avoided by using one of the algorithms presented in [30], [31] or [32]. In our algorithms we do not use an order oracle, instead we assume that a computationally feasible

global exponent E is given. Note that one can take $E = |\mathrm{GL}_n(q)|$ for an $n \times n$ matrix group over a field of size q.

2 Root $\mathrm{SL}_2(q)$-subgroups in finite groups of Lie type

Let $\bar{G}$ denote a connected simple algebraic group over an algebraically closed field of characteristic p, $\bar{T}$ a maximal torus of $\bar{G}$, $\bar{B}$ a Borel subgroup containing $\bar{T}$ and $\bar{\Sigma}$ be the corresponding root system. Let $\bar{N} = N_{\bar{G}}(\bar{T})$ and $W = \bar{N}/\bar{T}$ the Weyl group of $\bar{G}$. Let σ be a Frobenius endomorphism of $\bar{G}$ and $\bar{G}_\sigma$ the fixed point subgroup of $\bar{G}$ under σ. The subgroup $\bar{G}_\sigma$ is finite, and we denote $G = O^{p'}(\bar{G}_\sigma)$.

For each root $r \in \bar{\Sigma}$, there exists a $\bar{T}$-root subgroup of $\bar{G}$. If $\bar{T}$ is σ-invariant, then the map σ permutes these root subgroups and induces an isometry on the Euclidean space $\mathbb{R}\bar{\Sigma}$ spanned by $\bar{\Sigma}$. 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, where $T = \bar{T}_\sigma$ [41]. The root system of the finite group G is obtained by taking the fixed points of the isometry induced from σ on $\mathbb{R}\bar{\Sigma}$ [21, Section 2.3], and G is generated by the corresponding root subgroups. A root subgroup is called a long or short root subgroup, if the corresponding root is long or short, respectively. We refer the reader to [21, Table 2.4] for a complete description of the structure of the root subgroups in finite groups of Lie type.

Let $\Sigma = \{r_1, \ldots, r_n\}$ and $X_{r_1}, \ldots, X_{r_n}$ be the corresponding root subgroups. Set $M_i = \langle X_{r_i}, X_{-r_i}\rangle$, $Z_i = Z(X_{r_i})$ and $K_i = \langle Z_i, Z_{-i}\rangle$. Then X_{r_i} is a Sylow p-subgroup of M_i and Z_i is a Sylow p-subgroup of K_i. The subgroup $K_i \leqslant G$ is called *long or short root* $\mathrm{SL}_2(q)$*-subgroup*, if the corresponding root $r_i \in \Sigma$ is a long or short, respectively. Here, q is the order of the centre of a long root subgroup of G. Note that if $G \cong \mathrm{PSU}_{2n+1}(q)$, then there exists a long root subgroup X_r of order q^3 where $M = \langle X_r, X_{-r}\rangle \cong \mathrm{PSU}_3(q)$. For this root subgroup we also have $K_r = \langle Z(X_r), Z(X_{-r})\rangle \cong \mathrm{SL}_2(q)$. We have the following fundamental result about long root $\mathrm{SL}_2(q)$-subgroups.

Theorem 2.1 ([2, Theorem 14.5]) *Let G be a finite simple group of Lie type defined over a field of odd order $q > 3$ different from $\mathrm{PSL}_2(q)$ and ${}^2G_2(q)$. With the above notation, 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 $N_G(Z_i)$.*

(3) *$K \trianglelefteq C_G(z)''$. Moreover, if G is not orthogonal, then $N_G(K) = C_G(z)$.*

We call the involutions in long root $\mathrm{SL}_2(q)$-subgroups *classical* involutions.

Following the above notation, it is worth to list the short root $\mathrm{SL}_2(q)$-subgroups in classical groups.

$G(q)$	condition	$K_r = M_r$
$\mathrm{PSp}_{2n}(q)$	$n \geqslant 3$	$\mathrm{SL}_2(q)$
$\mathrm{PSU}_n(q)$	$n \geqslant 4$	$\mathrm{PSL}_2(q^2)$
$\mathrm{P}\Omega^-_{2n}(q)$	$n \geqslant 2$	$\mathrm{PSL}_2(q^2)$
$\Omega_{2n+1}(q)$	$n \geqslant 2$	$\mathrm{PSL}_2(q)$

Table 1: Short root $\mathrm{SL}_2(q)$-subgroups in classical groups [2, Table 14.4].

3 Involutions in classical groups

We summarise the conjugacy classes of involutions and their centralisers in simple classical groups in Table 2. The table is extracted from [21, Table 4.5.1] for the convenience of the reader. The proofs of the results presented in Table 2 can be found in [21, Chapter 4].

Let V denote the underlying natural module for classical groups. The involutions t_k in $\mathrm{PSL}^\varepsilon_n(q)$ act as involutions in $\mathrm{GL}^\varepsilon_n(V)$ where the eigenvalue -1 has multiplicity k. If n is even, then there is an involution of type $t'_{n/2}$ which arises from an element of order 4 in $Z(\mathrm{GL}_{n/2}(q^2))$. Note that $\mathrm{GL}_{n/2}(q^2)$ acts naturally on a totally isotropic subspace of dimension $n/2$ in a unitary geometry.

In $\mathrm{PSp}_{2n}(q)$, the involutions of type t_k for $1 \leqslant k < n/2$ represent an element of order 2 in $\mathrm{Sp}_{2n}(q)$ whereas an involutions of type t_n and t'_n represent an element $t \in \mathrm{Sp}_{2n}(q)$ such that $t^2 = -I$ where I is $2n \times 2n$ identity matrix. The eigenvalue -1 has multiplicity $2k$ for an involution of type t_k, $1 \leqslant k < n/2$. If $q \equiv 1 \bmod 4$, then an element of $Z(\mathrm{GL}_n(q))$ of order 4 induces an involution in $\mathrm{PSp}_{2n}(q)$ which is denoted by t_n. Note that $\mathrm{GL}_n(q)$ can be viewed as a stabiliser of a maximal totally isotropic subspace. Similarly, when $q \equiv -1 \bmod 4$, $\mathrm{GU}_n(q)$ can be embedded in $\mathrm{Sp}(V)$ and similar construction induces an involution denoted by t'_n

In $\Omega_{2n+1}(q)$, the involutions of type t_k, t'_k act as involutions in $\mathrm{O}(V)$ where the eigenvalue -1 has multiplicity $2k$. Note that the spinor norm determines whether $-I_{2k}$ belongs to $\Omega(W)$ where W is $2k$ dimensional orthogonal geometry. Indeed, $-I_{2k} \in \Omega^+_{2k}(q)$ if and only if $q^k \equiv 1 \bmod 4$ and $-I_{2k} \in \Omega^-_{2k}(q)$ if and only if $q^k \equiv -1 \bmod 4$.

In $\mathrm{P}\Omega^\varepsilon_{2n}(q)$, the involutions of type t_k for $1 \leqslant k \leqslant n/2$ act similarly as in $\Omega_{2n+1}(q)$. The involutions of type t_{n-1} and t_n are $O(V)$-conjugate. As in $\mathrm{PSp}_{2n}(q)$, $\mathrm{GL}_n(q)$ can be embedded in $O^+(V)$ as a stabiliser of a maximal totally isotropic subspace. If $q \equiv 1 \bmod 4$, then the description of an involution of type t_n is same as in $\mathrm{PSp}_{2n}(q)$. Similarly $\mathrm{GU}_n(q)$ can be embedded in $\mathrm{O}^\varepsilon_{2n}(q)$ where $\varepsilon = (-1)^n$ and the involutions of type t'_{n-1} and t'_n arises from $Z(\mathrm{GU}_n(q))$ for $\mathrm{P}\Omega^+_{4m}$ when $q \equiv -1 \bmod 4$. The description of the involutions of type t_n in $\mathrm{P}\Omega^-_{2(2m+1)}(q)$ is similar.

Table 2: Centralisers of involutions in finite simple classical groups

G	conditions	type	$O^{p'}(C_G(i))$
$\mathrm{PSL}_n^\varepsilon(q)$	$2 \leqslant k \leqslant n/2$	t_1	$\mathrm{SL}_{n-1}^\varepsilon(q)$
		t_k	$\mathrm{SL}_k^\varepsilon(q) \circ \mathrm{SL}_{n-k}^\varepsilon(q)$
	n even	$t'_{n/2}$	$\frac{1}{(n/2,q-\varepsilon)}\mathrm{SL}_{n/2}(q^2)$
$\Omega_{2n+1}(q)$ $n \geqslant 2$		t_1	$\Omega_{2n-1}(q)$
		t'_1	$\Omega_{2n-1}(q)$
	$2 \leqslant k < n$	t_k	$\Omega_{2k}^+(q) \times \Omega_{2(n-k)+1}(q)$
	$2 \leqslant k < n$	t'_k	$\Omega_{2k}^-(q) \times \Omega_{2(n-k)+1}(q)$
		t_n	$\Omega_{2n}^+(q)$
		t'_n	$\Omega_{2n}^-(q)$
$\mathrm{PSp}_{2n}(q)$ $n \geqslant 2$	$1 \leqslant k < n/2$	t_k	$\mathrm{Sp}_{2k}(q) \circ_2 \mathrm{Sp}_{2(n-k)}(q)$
		t_n	$\frac{1}{(2,n)}\mathrm{SL}_n(q)$
		t'_n	$\frac{1}{(2,n)}\mathrm{SU}_n(q)$
$\mathrm{P}\Omega_{2n}^\varepsilon(q)$ $n \geqslant 4$		t_1	$\Omega_{2n-2}^\varepsilon(q)$
		t'_1	$\Omega_{2n-2}^{-\varepsilon}(q)$
	$2 \leqslant k < n/2$	t_k	$\Omega_{2k}^+(q) \circ_2 \Omega_{2(n-k)}^\varepsilon(q)$
	$2 \leqslant k < n/2$	t'_k	$\Omega_{2k}^-(q) \circ_2 \Omega_{2(n-k)}^{-\varepsilon}(q)$
	$\mathrm{P}\Omega_{4m}^+(q)$	$t_{n/2}$	$\Omega_{2m}^+(q) \circ_2 \Omega_{2m}^+(q)$
	$\mathrm{P}\Omega_{4m}^+(q)$	$t'_{n/2}$	$\Omega_{2m}^-(q) \circ_2 \Omega_{2m}^-(q)$
	$\mathrm{P}\Omega_{4m}^+(q)$	t_{n-1}, t_n	$\frac{1}{2}\mathrm{SL}_{2m}(q)$
	$\mathrm{P}\Omega_{4m}^+(q)$	t'_{n-1}, t'_n	$\frac{1}{2}\mathrm{SU}_{2m}(q)$
	$\mathrm{P}\Omega_{4m}^-(q)$	$t_{n/2}$	$\Omega_{2m}^-(q) \times \Omega_{2m}^+(q)$
	$\mathrm{P}\Omega_{2(2m+1)}^\varepsilon(q)$	t_n	$\mathrm{SL}_{2m+1}^\varepsilon(q)$

4 Curtis-Phan-Tits presentation

The finite groups of Lie type have a special presentation called the *Steinberg presentation* [43] where the generators and relations are given by 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

$$x_r(t+u) = x_r(t)x_r(u), \tag{1}$$

$$[x_r(t), x_s(u)] = \prod_{\substack{\gamma = ir + js,\ i,j \in \mathbb{N}^* \\ r,s \in \Sigma,\ r \neq \pm s}} x_\gamma(c_{i,j,r,s} t^i u^j), \tag{2}$$

$$h_r(t)h_r(u) = h_r(tu) \quad tu \neq 0, \tag{3}$$

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 untwisted simple group of Lie type with root system Σ, see [43, Theorem 8, p. 66] or [18, Theorem 12.1.1]. The analogue of the Steinberg presentation holds also for twisted groups of Lie type where the defining relations are more sophisticated, a detailed discussion can be found in [21, Section 2.4].

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 fundamental roots. Therefore the Curtis-Tits presentation involves the pairs of fundamental roots which are edges or non-edges in the Dynkin diagram. More precisely;

Theorem 4.1 *[20, 45] 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 followings 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 connected 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 4.2 [43, 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 given as follows.

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

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, it is enough to use the generators $x_{ij}(t)$ where $\mid i - j \mid \leqslant 2$.

In [38], Phan proved a similar result for the groups ${}^2A_n(q)$, $D_{2n}(q)$, ${}^2D_{2n+1}(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$. His fundamental result is the following.

Theorem 4.3 *[38] Let G be a finite group containing subgroups $K_i \cong \mathrm{SU}_2(q)$, $q \geqslant 5$, for $i = 1, 2, \ldots, n$ and let H_i be a maximal torus of order $q+1$ in K_i. Assume that*

(P1) $G = \langle K_i \mid i = 1, \ldots, n \rangle$;

(P2) $[K_i, K_j] = 1$ *if* $|i - j| > 1$;

(P3) $\langle K_i, K_j \rangle \cong \mathrm{SU}_3(q)$ *and* $\langle K_i, H_j \rangle \cong \mathrm{GU}_2(q)$ *if* $|i - j| = 1$; *and*

(P4) $\langle H_i, H_j \rangle = H_i \times H_j$ *for all* $i \neq j$.

Then G is isomorphic to a factor group of $\mathrm{SU}_{n+1}(q)$.

It is clear that the subgroups K_i, $i = 1, 2, \ldots, n$ in Theorem 4.3 play the role of the subgroups corresponding to the nodes in the Dynkin diagram of $\mathrm{PSL}_{n+1}(q)$ as in its Curtis-Tits presentation. However, they are not root $\mathrm{SL}_2(q)$-subgroups corresponding to the roots in a fixed fundamental root system of $\mathrm{SU}_{n+1}(q)$.

Following Tits' geometric approach on the identification of the untwisted groups of Lie type, a new Phan theory is introduced in [8], and Bennet and Shpectorov [9] gave a new proof of Phan's theorem, Theorem 4.3, with weaker assumptions which also covers the cases $q = 2, 3, 4$. This new approach to Phan's theorem gives birth to new Phan-type amalgamations for the untwisted groups of Lie type, see [22, 24, 25] for symplectic groups, [23] for even dimensional orthogonal groups and [7] for odd dimensional orthogonal groups.

Let K_r, $r \in \Pi$ and H be the subgroups as in Theorem 4.1. Then we call $(\{K_r \mid r \in \Pi\}; H)$ a *Curtis-Tits system* for G corresponding to the maximal torus H. Let $\Pi^* = \Pi \cup \{\alpha\}$ where α is the highest root in Π. Then $H \leqslant N_G(K_\alpha)$ where K_α is the corresponding root $\mathrm{SL}_2(q)$-subgroup and we call $(\{K_r \mid r \in \Pi^*\}; H)$ an *extended Curtis-Tits system* for G corresponding to the maximal torus H.

Similarly, we define an extended Phan system for a group G.

Definition 4.4 *Let Σ be an irreducible root system of rank at least 3 with fundamental system Π and Dynkin diagram Δ. Let $\Pi^* = \Pi \cup \{\alpha\}$ where α is the highest root in Π and Δ^* be the extended Dynkin diagram. Let G be a finite group and assume that the followings are satisfied.*

- $G = \langle K_r \mid r \in \Pi \rangle$, $K_r \cong \mathrm{SU}_2(q)$.
- *For all* $r, s \in \Pi^*$, $H_r \leqslant N_G(K_s)$, $|H_r| = q + 1$ *and* $H = \langle H_r \mid r \in \Pi^* \rangle$ *is an abelian group.*
- $[K_r, K_s] = 1$ *if* r *and* s *are not connected in* Δ^*.
- $\langle K_r, K_s \rangle \cong (\mathrm{P})\mathrm{SU}_3(q)$ *if* r *and* s *are connected with a single bond.*
- $\langle K_r, K_s \rangle \cong (\mathrm{P})\mathrm{Sp}_4(q)$ *if* r *and* s *are connected with a double bond.*

Then $(\{K_r \mid r \in \Pi\}; H)$ *is called a Phan system and* $(\{K_r \mid r \in \Pi^*\}; H)$ *is called an extended Phan system for* G.

In [12], we generalise the Curtis-Tits system to all possible amalgamations in a finite group of Lie type of odd characteristic. In particular, we obtain the following result which elaborates the relation between Phan and Curtis-Tits systems in terms of root $\mathrm{SL}_2(q)$-subgroups and the corresponding maximal torus normalising them.

Theorem 4.5 *[12] Let* $\bar{G}$ *be a simply connected simple algebraic group of type* B_n, C_n, D_{2n}, E_7, E_8, F_4 *or* G_2 *over an algebraically closed field of odd characteristic. Let* σ *be a standard Frobenius homomorphism and* $\bar{T}$ *a* σ*-invariant maximal torus. Let* $(\{\bar{K}_r \mid r \in \Pi^*\}; \bar{T})$ *be an extended Curtis-Tits System for* $\bar{G}$. *Then* $(\{(\bar{K}_r^g)_\sigma \mid r \in \Pi^*\}; (\bar{T}^g)_\sigma)$ *is an extended Phan system for* $\bar{G}_\sigma$ *where* $g \in \bar{G}$ *such that* $g^{-1}\sigma(g)\bar{T} \in Z(N_{\bar{G}}(\bar{T})/\bar{T})$.

Note that the groups listed in Theorem 4.5 are the only simple algebraic groups whose Weyl groups have non-trivial centre. Therefore the finite groups obtained from these groups are the only untwisted groups of Lie type which have Phan system. The same result also holds for the groups ${}^2A_n(q)$, ${}^2D_{2n+1}(q)$, ${}^2E_6(q)$, ${}^3D_4(q)$ in which case the Frobenius automorphism σ induces a graph automorphism.

5 Construction of $C_G(i)$ in black box groups

In this section, we recall the construction of the centralisers of involutions in black-box groups following [10], see also [13].

Let X be a black-box finite 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

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

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 $1/4$ [27].

Let i be an involution in X. Then, by [10, Section 6], there is a partial map $\zeta^i = \zeta_0^i \sqcup \zeta_1^i$ defined by

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

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

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

Theorem 5.1 ([10]) *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 $\zeta_1^i(x)$ are uniformly distributed and independent in $C_X(i)$ and*
2. *the elements $\zeta_0^i(x)$ form a normal subset of involutions in $C_X(i)$.*

By convention, we write $\zeta_0^i(g) = 1$ (resp. $\zeta_1^i(g) = 1$) when ii^g is of odd order (resp. even order). It is clear from Theorem 5.1 that $\langle \zeta_1^i(G) \rangle = C_G(i)$ and $\langle \zeta_0^i(G) \rangle \trianglelefteq C_G(i)$. By [47, Theorem 5.7], $\langle \zeta_0^i(G) \rangle$ contains the semisimple socle of the centraliser of an involution $i \in G$ for a simple group G of Lie type of odd characteristic except for $G \cong \mathrm{PSp}_{2n}(q)$ and the involution of type t_1.

Kantor and Lubotzky [28] proved that randomly chosen two elements in a finite simple classical group G generate G with probability $\to 1$ as $|G| \to \infty$. They also prove an analogous result for the direct product of finite simple classical groups assuming the order of the each direct factor approaches ∞. Therefore some reasonable number of random elements generate the centraliser of an involution in finite simple classical groups over large fields with high probability. By Theorem 5.1, we shall use the map ζ_1^i to produce uniformly distributed random elements in $C_G(i)$. For an arbitrary involution $i \in G$ where G 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 dimension of the underlying vector space [37]. For the classical involutions in classical groups, such a proportion is proved to be bounded from below by an absolute constant [47, Theorem 8.1].

The map ζ_0^i is also an efficient tool to generate a subgroup containing semisimple socle of the centraliser of an involution. By Lemma 5.6 and Theorem 5.7 in [47], the image of ζ_0^i generates a subgroup containing semisimple socle of $C_G(i)$ where G is any simple group of Lie type of odd characteristic except that $G \cong \mathrm{PSp}_{2n}(q)$ and i is an involution of type t_1. For the construction of a centraliser of an involution $\mathrm{i}(g)$ for some random element $g \in G$ by using only the map ζ_0, we first note that random elements are powered upto *strong* involutions (eigenspace for the eigenvalue -1 has dimension between $n/3$ and $2n/3$) with probability at least $c/\log n$ for an absolute constant c [33]. Moreover, by [40], if

$G \cong \mathrm{GL}_n(q)$ and $i \in G$ is a strong involution, then $\zeta_0^i(g)$ is a strong involution with probability at least $c/\log n$ for an absolute constant c. By [39], we have that constant number of strong involutions generate the semisimple socle of the centralisers of involutions with probability $1-1/q^n$. A similar result is expected to hold for the rest of the classical groups.

We shall note here that the map ζ_0 plays a crucial role in our construction of Curtis-Phan-Tits system. Recall that ζ_0^i produces involutions in $C_G(i)$, and we use ζ_0^i for a classical involution $i \in G$ to produce a new classical involution $j \in N_G(K)\backslash C_G(K)$ where K is the long root $\mathrm{SL}_2(q)$-subgroup containing i. With the long root $\mathrm{SL}_2(q)$-subgroup L containing j, we have $\langle K, L\rangle \cong \mathrm{SL}_3^{\varepsilon}(q)$, see Lemmas 6.5, 6.10 and 6.11. This is the base of our construction.

The following simple lemma will be used frequently in the sequel.

Lemma 5.2 *[47, Lemma 5.1] Let G be a finite group and $i \in G$ be an involution. Then the image of ζ_0^i does not contain involutions from the coset $iZ(G)$.*

6 Probabilistic estimates and other results

In this section, we obtain estimates that we need for a polynomial time algorithm constructing Curtis-Phan-Tits systems for black box classical groups. The estimates are far from being sharp, see Lemmas 6.6, 6.7, 6.12, 6.14, and as some computer experiments in GAP suggests, we believe that the actual probabilities are much bigger.

Lemma 6.1 *Let T be a torus in G inverted by an involution $i \in G$ and $S = \{x \in T \mid x \text{ is regular and } x = t^2 \text{ for some } t \in T\}$. Then the proportion of elements of the form ii^g for random $g \in G$ is at least*

$$\frac{|S|^2|C_G(i)|^2}{2|N_G(T)||G|}.$$

Proof. We follow the same idea in the proof of Lemma 2.9 in [1], see also Theorem 8.1 in [47]. Consider the map

$$\begin{aligned} \varphi : i^G \times i^G &\to G \\ (i^g, i^h) &\mapsto i^g i^h. \end{aligned}$$

Let $x \in T$ and $x = t^2$ for some $t \in T$. Since i inverts T,

$$ii^t = it^{-1}it = tt = x.$$

Hence the image of φ contains all the elements of the form t^2 where $t \in T$.

Let $x \in S$, that is, x is regular and $x = t^2$ for some $t \in T$. Then, we claim that $|\varphi^{-1}(x)| \geqslant |S|/2$. Observe that $i^h i^{th} = (ii^t)^h = (tt)^h = x^h = x$ for any $h \in T$. Moreover, since i inverts T, $i^{h_1} = i^{h_2}$ for some $h_1, h_2 \in T$ if and

only if $h_1 = h_2$ or $h_1^2 = h_2^2$. Therefore there are at least $|S|/2$ distinct pairs of involutions (i^h, i^{th}) which map to x. Hence the claim follows.

Let R the set of all regular elements in G whose elements are conjugate to elements in S, then

$$|R| = |G : N_G(T)||S|,$$

and the proportion of pairs of involutions which are mapped to R is

$$\frac{|\varphi^{-1}(R)|}{|i^G \times i^G|} \geqslant \frac{|R||S||C_G(i)|^2}{2|G|^2} = \frac{|S|^2|C_G(i)|^2}{2|N_G(T)||G|}.$$

The results follow from the identity $i^g i^h = (ii^{hg^{-1}})^g$. □

Lemma 6.2 *Let G be a group and $i \in G$ be an involution. Assume that $1 \neq j = \zeta_0^i(g)$ for some $g \in G$. Then the proportion of elements of the form ii^h for random $h \in G$ belonging to $C_G(j)$ is at most $|1/|C_G(i)|$.*

Proof. By the definition of the map $\zeta_0^i(g)$, $i \in C_G(j)$ which implies that $ii^h j = jii^h$ if and only if $i^h j = ji^h$. Since the number of conjugates of i is $|G|/|C_G(i)|$, the result follows. □

6.1 Groups of type A_{n-1}

Lemma 6.3 *Assume that $G \cong \mathrm{PSL}_n^\varepsilon(q)$ where $n \geqslant 3$ and $n \neq 4$. Let K be a long root $\mathrm{SL}_2(q)$-subgroup of G and i be the unique classical involution in K. Assume also that $\zeta_0^i(g) \neq 1$ for some $g \in G$. Then $\zeta_0^i(g) \notin C_G(K)$ if and only if $\zeta_0^i(g)$ is a classical involution in G. Moreover, $\zeta_0^i(g) \in N_G(K)$.*

Proof. We prove the claim when $G \cong \mathrm{PSL}_n(q)$ and the case $G \cong \mathrm{PSU}_n(q)$ is analogous.

Assume that $\zeta_0^i(g) \neq 1$ for some $g \in G$. If $n \geqslant 5$, then the subgroup $\langle K, K^g \rangle$ is contained in a subgroup $L \cong \mathrm{SL}_4(q)$ and the involutions in L are either classical in G or the central involution in L. Hence if $\zeta_0^i(g) \notin C_G(K)$, then $\zeta_0^i(g)$ is a classical involution. Conversely, assume that $\zeta_0^i(g)$ is a classical involution in G. Notice that the only classical involutions in L which commute with K belong to $iZ(L)$. By Lemma 5.2, $\zeta_0^i(g) \notin iZ(L)$ for any $g \in L$. Hence $\zeta_0^i(g) \notin C_G(K)$.

If $G \cong \mathrm{PSL}_3(q)$, then all involutions are conjugate and classical. Thus $\zeta_0^i(g)$ is a classical involution. Conversely, the only classical involution in G which commutes with K is the involution $i \in K$, and $\zeta_0^i(g) \neq i$ for any $g \in G$ by Lemma 5.2.

By Theorem 2.1, $C_G(i) = N_G(K)$ so $\zeta_0^i(g) \in N_G(K)$. □

Remark 6.4 Assume that $G \cong \mathrm{PSL}_4(q)$. If i is a classical involution in G, then the involutions of the form $\zeta_0^i(g)$ are not necessarily classical involutions. However, it is clear that the image of $\zeta_0^i(G)$ contains classical involutions. There

are three conjugacy classes of involutions which are of type t_1, t_2 (classical) and t_2' in G. Note that involutions of type t_2' exists in G exactly when $q \equiv -1 \bmod 4$ and they are conjugate to

$$j = \begin{bmatrix} 0 & I_2 \\ -I_2 & 0 \end{bmatrix} Z.$$

Assume that

$$i = \begin{bmatrix} -I_2 & 0 \\ 0 & I_2 \end{bmatrix} Z$$

then i is conjugate to

$$t = \begin{bmatrix} 0 & -I_2 \\ -I_2 & 0 \end{bmatrix} Z,$$

say $t = i^g$ for some $g \in G$. Now $j = it = ii^g = \zeta_0^i(g)$ is an involution in $\mathrm{PSL}_4(q)$ which is of type t_2' in $\mathrm{PSL}_4(q)$.

Lemma 6.5 *Assume that $G \cong \mathrm{PSL}_n^\varepsilon(q)$ where $n \geqslant 4$. Let K_1 and K_2 be two long root $\mathrm{SL}_2(q)$-subgroups of G containing the classical involutions i_1 and i_2, respectively. If i_1 and i_2 commute with each other and $i_2 \notin C_G(K_1)$, then $\langle K_1, K_2\rangle \cong \mathrm{SL}_3^\varepsilon(q)$. If $G \cong \mathrm{PSL}_3^\varepsilon(q)$, then $\langle K_1, K_2\rangle = G$.*

Proof. Let $G \cong \mathrm{SL}_n(q)$, $n \geqslant 4$, and V be the natural module for G. Let $V = V_-^1 \oplus V_+^1 = V_-^2 \oplus V_+^2$ where $V_\pm^1$ and $V_\pm^2$ are the eigenspaces of the involutions i_1 and i_2 corresponding to the eigenvalues ± 1, respectively. We assume that $\dim V_-^1 = \dim V_-^2 = 2$ since i_1 and i_2 are classical involutions. Notice that $\langle i_1, i_2\rangle < \mathrm{SL}(V_-^1 + V_-^2)$. Since $i_2 \in C_G(i_1)$, we have $i_2 \in N_G(K_1)$ by Theorem 2.1 so i_2 leaves invariant the subspaces V_-^1, V_+^1. Moreover, $[i_2, V_-^1] \neq 0$ since $i_2 \notin C_G(K_1)$. Now, if $\dim[i_2, V_-^1] = 2$, then $i_1 = i_2$. Therefore we have $\dim[i_2, V_-^1] = 1$ which implies that $\dim(V_-^1 + V_-^2) = 3$ and $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$. The proof is analogous for $G \cong \mathrm{PSU}_n(q)$ and $\mathrm{PSL}_3^\varepsilon(q)$. □

Lemma 6.6 *Assume that $G \cong \mathrm{PSL}_n^\varepsilon(q)$ where $n \geqslant 3$. Let K be a long root $\mathrm{SL}_2(q)$-subgroup of G and i be the unique involution in K. Then the probability of finding an element $g \in G$, where $\zeta_0^i(g)$ is a classical involution, is at least $1/750(1 - 2/q)$.*

Proof. Assume first that $n \geqslant 5$. For $g \in G$, the subgroup $\langle i, i^g\rangle$ is contained in a subgroup L isomorphic to $\mathrm{SL}_4^\varepsilon(q)$. Indeed, for a random element $g \in G$, we have $L = \langle K, K^g\rangle \cong \mathrm{SL}_4^\varepsilon(q)$ with probability at least $1 - 2/q$, see Theorem 7.1. Therefore, it is enough to find the estimate in $\mathrm{SL}_4(q)$ and $\mathrm{SU}_4(q)$.

Assume that $L \cong \mathrm{SL}_4(q)$. Then L has a subgroup of the form $N = N_1 \times N_2$ where $N_1 \cong N_2 \cong \mathrm{SL}_2(q)$ and i acts as an involution of type t_1 on both N_1 and N_2. It is clear that i inverts a torus of order $q \pm 1$ on N_1 and N_2.

Assume that $q \equiv 1 \bmod 4$ and consider a torus $T = T_1 \times T_2 \leqslant N = N_1 \times N_2$ where T is inverted by i and $|T_1| = q-1$ and $|T_2| = (q+1)/2$. Observe that T is uniquely contained in a maximal torus of order $(q-1)^2(q+1)$. Since $(q+1)/2$ is

odd, the involution in T belongs to N_1 and hence it is a classical involution. It is clear that this involution does not centralise K. Now, observe that $|N_L(T)| = 4(q-1)^2(q+1)$, $|C_L(i)| = q^2(q+1)^2(q-1)^3$ and $|L| = q^6(q^2-1)(q^3-1)(q^4-1)$. Setting

$$S = \{x \in T \mid x \text{ is regular, } |x| \text{ is even and } x = t^2 \text{ for some } t \in T\}$$

we have $|S| \geqslant |T|/4 = (q^2-1)/8$. By Lemma 6.1, ii^g has even order and $\zeta_0^i(g)$ is a classical involution with probability at least

$$\begin{aligned}\frac{|S|^2|C_L(i)|^2}{2|N_L(T)||L|} &= \frac{\frac{(q^2-1)^2}{64}q^4(q+1)^4(q-1)^6}{8(q-1)^2(q+1)q^6(q^2-1)(q^3-1)(q^4-1)} \\ &= \frac{1}{512}\frac{(q^2-1)^2}{q^4+q^2}\frac{q^2-1}{q^2+q+1} \\ &\geqslant \frac{1}{750}\end{aligned}$$

since $q \geqslant 5$.

If $q \equiv -1 \bmod 4$, then we consider a torus $T = T_1 \times T_2 \leqslant N$ where T is inverted by i and $|T_1| = (q-1)/2$ and $|T_2| = q+1$. The rest of the proof is same as above.

The proof is the same for the groups $L \cong \mathrm{SU}_4(q)$.

The computations in the case $L \cong \mathrm{PSL}_4(q)$ are analogous, namely, we consider the central product $N = N_1 \circ_2 N_2$ and apply the above arguments. If $L \cong \mathrm{PSL}_3(q)$, then the only involution in $C_L(i)$ which centralise the component $\mathrm{SL}_2(q)$ is the involution i itself. Therefore, for any $g \in L$, if $\zeta_0^i(g) \neq 1$ or equivalently ii^g has even order, then $\zeta_0^i(g)$ does not centralise K since $\zeta_0^i(g) \neq i$ by Lemma 5.2. The proportion of the elements $g \in L$ such that ii^g has even order is at least $1/750$ by the similar computations.

The cases $\mathrm{PSU}_n(q)$ for $n = 3, 4$ are similar. □

Lemma 6.7 *Let $G \cong \mathrm{PSL}_n^\varepsilon(q)$, $n \geqslant 3$, and i be an involution of type t_1. Then ii^g has even order with probability at least 1/30 for a random element $g \in G$. Moreover, $\zeta_0^i(g)$ is a classical involution in G.*

Proof. Observe that $\langle i, i^g\rangle \leqslant L$ where $L \cong \mathrm{SL}_2(q)$. Therefore it is enough to find the estimate in L. Observe also that i inverts a torus $T \leqslant L$ of order $q \pm 1$. Assume that $q \equiv 1 \bmod 4$, the other case is analogous. Then take a torus T of order $q-1$ which is inverted by i. Note that $|N_G(T)| = 2|T|$ and $|C_G(i)| = 2(q-1)$. Let

$$S = \{x \in T \mid x \text{ is regular, } |x| \text{ even, and } x = t^2 \text{ for some } t \in T\}.$$

Since T is cyclic and all elements are regular, $|S| \geqslant |T|/4$. By Lemma 6.1, ii^g has even order with probability at least

$$\begin{aligned}\frac{|S|^2|C_L(i)|^2}{2|N_L(T)||L|} &\geqslant \frac{4(q-1)^4}{64q(q-1)^2(q+1)}\\ &= \frac{(q-1)^2}{16q(q+1)}\\ &\geqslant \frac{1}{30}\end{aligned}$$

since $q \geqslant 5$. Since $\zeta_0^i(g)$ is an involution and $\zeta_0^i(g) \in L$, it must be a classical involution. □

6.2 Groups of type B_n and D_n

In this section we deal with all types of orthogonal groups simultaneously and we simply write $\mathrm{P}\Omega_n^\varepsilon(q)$, $\varepsilon = \pm$, to denote orthogonal groups of any type. If n is even, $\mathrm{P}\Omega_n^+(q)$ (resp. $\mathrm{P}\Omega_n^-(q)$) is the orthogonal group where the underlying vector space has Witt index $n/2$ (resp. $n/2-1$). If n is odd, ε should be ignored.

Lemma 6.8 *Assume that $G \cong \mathrm{P}\Omega_n^\varepsilon(q)$ where $n \geqslant 7$. Let K be a long root $\mathrm{SL}_2(q)$-subgroup of G and i be the unique classical involution in K. If $1 \neq \zeta_0^i(g) \notin C_G(K)$ for some $g \in G$, then $\zeta_0^i(g)$ is an involution of type t_1, t_2 (classical), t_3 or t_4 (in $\mathrm{P}\Omega_8^+(q)$).*

Proof. Let V be the natural module for $G \cong \Omega_n^\varepsilon(q)$ and $V_\pm$ be the eigenspaces of the involution i for the eigenvalues ± 1. Then $\dim V_- = 4$. Observe that $\langle i, i^g\rangle < L \cong \Omega(V_- + V_-^g)$ and $\dim(V_- + V_-^g) \leqslant 8$. Therefore the involution $\zeta_0^i(g) = \mathrm{i}(ii^g)$ is of type t_1, t_2, t_3 or t_4. If $n \geqslant 9$ and $\dim(V_- + V_-^g) = 8$, then i commutes with i^g and $\zeta_0^i(g) = ii^g \in C_L(K)$. Note that if $G \cong \Omega_7(q)$, then this case does not occur. If $G \cong \mathrm{P}\Omega_8^+(q)$, then the involutions of type t_3 and t_4 have orders 4 in $\Omega_8^+(q)$. □

Remark 6.9 Let $G \cong \mathrm{P}\Omega_8^+(q)$ and $K = K_1$ be a long root $\mathrm{SL}_2(q)$-subgroup containing the classical involution i. Then

$$C_G(i) = (((K_1 \circ_2 K_2) \circ_2 (K_3 \circ_2 K_4)) \rtimes \langle j_1, j_2\rangle) \rtimes \langle t\rangle$$

where $K_s \cong \mathrm{SL}_2(q)$ for $s = 1, \ldots, 4$. Here, j_1 (resp. j_2) are involutions of type t_1 interchanging K_1 and K_2 (resp. K_3 and K_4), and t is a classical involution interchanging $K_1 \circ_2 K_2$ and $K_3 \circ_2 K_4$. Notice that $j = j_1 j_2$ is a classical involution. Therefore, unlike in the case of $(\mathrm{P})\mathrm{SL}_n^\varepsilon(q)$, not all classical involutions in $C_G(i)$ belongs to $N_G(K)$, see Theorem 2.1. Moreover, since j and t are classical involutions, there exist $g_1, g_2 \in G$ such that $j = i^{g_1}$ and $t = i^{g_2}$, and $\zeta_0^i(g_1) = ij, \zeta_0^i(g_2) = it \notin N_G(K)$. However if a classical involution $z \in C_G(i)$ does not belong to $N_G(K)$, then $N = \langle K, K^z\rangle \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$. To decide whether a classical involution in $C_G(i)$ belongs to $N_G(K)$, we check whether the subgroup N contains elements of order dividing $q^2 - 1$ but not $q - 1$ and $q + 1$.

Lemma 6.10 *Assume that $G \cong \mathrm{P}\Omega_n^\varepsilon(q)$ where $n \geqslant 7$. Let K_1 and K_2 be two long root $\mathrm{SL}_2(q)$-subgroups of G containing the classical involutions i_1 and i_2, respectively. If i_1 and i_2 commute with each other and $i_2 \in N_G(K_1) \backslash C_G(K_1)$, then $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$.*

Proof. Let $G \cong \Omega_n^\varepsilon(q)$ and V be the natural module for G. Let $V = V_-^1 \oplus V_+^1 = V_-^2 \oplus V_+^2$ where $V_\pm^1$ and $V_\pm^2$ are the eigenspaces of the involutions i_1 and i_2 corresponding to the eigenvalues ± 1, respectively. We assume that $\dim V_-^1 = \dim V_-^2 = 4$ since i_1 and i_2 are classical involutions.

Since $i_2 \in N_G(K_1)$, i_2 induces an involution on $\Omega(V_-^1)$ and the induced quadratic form on $W = V_-^1 + V_-^2$ is non-degenerate. Moreover, since i_1 and i_2 are commuting with each other, we have $\dim(V_-^1 \cap V_-^2) = 0, 2$ or 4 which implies that $\dim(W) = 4, 6$ or 8. It is clear that $\langle i_1, i_2\rangle < \langle K_1, K_2\rangle \leqslant \Omega(W)$. If $\dim W = 4$, then $V_-^1 = V_-^2$ and $i_1 = i_2$. Moreover, if $\dim W = 8$, then $V_-^1 \cap V_-^2 = \{0\}$ and $i_2 \in C_G(K_1)$. Note that this case does not happen when $n = 7$. Hence $\dim W = 6$. Now since $\mathrm{P}\Omega(W) = \mathrm{P}\Omega_6^\pm(q) \cong \mathrm{PSL}_4^\varepsilon(q)$, the result follows from Lemma 6.5. □

Lemma 6.11 *Assume that $G \cong \mathrm{P}\Omega_n^\varepsilon(q)$ where $n \geqslant 9$ or $G \cong \mathrm{P}\Omega_8^+(q)$. Let K_1, K_2, K_3 be long root $\mathrm{SL}_2(q)$-subgroups of G containing the classical involutions i_1, i_2, i_3, respectively. Assume also that $[K_1, K_3] = 1$, $i_2 \in (N_G(K_1) \cap N_G(K_3)) \backslash\ (C_G(K_1) \cup C_G(K_3))$ and the involutions i_k, $k = 1, 2, 3$, mutually commute with each other. Then,*

(1) if $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$, then $\langle K_2, K_3\rangle \cong \mathrm{SL}_3(q)$, or

(2) if $\langle K_1, K_2\rangle \cong \mathrm{SU}_3(q)$, then $\langle K_2, K_3\rangle \cong \mathrm{SU}_3(q)$.

Proof. Let $G \cong \Omega_n^\varepsilon(q)$, $n \geqslant 9$, and V be the natural module for G. Let $V_\pm^k$ be the eigenspaces of the involutions i_k, $k = 1, 2, 3$, corresponding to the eigenvalues ± 1. Since $i_2 \in (N_G(K_1) \cap N_G(K_3)) \backslash (C_G(K_1) \cup C_G(K_3))$, $W = (V_-^1 + V_-^2 + V_-^3) = (V_-^1 + V_-^3)$ and W is an orthogonal 8-space with Witt index 4. Moreover $\langle K_1, K_2, K_3\rangle \leqslant \Omega(W)$.

Observe that $\langle K_1, K_2\rangle \leqslant \Omega(W_1)$ and $\langle K_2, K_3\rangle \leqslant \Omega(W_2)$ where $W_1 = (V_-^1 + V_-^2)$ and $W_2 = (V_-^2 + V_-^3)$. By the proof of Lemma 6.10, W_1 and W_2 are orthogonal 6-spaces with Witt indices 2 or 3. Hence $W_1 = V_-^2 \perp U$ where $U < V_-^1$ is either a hyperbolic plane or it does not contain any singular vectors. Moreover, $W = U \perp W_2$ since $W_1 \cap W_2 = V_-^2$.

If $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$, then it is clear that W_1 is an orthogonal 6-space with Witt index 3, and so U is a hyperbolic plane. Since W has Witt index 4 and $W = U \perp W_2$, W_2 is also an orthogonal 6-space with Witt index 3. Thus since $\langle K_2, K_3\rangle \leqslant \Omega(W_2)$ and $\mathrm{P}\Omega(W_2) \cong \mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$, we have $\langle K_2, K_3\rangle \cong \mathrm{SL}_3(q)$ by Lemma 6.5.

If $\langle K_1, K_2\rangle \cong \mathrm{SU}_3(q)$, then W_1 is an orthogonal 6-space with Witt index 2, and so U does not contain any singular vectors. Since W has Witt index 4 and $W = U \perp W_2$, W_2 is also an orthogonal 6-space with Witt index 2. Thus since $\langle K_2, K_3\rangle \leqslant \Omega(W_2)$ and $\mathrm{P}\Omega(W_2) \cong \mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$, we have $\langle K_2, K_3\rangle \cong \mathrm{SL}_3(q)$ by Lemma 6.5.

The proof for $\mathrm{P}\Omega_8^+(q)$ is similar. □

Lemma 6.12 *Assume that $G \cong \mathrm{P}\Omega_n^\varepsilon(q)$ where $n \geqslant 7$. Let K be a long root $\mathrm{SL}_2(q)$-subgroup of G and i be the unique classical involution in K. Then the probability of finding an element $g \in G$ where $\zeta_0^i(g)$ is a classical involution and $\zeta_0^i(g) \in N_G(K)$ is bounded from below by $(1/2^{16} - 1/q^{11})(1 - 2/q)$.*

Proof. Assume first that $n \geqslant 9$. Take $g \in G$ and consider the subgroup $L = \langle K, K^g \rangle$. By Theorem 7.1, $L \cong \Omega_8^+(q)$ with probability at least $1 - 2/q$. Since $\zeta_0^i(g) \in L$, it is enough to find the estimate in $\Omega_8^+(q)$. Assume now that $L \cong \Omega_8^+(q)$, then L contains a subgroup of the form $N = N_1 \times N_2$ where $N_1 \cong N_2 \cong \Omega_4^+(q)$ and $i \in N_L(N_1) \cap N_L(N_2)$ acting as an involution of type t_1 on both N_1 and N_2. Observe that an involution of type t_1 in $\Omega_4^+(q)$ inverts a torus of order $(q \pm 1)^2/2$.

Assume that $q \equiv 1 \bmod 4$ and consider a torus $T = T_1 \times T_2 \leqslant N = N_1 \times N_2$ where T is inverted by i and $|T_1| = (q-1)^2/2$ and $|T_2| = (q+1)^2/4$. Observe that T is a maximal torus of L. Since $(q+1)^2/4$ is odd, involutions in T belong to $T_1 < N_1$ and hence they are of type t_1 or t_2 in L. Observe also that the torus $T_1 = \frac{1}{2}P_1P_2$ where $|P_1| = |P_2| = q - 1$. Hence an element $g = (g_1, g_2) \in T_1$ powers upto an involution of type t_2 in L if and only if the 2-heights of g_1 and g_2 are same. Now it is easy to see that the probability of a random element which powers upto an involution of type t_2 is at least $1/4$. Now we have $|N_L(T)| = 32|T|$. Moreover, $|C_L(i)| = 4|\Omega_4^+(q)|^2 = q^4(q^2-1)^4$ and $|L| = q^{12}(q^6-1)(q^4-1)^2(q^2-1)/2$. Let S be the regular semisimple elements of even order of the form t^2 for some $t \in T$. Then $|S| \geqslant |T|/4$. Hence, by Lemma 6.1, ii^g has even order and $\zeta_0^i(g)$ is a classical involution for a random element $g \in L$ with probability at least

$$\begin{aligned}
\frac{1}{4} \cdot \frac{|S|^2|C_L(i)|^2}{2|N_L(T)||L|} &\geqslant \frac{1}{8} \frac{\frac{(q^2-1)^4}{1024} q^8 (q^2-1)^8}{\frac{32(q^2-1)^2}{8} q^{12}(q^6-1)(q^4-1)^2(q^2-1)} \\
&= \frac{1}{32768} \cdot \frac{(q^2-1)^2}{q^4} \cdot \frac{(q^2-1)^2}{(q^2+1)^2} \cdot \frac{(q^2-1)^2}{q^4+q^2+1} \\
&\geqslant \frac{1}{32768} \cdot \frac{8}{9} \cdot \frac{6}{8} \cdot \frac{6}{7} \\
&\geqslant \frac{1}{2^{16}}.
\end{aligned}$$

Now we shall find an upper bound for the proportions of elements $g \in L$ where $\zeta_0^i(g)$ is a classical involution and $\zeta_0^i(g) \notin N_L(K)$. Setting $K = K_1$, we have $C_L(i) = (K_1 \circ_2 K_2) \times (K_3 \circ_2 K_4) \rtimes \langle j_1, j_2 \rangle$. Recall that j_1 and j_2 are involutions of type t_1 in L commuting with each other (see Remark 6.9). The involution j_1 (resp. j_2) interchanges K_1 and K_2 (resp. K_3 and K_4) and fixes K_3 and K_4 (resp. K_1 and K_2). Hence $j = j_1j_2$ is a classical involution since it is a product of two commuting involutions of type t_1 acting on disjoint subspaces. Clearly $j \notin N_L(K)$. Moreover, the only classical involutions in $C_L(i)$ which do not belong to $N_L(K)$ are j and jz where $z \in Z(C_L(i))$ is an involution. By

Lemma 6.2, the proportion of elements $g \in L$ satisfying $\zeta_0^i(g) = j$ or jz is at most $4/|C_L(i)| < 1/q^{11}$. Thus $\zeta_0^i(g)$ is a classical involution belonging to $N_G(K)$ with probability at least $(1/2^{16} - 1/q^{11})(1 - 2/q)$.

If $G \cong \mathrm{P}\Omega_8^+(q)$, then $L = G$ with probability at least $1 - 2/q$ by Theorem 7.1. By the same computations as above, we have $\zeta_0^i(g)$ is classical with probability at least $1/2^{16}$. Note that, by Remark 6.9, there is another classical involution in $C_L(i)$ which interchanges $K_1 \circ_2 K_2$ and $K_3 \circ_2 K_4$. However the same computations above yield the same estimate.

Assume that $G \cong \mathrm{P}\Omega_8^-(q)$. Then $L = G$ with probability at least $1 - 2/q$ by Theorem 7.1. In this case L contains a subgroup of the form $N = N_1 \times N_2$ where $N_1 \cong \Omega_4^-(q)$ and $N_2 \cong \Omega_4^+(q)$. Let $i = (j_1, j_2) \in N$ be an involution where $j_1 \in N_1$ and $j_2 \in N_2$ are involutions of type t_1 in L. Now j_1 inverts a torus of order $(q^2 \pm 1)/2$ in N_1 and j_2 inverts a torus of order $(q \pm 1)/2$ in N_2. Hence, by taking a torus of order $(q^2+1)/2$ in N_1 and a torus of order $(q-1)/2$ or $(q+1)/2$ in L_2 depending on $q \equiv 1$ or $3 \bmod 4$, respectively, the proof follows from the same computations as above.

If $G \cong \Omega_7(q)$, then $L = G$ with probability at least $1 - 2/q$ by Theorem 7.1. Consider the subgroup $N = N_1 \times N_2 \leqslant L$ where $N_1 \cong \Omega_4^-(q)$ and $N_2 \cong \Omega_3(q)$. Let j_1 and j_2 be involutions of type t_1 in N_1 and N_2, respectively. Then j_1 inverts a torus of order $(q^2 \pm 1)$ and j_2 inverts a torus of order $(q \pm 1)$. The result follows from the same computations. □

Lemma 6.13 *Let $G \cong \mathrm{P}\Omega_n^\varepsilon(q)$, $n \geqslant 5$ and K be a long root $\mathrm{SL}_2(q)$-subgroup in G. Let i be the unique involution in K. Then the proportion of elements $g \in C_G(i)$ such that $\langle K, K^g \rangle \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ is at least 1/8.*

Proof. Recall that $C_G(i)'' = K\tilde{K}L$ where $L \cong \Omega_{n-4}^\varepsilon(q)$. By [21, Table 4.5.1], there exists an involution $t \in C_G(i)$ which interchanges K and $\tilde{K}$. Hence the elements which belong to the coset $tC_G(i)''$ interchanges K and $\tilde{K}$ and the result follows from the fact that $|C_G(i) : C_G(i)''| \leqslant 8$. □

Lemma 6.14 *Let $G \cong \mathrm{P}\Omega_n^\varepsilon(q)$, $n \geqslant 5$, and i be an involution of type t_1. Then the probability of finding an element $g \in G$ such that $\zeta_0^i(g)$ is a classical involution is at least 1/960.*

Proof. By the proof of [29, Lemma 4.12 (i)], $\langle i, i^g \rangle \leqslant L \cong \Omega_4^+(q)$ with probability at least 1/32. Since i acts as an involution of type t_1 on the components of L, the result follows from Lemma 6.7. □.

6.3 Groups of type C_n

Recall that the group $G = \mathrm{PSp}_{2n}(q)$ contains maximal tori of order $(q^n-1)/2$ and $(q^n+1)/2$ corresponding to maximal positive and negative cycle of length n in the Weyl group, respectively. We call these tori *maximal twisted tori* and write $\frac{1}{2}T_{q^n \pm 1}$.

Lemma 6.15 *[1, Lemma 2.13] The involutions in maximal twisted tori $\frac{1}{2}T_{q^n\pm 1}$ are of type t_n.*

Lemma 6.16 *The number of regular elements belonging to a maximal twisted torus is at least $\frac{1}{5n}|G|$.*

Proof. This is Lemma 2.3 in the corrected version of [1]. □

Lemma 6.17 *Assume that $G \cong \mathrm{PSp}_{2n}(q)$ and K be a short root $\mathrm{SL}_2(q)$-subgroup of G.*

1. *If $n \geqslant 3$, then $K \cong \mathrm{SL}_2(q)$ and $C_G(i)'' \cong \mathrm{Sp}_4(q) \circ_2 \mathrm{Sp}_{2n-4}(q)$ where i is the unique involution in K.*
2. *If $n = 2$, then $K \cong \mathrm{PSL}_2(q)$.*

Proof. (1) Since $n \geqslant 3$, $K \cong \mathrm{SL}_2(q)$ by Table 2. Let V be the underlying symplectic geometry. Note that K acts irreducibly on a totally isotropic subspace of dimension 2. Let i be the involution in K then $K \leqslant \mathrm{Sp}(V_-)$ where V_- be the eigenspace of i corresponding to the eigenvalue -1. Since V_- is non-degenerate, $\mathrm{Sp}(V_-) = \mathrm{Sp}_4(q)$ and $C_G(i)'' \cong \mathrm{Sp}_4(q) \circ_2 \mathrm{Sp}_{2n-4}(q)$.

(2) Since $\mathrm{PSp}_4(q) \cong \Omega_5(q)$, the result follows from Table 2. □

Lemma 6.18 *Let $G \cong \mathrm{PSp}_4(q)$ and $i \in G$ be an involution of type t_2, then the probability of producing a classical involution $j \in C_G(i)$ by the map ζ_0^i which does not centralise K is bounded from below by the constant $1/768$.*

Proof. Let $G = \mathrm{Sp}_4(q)$ and V be the natural module for G. Write $V = V_1 \perp V_2$ where V_1 and V_2 are hyperbolic planes. Then $\mathrm{Sp}(V_1) \cong \mathrm{Sp}(V_2) \cong \mathrm{SL}_2(q)$. Consider the tori $T_1 \leqslant \mathrm{Sp}(V_1)$ and $T_2 \leqslant \mathrm{Sp}(V_2)$ where $|T_1| = |T_2| = q-1$ or $q+1$ when $q \equiv 1 \bmod 4$ or $q \equiv -1 \bmod 4$, respectively. It is clear that the involutions in T_1 and T_2 are classical involutions.

Now let $G \cong \mathrm{PSp}_4(q)$ and consider the image $\bar{T}$ of $T = T_1 \times T_2$ in G. We have $\bar{T} = \frac{1}{2}(T_1 \times T_2)$. By [1, Lemma 2.8], there exists $j \in i^G$ such that $\bar{T}$ is inverted by j. Let

$$S = \{x \in \bar{T} \mid x \text{ is regular, } |x| \text{ even, and } x = t^2 \text{ for some } t \in \bar{T}\}.$$

Then $|S| \geqslant |\bar{T}|/8$. Moreover $|N_G(\bar{T})| = 4|\bar{T}|$ and $C_G(j)| = \frac{1}{2}q(q-1)^2(q+1)$. Therefore, by Lemma 6.1, the elements of the form ii^g, which have even order, is at least

$$\begin{aligned}\frac{|S||T||C_G(j)|^2}{2|N_G(T)||G|} &= \frac{q^2(q-1)^6(q+1)^2}{128q^4(q^2-1)(q^4-1)} \\ &= \frac{(q-1)^4}{128q^2(q^2+1)} \\ &\geqslant \frac{1}{128}\cdot\frac{1}{3} = \frac{1}{384}\end{aligned}$$

since $q \geqslant 5$. Note that at least half of the elements $\zeta_0^j(g)$ belong to only T_1 or T_2 and the result follows. □

7 Preliminary algorithms

7.1 Probabilistic recognition of classical groups

A probabilistic recognition algorithm for finite simple groups of Lie type, that is, computation of their standard names, is presented in [5] by using the order oracle. The idea is based on the analysis of the statistics of element orders, which are specific for each group of Lie type except for the groups $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$. This approach fails to distinguish these two classes of groups since, especially when the size of the field is large, random elements are regular semisimple with probability close to 1 and the statistics of orders of regular semisimple elements are virtually the same for $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$, see [1] for thorough discussion. To complete the recognition problem for all finite simple groups of Lie type Altseimer and Borovik presented an algorithm distinguishing $\mathrm{PSp}_{2n}(q)$ from $\Omega_{2n+1}(q)$, q odd, by using the centralisers of involutions and conjugacy classes in these groups [1].

We present an alternative probabilistic recognition algorithm for black box classical groups of odd characteristic. The algorithm determines the type of the given black box classical group G, that is, it decides whether G is linear, unitary, symplectic or orthogonal without using the order oracle. This procedure is necessary in the construction of the Curtis-Phan-Tits system of G, see Remark 8.1.

Let p be prime and $k \geqslant 2$, then there is a prime dividing $p^k - 1$ but not $p^i - 1$ for $1 \leqslant i < k$, except when either $p = 2$, $k = 6$, or $k = 2$ and p is a Mersenne prime. Such a prime is called *primitive prime divisor* of $p^k - 1$. In our algorithm we are concerned with the primitive prime divisors of $q^a - 1$ where $q = p^k$ for some $k \geqslant 1$. It is clear from the definition that each primitive prime divisor of $p^{ak} - 1$ is a primitive prime divisor of $q^a - 1$. An integer which is a primitive prime divisor of $q^a - 1$ is said to have *primitive prime divisor rank* a. If the order of a group element g has primitive prime divisor rank a, then we say that g has primitive prime divisor rank a and we write $\mathrm{pdrank}(g) = a$.

Our algorithm is based on the following result.

Theorem 7.1 *Let G be finite simple classical group of odd characteristic and K be a long root $\mathrm{SL}_2(q)$-subgroup. Let $L = \langle K, K^g \rangle$ for a random element $g \in G$. Then, with probability at least $1 - 2/q$, the followings hold.*

1. *If $G \cong \mathrm{PSL}^{\varepsilon}_n(q)$, then $L \cong (\mathrm{P})\mathrm{SL}^{\varepsilon}_4(q)$ for $n \geqslant 4$; $L = G$ for $n = 2, 3$.*
2. *If $G \cong \mathrm{PSp}_{2n}(q)$, then $L \cong (\mathrm{P})\mathrm{Sp}_4(q)$ for $n \geqslant 2$.*
3. *If $G \cong \Omega_{2n+1}(q)$ or $\mathrm{P}\Omega^{\pm}_{2n}(q)$, then $L \cong (\mathrm{P})\Omega^{+}_8(q)$ or $L = G \cong \mathrm{P}\Omega^{-}_8(q)$ for $n \geqslant 4$; $L = G$ for $n \leqslant 3$.*

Proof. This is combination of the results presented in [47, Section 3].

Theorem 7.2 *Let G be a simple black box classical group of odd characteristic. Then there exists a polynomial time Monte–Carlo algorithm which computes the type of G.*

Proof. Let $G \cong \mathrm{PSL}_n^{\varepsilon}(q), \mathrm{PSp}_{2n}(q)$, $\Omega_{2n+1}(q)$ or $\mathrm{P}\Omega_{2n}^{\varepsilon}(q)$. We construct a long root $\mathrm{SL}_2(q)$-subgroup K in G by [47, Theorem 1.1] and take a random element $g \in G$. Then, with probability at least $1 - 2/q$, the structure of the subgroup $L = \langle K, K^g \rangle$ is determined by Theorem 7.1.

If $n \geqslant 4$, then, by Theorem 7.1, $L \cong (\mathrm{P})\mathrm{SL}_4^{\varepsilon}(q), (\mathrm{P})\mathrm{Sp}_4(q)$ or $(\mathrm{P})\Omega_8^{\pm}(q)$. Consider a subset $S \subset L$ consisting of random elements from L and let $\mathrm{pdrank}(L) = \max\{\mathrm{pdrank}(g) \mid g \in S\}$. By applying the same arguments in the proof of Lemma 2.5 in [29], we can find an element $g \in L$ with maximal primitive prime divisor rank with probability bounded from below by constant, see also [34, Section 6] for more details about the distribution of these elements. It is easy to see that $\mathrm{pdrank}(L) = 2, 3, 4, 6$ or 8. Recall that

$$|\mathrm{SL}_4(q)| = q^6(q^2-1)(q^3-1)(q^4-1),$$

$$|\mathrm{SU}_4(q)| = q^6(q^2-1)(q^3+1)(q^4-1),$$

$$|\mathrm{Sp}_4(q)| = q^4(q^2-1)(q^4-1),$$

$$|\Omega_8^+(q)| = \frac{1}{2}q^{12}(q^4-1)(q^2-1)(q^4-1)(q^6-1),$$

$$|\Omega_8^-(q)| = \frac{1}{2}q^{12}(q^4+1)(q^2-1)(q^4-1)(q^6-1).$$

If $\mathrm{pdrank}(L) = 8$, then $L \cong (\mathrm{P})\Omega_8^-(q)$. Note that there are at least $|(\mathrm{P})\Omega_8^-(q)|/16$ elements of primitive divisor rank 8 by [29, Lemma 2.5 and Section 4.1.5].

We assume now that $L \ncong (\mathrm{P})\Omega_8^-(q)$. If $\mathrm{pdrank}(L) = 6$, then $L \cong (\mathrm{P})\Omega_8^+(q)$, $(\mathrm{P})\mathrm{SU}_4(q)$ or $L = G \cong \mathrm{PSU}_3(q)$, $\Omega_7(q)$. Similarly, the proportion of elements of primitive divisor rank 6 in these groups is at least $1/16$. In $(\mathrm{P})\Omega_8^+(q)$, there are elements of order $(q^4-1)/4$ whereas $(\mathrm{P})\mathrm{SU}_4(q)$, $\mathrm{PSU}_3(q)$ and $\Omega_7(q)$ do not have such elements. Similarly, in $\Omega_7(q)$, there are elements of order q^3-1 where as $(\mathrm{P})\mathrm{SU}_4(q)$, $\mathrm{PSU}_3(q)$ do not have such elements. Note that we do not need to compute the exact orders of the elements. For example, to distinguish $\Omega_7(q)$ from $(\mathrm{P})\mathrm{SU}_4(q)$ and $\mathrm{PSU}_3(q)$, we look for an element $g \in L$ satisfying $g^{q^3-1} = 1$ but $g^{q^4-1} \neq 1$ and $g^{q^3+1} \neq 1$.

If $\mathrm{pdrank}(L) = 4$, then $L \cong (\mathrm{P})\mathrm{SL}_4(q), (\mathrm{P})\mathrm{Sp}_4(q)$. In $\mathrm{SL}_4(q)$, there are at least $|(\mathrm{P})\mathrm{SL}_4(q)|/16$ elements of order $(q^4-1)/4(q-1)$ by [29, Lemma 2.5] whereas $(\mathrm{P})\mathrm{Sp}_4(q)$ does not have such elements.

If $\mathrm{pdrank}(L) = 2$ or 3, then $L = G \cong \mathrm{PSL}_2(q)$ or $\mathrm{PSL}_3(q)$, respectively. □

An important corollary of Theorem 7.2 is an alternative algorithm to Altseimer-Borovik algorithm [1] distinguishing the groups $\mathrm{PSp}_{2n}(q)$ and $\Omega_{2n+1}(q)$.

Corollary 7.3 *Let G be a black box group isomorphic to $\mathrm{PSp}_{2n}(q)$ or $\Omega_{2n+1}(q)$, $q > 3$, q odd, $n \geqslant 3$. Then there is a one sided Monte–Carlo polynomial time algorithm which decides whether G is isomorphic to $\mathrm{PSp}_{2n}(q)$ or not.*

7.2 Recognising classical involutions in black box groups

In this section we present an algorithm which decides whether a given involution in a black box group is classical or not.

Lemma 7.4 *Let L be a finite quasisimple classical group over a field of odd size $q \geqslant 5$, $L \ncong (\mathrm{P})\mathrm{SL}_2(q)$ and $K \cong \mathrm{SL}_2(q)$. Let $G = KL$ be a commuting product of K and L. Given an exponent E for G and the value of q, there exists a polynomial time Monte-Carlo algorithm which constructs K and L.*

Proof. The proof follows from Step 4 of the presentation of Algorithm 6.8 in [47].

Lemma 7.5 *Let G be a commuting product of subgroups isomorphic to $(\mathrm{P})\mathrm{SL}_2(q)$, $q \geqslant 5$ odd. Then there exists a Monte-Carlo algorithm which constructs all components of G.*

Proof. This is [47, Algorithm 6.8] together with the remark following it. □

Lemma 7.6 *Let G be a simple black box classical group over a field of odd size $q \geqslant 5$ and $i \in G$ be an involution. Given an exponent for G and the value of q, there exists a polynomial time Monte-Carlo algorithm which decides whether i is a classical involution or not.*

Proof. By [47, Theorem 1.2], we can check whether a subgroup $K \leqslant G$ isomorphic to $(\mathrm{P})\mathrm{SL}_2(q^k)$ is a long root $\mathrm{SL}_2(q)$-subgroup or not. Recall that the long root $\mathrm{SL}_2(q)$-subgroups are indeed isomorphic to $\mathrm{SL}_2(q)$ and, by definition, the unique involution that belongs to a long root $\mathrm{SL}_2(q)$-subgroup is a classical involution in G.

Let $C = C_G(i)''$. If $i \in G$ is a classical involution, then C is a commuting product of subgroups K and L where $K \cong \mathrm{SL}_2(q)$ and $L \cong \mathrm{SL}_{n-2}(q)$, $\mathrm{Sp}_{2n-2}(q)$, $\mathrm{SL}_2(q) \circ_2 \Omega_{2n-3}(q)$ or $\mathrm{SL}_2(q) \circ_2 \Omega^{\pm}_{2n-4}(q)$ when $G \cong \mathrm{PSL}_n(q)$, $\mathrm{PSp}_{2n}(q)$, $\Omega_{2n+1}(q)$ or $\mathrm{P}\Omega^{\pm}_{2n}(q)$, respectively. Now, by Lemma 7.4 we construct K and L and check whether K is a long root $\mathrm{SL}_2(q)$-subgroup in G by [47, Theorem 1.2].

If i is not a classical involution, then either C is isomorphic to a commuting product of quasisimple classical groups K and L with $K, L \ncong \mathrm{SL}_2(q)$ or C has only one component. Hence the algorithm presented in Lemma 7.4 never returns a subgroup H which is isomorphic to $\mathrm{SL}_2(q)$. We check whether $H \ncong (\mathrm{P})\mathrm{SL}_2(q)$ in the following way. If $H \ncong (\mathrm{P})\mathrm{SL}_2(q)$, then there are sufficiently elements $h \in H$ such that $h^{q(q^2-1)} \neq 1$. Note that C may have only one component isomorphic to $\mathrm{PSL}_2(q^k)$ for some $k \geqslant 1$, for example, if $G \cong \mathrm{PSL}_4(q)$ ($q \equiv -1 \bmod 4$) or $\mathrm{PSp}_4(q)$, then there exists an involution $i \in G$ such that $C = C_G(i)'' \cong \mathrm{PSL}_2(q^2)$ or $\mathrm{PSL}_2(q)$, respectively. Clearly, in such cases C does not have central involutions. □

8 Construction of Curtis-Phan-Tits system

The aim of this section is to prove Theorem 1.1. We present the following algorithm.

Algorithm: `CPT_Classical`
Input:
• A black box group G known to be isomorphic to a quasisimple classical group over a field of odd size $q \geqslant 5$.
• An exponent E for G.
• The characteristic p of the underlying field.
Output:
• Generators for all root $\mathrm{SL}_2(q)$-subgroups which forms a extended Curtis-Phan-Tits system for G corresponding to some maximal torus.

The proof of Theorem 1.1 follows from the following three routines.

Step 1. Construction of a long root $\mathrm{SL}_2(q)$-subgroup in G; [47, Theorem 1.1].

Step 2. Identification of the type of G; Theorem 7.2.

Step 3. Construction of all root $\mathrm{SL}_2(q)$-subgroups associated with the nodes of the extended Dynkin diagram of the corresponding algebraic group; Sections 8.1, 8.2 and 8.3.

Remark 8.1 1. Except for the groups $\mathrm{PSp}_{2n}(q)$, the structure of the algorithm is, generically, based on constructing a long root $\mathrm{SL}_2(q)$-subgroup which together with a given long root $\mathrm{SL}_2(q)$-subgroup generate a subgroup isomorphic to $\mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$. This approach fails for the groups $\mathrm{PSp}_{2n}(q)$ since the nodes of the extended Dynkin diagram correspond to short root $\mathrm{SL}_2(q)$-subgroups except for the end nodes, see Figure 5. For this reason, we follow a different but simpler approach for the groups $\mathrm{PSp}_{2n}(q)$.

2. By the above remark, we need to know the type of the given black box classical group in order to start constructing the root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes of the extended Dynkin diagram. One can use a probabilistic recognition algorithm presented in [5], which uses order oracle, at the beginning of our algorithm but this algorithm does not distinguish the groups $\Omega_{2n+1}(q)$ and $\mathrm{PSp}_{2n}(q)$ in which case one has to use the algorithm presented in [1]. To make the arguments in our algorithm uniform, we use the algorithm presented in Theorem 7.2.

3. Note that we find the size of the underlying field q at the end of the Step 1 by applying the algorithm presented in [46, Section 5.1.3]. Note that q is the size of the centre of a long root $\mathrm{SL}_2(q)$-subgroup in G, .

8.1 Groups of type A_{n-1}

In this subsection, we present an algorithm which constructs all long root $\mathrm{SL}_2(q)$-subgroups in a black box group G isomorphic to $A^{\varepsilon}_{n-1}(q) = \mathrm{PSL}^{\varepsilon}_n(q)$,

$n \geqslant 3$, $q \geqslant 5$ corresponding to the nodes in the extended Dynkin diagram of $\mathrm{PSL}_n^{\varepsilon}(q)$. We present the algorithm for $\mathrm{PSL}_n(q)$ and the algorithm for $\mathrm{PSU}_n(q)$ can be read along the same steps by changing the notation SL to SU. The algorithm returns an extended Curtis-Tits system for the groups $\mathrm{PSL}_n(q)$ and a Phan system for PSU_n.

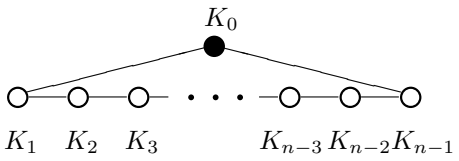

Figure 1: Extended Dynkin diagram of A_n

Algorithm: `CPT_PSLn`
1. Construct a long root $\mathrm{SL}_2(q)$-subgroup K_1 and $C_G(i_1)'' = K_1L_1$ where $i_1 \in Z(K_1)$ and $L_1 \cong \mathrm{SL}_{n-2}(q)$.
2. Construct a classical involution $i_2 \in C_G(i_1)$ where $i_2 \notin C_G(K_1)$. Construct also $C_G(i_2)'' = K_2L$ and K_2. Set $L_2 = C_{L_1}(i_2) \cong \mathrm{SL}_{n-3}(q)$.
3. For $s = 3, \ldots, n-1$, construct classical involutions $i_s \in C_{L_{s-2}}(i_{s-1})$ where $i_s \notin C_G(K_{s-1})$, $C_{L_{s-2}}(i_s)'' = K_sL_s$, K_s and L_s. Note that $L_{n-2} = 1$.
4. Construct $i_0 = i_1i_2 \cdots i_n$, $C_G(i_0)'' = K_0L_0$ and K_0.

Step 1. Construction of K_1

We use [47, Theorem 1.1] to construct a long root $\mathrm{SL}_2(q)$-subgroup $K_1 \leqslant G$. Let i_1 be the unique involution in K_1 and $C_1 = C_G(i_1)'' = K_1L_1$ where $L_1 \cong \mathrm{SL}_{n-2}(q)$. By Lemma 7.4, we can construct L_1.

Step 2: Construction of K_2

By Lemma 6.6, we can find an element $g \in G$ such that $i_2 = \zeta_0^{i_1}(g) \notin C_G(K_1)$ is a classical involution with probability at least $1/750$. Recall that, by the definition of the map $\zeta_0^{i_1}$, the involution $i_2 \in C_G(i_1)$. If $G \ncong \mathrm{PSL}_4(q)$, then i_2 is a classical involution by Lemma 6.3. If $G \cong \mathrm{PSL}_4(q)$, then we check whether i_2 is a classical involution or not by Lemma 7.6. Now, assume that i_2 is a classical involution and construct $C_2 = C_G(i_2)'' = K_2L$ where $K_2 \cong \mathrm{SL}_2(q)$ and $L \cong \mathrm{SL}_{n-2}(q)$. By Lemma 7.4, we can construct K_2, and it follows from Lemma 6.5 that $\langle K_1, K_2 \rangle \cong \mathrm{SL}_3(q)$.

Since $i_2 \in C_G(i_1)$, we have $i_2 \in N_G(L_1)$ by Theorem 2.1. Moreover, i_2 acts as an involution of type t_1 on L_1 since it is a classical involution in G and $i_2 \notin L_1$. Since i_2 acts as an involution of type t_1 on L_1 and $i_2 \in N_G(L_1)$, we have $L_2 = C_{L_1}(i_2)'' \cong \mathrm{SL}_{n-3}(q)$.

Observe that i_1 acts an involution of type t_1 on K_2. Therefore, if $C_{K_2}(i_1)'' = 1$, then $G \cong \mathrm{PSL}_3(q)$. In this case, we start constructing the subgroup corresponding to the extra node in the extended Dynkin diagram. It is clear that

the involution $i_0 = i_1 i_2$ is a classical involution in G satisfying $i_0 \in C_G(i_s)$ and $i_0 \notin C_G(K_s)$ for $s = 1, 2$. Let $K_0 = C_G(i_0)''$ be the corresponding long root $\mathrm{SL}_2(q)$-subgroup. Then $\langle K_1, K_2\rangle = \langle K_2, K_0\rangle = \langle K_0, K_1\rangle \cong \mathrm{PSL}_3(q)$ by Lemma 6.5. Hence, the subgroups K_0, K_1 and K_2 correspond to the nodes in the extended Dynkin diagram.

Step 3: Construction of $K_3, K_4, \ldots, K_{n-1}$

Assume that $n \geqslant 4$. We first check whether $L_2 = C_{L_1}(i_2)'' = 1$. By the above construction, if $L_2 = 1$, then $G \cong \mathrm{PSL}_4(q)$. In this case, $L_1 \cong L \cong \mathrm{SL}_2(q)$ where L is the subgroup constructed in Step 2. We have $\langle K_1, K_2\rangle \cong \langle K_2, L_1\rangle \cong \langle L_1, L\rangle \cong \mathrm{SL}_3(q)$ by Lemma 6.5, and $[K_1, L_1] = [K_2, L] = 1$. Therefore, setting $K_3 = L_1$ and $K_4 = L$, the subgroups K_1, K_2, K_3 and K_4 form a extended Curtis-Tits system for G.

Assume now that $n \geqslant 5$ and start working in $L_1 \cong \mathrm{SL}_{n-2}(q)$. Since $i_2 \in N_G(L_1)$, we have $i_2 i_2^g \in L_1$ for any $g \in L_1$. Moreover, $i_2 i_2^g$ has even order with probability at least $1/8$ by Lemma 6.7. Hence we can construct an involution $i_3 = \zeta_0^{i_2}(g) \in L_1$ for some $g \in L_1$ with probability at least $1/8$. By Lemma 6.7, i_3 is a classical involution in L_1 so, by Lemma 6.3, $i_3 \notin C_G(K_2)$. Now we construct $C_{L_1}(i_3)'' = K_3 L_3$ where $K_3 \cong \mathrm{SL}_2(q)$ and $L_3 \cong \mathrm{SL}_{n-4}(q)$. It is clear that $L_3 \leqslant L_2$. By Lemma 7.4, we can construct K_3 and L_3, and by Lemma 6.5, $\langle K_2, K_3\rangle \cong \mathrm{SL}_3(q)$. We have

- $[i_s, i_t] = 1$ for $s, t = 1, 2, 3$.
- $[K_1, K_3] = 1$.
- $\langle K_1, K_2\rangle \cong \langle K_2, K_3\rangle \cong \mathrm{SL}_3(q)$.

Similarly, we construct a classical involution $i_4 = \zeta_0^{i_3}(g) \in L_2$ for some $g \in L_2$ and continue in this way. Notice that $L_{n-3} \cong \mathrm{SL}_2(q)$ and $L_{n-2} = 1$. Hence, the last recursion step occurs for a classical involution $i_{n-1} \in C_{L_{n-3}}(i_{n-2})$. Indeed, following the above construction, we have $C_{L_{n-3}}(i_{n-1})'' = K_{n-1} \cong \mathrm{SL}_2(q)$ so $K_{n-1} = L_{n-3}$. Hence, we obtain

- $[i_s, i_t] = 1$ for $s, t = 1, \ldots, n-1$.
- $[K_s, K_t] = 1$ for all $s, t = 1, \ldots n-1$ with $|s - t| \geqslant 2$.
- $\langle K_s, K_{s+1}\rangle \cong \mathrm{SL}_3(q)$ for $s = 1, \ldots, n-2$.

Step 5: Construction of K_0

Let $i_0 = i_1 i_2 \cdots i_{n-1}$. It is clear that i_0 is a classical involution and it does not centralise K_1 and K_{n-1}. Moreover, $i_0 \in N_G(K_1) \cap N_G(K_{n-1})$. Let K_0 be the long root $\mathrm{SL}_2(q)$-subgroup containing i_0. Then, by construction, $[K_0, K_s] = 1$ for $s = 2, 3, \ldots, n-2$ and $\langle K_0, K_1\rangle \cong \langle K_0, K_{n-1}\rangle \cong \mathrm{SL}_3(q)$ by Lemma 6.5. Hence the subgroups $K_0, K_1, \ldots, K_{n-1}$ form an extended Curtis-Tits system for G.

8.2 Groups of type B_n and D_n

In this section we present our algorithm for $B_n(q) = \Omega_{2n+1}(q)$ where $n \geqslant 3$ and $D_n^{\varepsilon}(q) = \mathrm{P}\Omega_{2n}^{\pm}(q)$ where $n \geqslant 4$ and $q \geqslant 5$. Recall that $\Omega_5(q) \cong \mathrm{PSp}_4(q)$, $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$ and $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$. We present our algorithm for $B_n(q)$ and $D_n(q)$ separately.

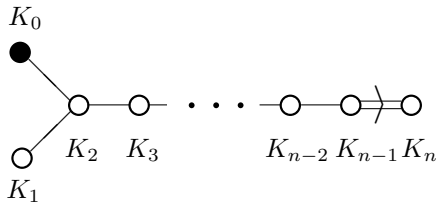

Figure 2: Extended Dynkin diagram of B_n

Algorithm: `CPT_Bn`

1. Construct long root $\mathrm{SL}_2(q)$-subgroup K_1 and $C_G(i_1)'' = K_0K_1L_1$ where $i_1 \in Z(K_1)$. Construct also K_0 and $L_1 \cong \Omega_{2n-3}(q)$.
2. Construct a classical involution $i_2 \in C_G(i_1)$ where $i_2 \in N_G(K_1)\backslash C_G(K_1)$. Construct also $C_G(i_2)'' = K_2\tilde{K}_2L$ and K_2. Set $L_2 = C_{L_1}(i_2)'' \cong \Omega_{2n-5}(q)$.
3. For $s = 3, \ldots, n-1$, construct classical involutions $i_s \in C_{L_{s-2}}(i_{s-1})$ where $i_s \in N_G(K_{s-1})\backslash C_G(K_{s-1})$, $C_{L_{s-2}}(i_s)'' = K_s\tilde{K}_sL_s$, K_s and $L_s \cong \Omega_{2(n-s)-1}(q)$. Note that $L_{n-2} \cong \Omega_3(q) \cong \mathrm{PSL}_2(q)$ and $L_{n-1} = 1$.
4. Set $K_n = L_{n-2}$.

Step 1. We use [47, Theorem 1.1] to construct a long root $\mathrm{SL}_2(q)$-subgroup K_1 in G. Let i_1 be the unique involution in K_1. Then $C_G(i_1)'' = K_0K_1L_1$ where $K_1 \cong K_0 \cong \mathrm{SL}_2(q)$ and $L_1 \cong \Omega_{2n-3}(q)$.

By Lemma 6.13, we can find an element $g \in C_G(i_1)$ such that $\langle K_1, K_1^g\rangle \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$ with probability at least $1/8$. It is clear that the components are K_0 and K_1. By Lemma 7.5, we can construct K_0.

If $n = 3$, then $L_1 \cong \Omega_3(q) \cong \mathrm{PSL}_2(q)$ so $C_G(i_1)''$ is a commuting product of the subgroups K_0, K_1 and L_1 and we apply Lemma 7.5 to construct L_1. If $n \geqslant 4$, we apply Lemma 7.4 to construct L_1.

Step 2. We construct an involution $i_2 \in G$ by using the map $\zeta_0^{i_1}$ with the property that $i_2 \in N_G(K_1)\backslash C_G(K_1)$. By Lemma 6.8, i_2 is an involution of type t_1, t_2 (classical) or t_3. By Lemma 7.6, we can decide if i_2 is a classical involution. By Lemma 6.12, we can find an element $g \in G$ such that $i_2 = \zeta_0^{i_1}(g)$ is a classical involution and $i_2 \in N_G(K_1)\backslash C_G(K_1)$ with probability bounded from below by constant. Now $C_G(i_2)'' = K_2\tilde{K}_2L$ where $K_2 \cong \tilde{K}_2 \cong \mathrm{SL}_2(q)$ and $L \cong \Omega_{2n-3}(q)$. Observe that i_2 acts as an involution of type t_1 on both K_1 and L_1. Thus $L_2 = C_{L_1}(i_2)'' \cong \Omega_{2n-5}(q)$.

By Lemma 6.10, $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$. If $L_2 = 1$, then $n = 3$ and $L_1 \cong \Omega_3(q)$. In this case, the subgroup $\langle K_2, L_1\rangle$ acts irreducibly on a non-degenerate 5-dimensional orthogonal space. Hence $\langle K_2, L_1\rangle \cong \Omega_5(q) \cong \mathrm{PSp}_4(q)$. Thus, setting $K_3 = L_1$, the subgroups K_0, K_1, K_2, K_3 form an extended Curtis-Tits or Phan system depending on $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$, respectively.

Step 3. Assume now that $n \geqslant 4$. Recall that $L_1 \cong \Omega_{2n-3}(q)$. We first construct a classical involution $i_3 \in L_1$ such that $i_3 \in N_G(K_2)\backslash C_G(K_2)$. Since $i_2 \in N_G(L_1)$ and it acts as an involution of type t_1 on L_1, an element of the form $i_2 i_2^g$ has even order for a random element $g \in L_1$ with probability at least $1/960$ by Lemma 6.14. Hence, we can construct a classical involution $i_3 = \zeta_0^{i_2}(g)$ for some $g \in L_1$ with probability at least $1/960$. Since $i_3 \in C_G(i_2)$, by Lemma 6.12, $i_3 \in N_G(K_2)\backslash C_G(K_2)$ with probability bounded from below by constant. Note that $i_3 \in L_1$ since $i_2 \in N_G(L_1)$ and $g \in L_1$. Now $C_{L_1}(i_3)'' = K_3\tilde{K}_3 L_3$ where $K_3 \cong \tilde{K}_3 \cong \mathrm{SL}_2(q)$ and $L_3 \cong \Omega_{2n-7}(q)$. We construct K_3 and L_3 by using Lemma 7.4. Since $\langle K_1, K_2\rangle \cong \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$, we have $\langle K_2, K_3\rangle \cong \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ by Lemma 6.11, respectively. Hence, we start building either the Curtis-Tits system or the Phan system for G.

Similarly, we construct classical involutions $i_s \in C_{L_{s-2}}(i_{s-1})$ where $i_s \in N_G(K_{s-1})\backslash C_G(K_{s-1})$. We have $C_{L_{s-2}}(i_s)'' = K_s\tilde{K}_s L_s$ for $s = 4, \ldots, n-1$ where $K_s \cong \tilde{K}_s \cong \mathrm{SL}_2(q)$ and $L_s \cong \Omega_{2(n-s)-1}(q)$. Notice that $C_{L_{n-1}}(i_{n-1}) = K_{n-1}\tilde{K}_{n-1}$, that is, $L_{n-1} = 1$ and $L_{n-2} \cong \Omega_3(q)$. Hence, we have

- $K_0, K_1, \ldots, K_{n-1}$ where $K_s \cong \mathrm{SL}_2(q)$ for $s = 0, 1, 2, \ldots, n-1$.
- $\langle K_0, K_2\rangle$ and $\langle K_s, K_t\rangle$ are all isomorphic to $\mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ for $|s-t| = 1$, $s, t \geqslant 1$.
- $[K_s, K_t] = 1$ for $|s-t| \geqslant 2$, $(s,t) \neq (0,2)$ or $(2,0)$.
- $\langle K_0, K_1\rangle \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$.

Step 5. We set $K_n = L_{n-2}$. It is clear that the subgroup $\langle K_{n-1}, K_n\rangle$ acts irreducibly on 5-dimensional non-degenerate orthogonal space, hence $\langle K_{n-1}, K_n\rangle \cong \Omega_5(q) \cong \mathrm{PSp}_4(q)$. Thus the subgroups $K_0, K_1, \ldots, K_n$ form an extended Curtis-Phan-Tits system for G.

Now we present a Curtis-Phan-Tits system for the groups $\mathrm{P}\Omega_{2n}^+(q)$ where $n \geqslant 4$, $q \geqslant 5$. Recall that $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$ and $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$.

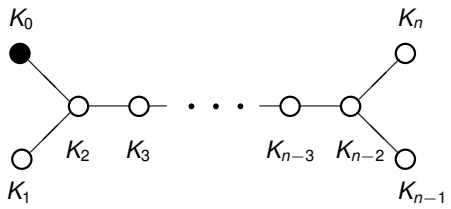

Figure 3: Extended Dynkin diagram of D_n

Algorithm: `CPT_Dn+`

---

1. Construct long root $\mathrm{SL}_2(q)$-subgroups K_0 and K_1, and $C_G(i_1)'' = K_0K_1L_1$ where $i_1 \in Z(K_1)$ and $L_1 \cong \Omega^+_{2n-4}(q)$.
2. Construct a classical involution $i_2 \in C_G(i_1)$ where $i_2 \in N_G(K_1)\backslash C_G(K_1)$. Construct also $C_G(i_2)'' = K_2\tilde{K}_2L$ and K_2. Set $L_2 = C_{L_1}(i_2)'' \cong \Omega^{\pm}_{2n-6}(q)$.
3. For $s = 3, \ldots, n-2$, construct classical involutions $i_s \in C_{L_{s-2}}(i_{s-1})$ where $i_s \in N_G(K_{s-1})\backslash C_G(K_{s-1})$, $C_{L_{s-2}}(i_s)'' = K_s\tilde{K}_sL_s$, K_s and $L_s \cong \Omega_{2(n-s)-2}(q)$. Note that $L_{n-3} \cong \Omega^{\pm}_4(q))$ and $L_{n-2} = 1$.
4. If $L_{n-3} \cong \Omega^+_4(q)$, then construct the components K_{n-1} and K_n. If $L_{n-3} = \Omega^-_4(q)$, then we set $K_{n-1} = L_{n-3} \cong \mathrm{PSL}_2(q^2)$.

Step 1,2,3. Same as in the groups of type B_n.
Step 4. We have

- $K_0, K_1, \ldots, K_{n-2}$ where $K_s \cong \mathrm{SL}_2(q)$ for $s = 0, 1, 2, \ldots, n-2$.
- $\langle K_s, K_t\rangle$ and $\langle K_0, K_2\rangle$ are all isomorphic to $\mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ for $|s-t| = 1$, $s, t \geqslant 1$.
- $[K_s, K_t] = 1$ for $|s-t| \geqslant 2$, $(s,t) \neq (0,2)$ or $(2,0)$.
- $\langle K_0, K_1\rangle \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$

Observe that if $\langle K_s, K_t\rangle$ are all isomorphic to $\mathrm{SL}_3(q)$ for $s, t \geqslant 1$ with $|s-t| = 1$, then $L_{n-3} = K_{n-1} \circ_2 K_n \cong \Omega^+_4(q)$ where $K_{n-1} \cong K_n \cong \mathrm{SL}_2(q)$. Moreover $i_{n-1} = i_n$ where i_{n-1} and i_n are the unique involutions in K_{n-1} and K_n, respectively. By the construction, it is clear that the involution i_n commute with i_{n-2}. Hence, by Lemma 6.11, $\langle K_{n-2}, K_{n-1}\rangle \cong \langle K_{n-2}, K_n\rangle \cong \mathrm{SL}_3(q)$. Thus we obtain an extended Curtis-Tits system for G.

If $\langle K_s, K_t\rangle$ are all isomorphic to $\mathrm{SU}_3(q)$ for $s, t \geqslant 1$ with $|s-t| = 1$, then $L_1 \cong \Omega^+_{2n-4}(q)$, $L_2 \cong \Omega^-_{2n-6}(q)$ and so on. In general, $L_s \cong \Omega^{\varepsilon_s}_{2(n-s)-2}(q)$ where $\varepsilon_s = (-1)^{s+1}$. Therefore, if n is even, then $L_{n-3} = K_{n-1} \circ_2 K_n \cong \Omega^+_4(q)$ and we apply the arguments in the previous paragraph to obtain an extended Phan system for G. If n is odd, then $L_{n-3} = \langle K_{n-1}, K_n\rangle \cong \Omega^-_4(q) \cong \mathrm{PSL}_2(q^2)$. In this case, we set $K_{n-1} = L_{n-3}$. Note that this is not an extended Phan system for G according to Definition 4.4.

The algorithm for the groups $\mathrm{P}\Omega^-_{2n}(q)$ is the same as above except for Step 4. Let $G \cong \mathrm{P}\Omega^-_{2n}(q)$. Applying Step 1, 2 and 3 of the algorithm for the groups B_n, we have

- $K_0, K_1, \ldots, K_{n-2}$ where $K_s \cong \mathrm{SL}_2(q)$ for $s = 0, 1, 2, \ldots, n-2$.
- $\langle K_0, K_2\rangle$ and $\langle K_s, K_t\rangle$ are all isomorphic to $\mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ for $|s-t| = 1$, $s, t \geqslant 1$.
- $[K_s, K_t] = 1$ for $|s-t| \geqslant 2$, $(s,t) \neq (0,2)$ or $(2,0)$.
- $\langle K_0, K_1\rangle \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$

If $\langle K_s, K_t\rangle$ are all isomorphic to $\mathrm{SL}_3(q)$ for $s, t \geqslant 1$ with $|s-t| = 1$, then $L_s \cong \Omega^-_{2(n-s)-2}(q)$ for $s = 1, 2, \ldots, n-2$. In particular, $L_{n-3} = \langle K_{n-1}, K_n\rangle \cong \Omega^-_4(q) \cong \mathrm{PSL}_2(q^2)$. In this case, we set $K_{n-1} = L_{n-3}$. Hence we obtain an extended Curtis-Tits system for G.

If $\langle K_s, K_t\rangle$ are all isomorphic to $\mathrm{SU}_3(q)$ for $s, t \geqslant 1$ with $|s-t| = 1$, then $L_1 \cong \Omega^-_{2n-4}(q)$, $L_2 \cong \Omega^+_{2n-6}(q)$ and so on. In general $L_s \cong \Omega^{\varepsilon_s}_{2(n-s)-2}(q)$ where $\varepsilon_s = (-1)^s$. Therefore, if n is even, then $L_{n-3} = \langle K_{n-1}, K_n\rangle \cong \Omega^-_4(q)$. In this case, we set $K_{n-1} = L_{n-3}$. Note that this is neither Curtis-Tits nor Phan sytem for G, see Definition 4.4. If n is odd, then $L_{n-3} = K_{n-1} \circ_2 K_n \cong \Omega^+_4(q)$ where $K_{n-1} \cong K_n \cong \mathrm{SL}_2(q)$. Moreover $i_{n-1} = i_n$ where i_{n-1} and i_n are the unique involutions in K_{n-1} and K_n, respectively. By the construction, it is clear that $i_{n-1} = i_n$ commute with i_{n-2}. Hence, by Lemma 6.11, $\langle K_{n-2}, K_{n-1}\rangle \cong \langle K_{n-2}, K_n\rangle \cong \mathrm{SU}_3(q)$. Thus we obtain an extended Phan system for G.

8.3 Groups of type C_n

In this section we present our algorithm for symplectic groups $C_n(q) = \mathrm{PSp}_{2n}(q)$ where $n \geqslant 2$, $q \geqslant 5$.

8.3.1 A small case: $\mathrm{PSp}_4(q)$

The algorithm for $G \cong \mathrm{PSp}_4(q)$ is different from the general case at one stage. Therefore, we first construct a Curtis-Phan-Tits system for $G \cong \mathrm{PSp}_4(q)$. Note that it is straightforward to distinguish $\mathrm{PSp}_4(q)$ from $\mathrm{PSp}_{2n}(q)$ for $n \geqslant 3$.

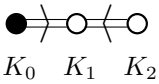

Figure 4: Extended Dynkin diagram of C_2

Algorithm: `CPT_C2`
1. Produce an involution t of type t_2 and construct $C = C_G(t)$ and $C'' \cong \mathrm{PSL}_2(q)$.
2. Construct a classical involution $i \in G$ where $[i,t] = 1$.
3. Construct the components of $C_G(i)'' \cong \mathrm{SL}_2(q) \circ_2 \mathrm{SL}_2(q)$.

Step 1: By Lemma 6.15 and 6.16, we can construct an involution of type t_2 with probability at least $1/10$. In G, there are two conjugacy classes of involutions: involutions of type t_1 (classical) and of type t_2. Therefore, we can decide whether an involution $t \in G$ is of type t_2 or not by Lemma 7.6. Let t be an involution of type t_2 and set $K_1 = C_G(t)'' \cong \mathrm{PSL}_2(q)$.
Step 2: We need to construct a classical involution $i \in G$ which commutes with t. To do this, we use ζ_0^t, and, by Lemma 6.18, we can construct such an involution with probability at least $1/768$. Note that we can check whether i is classical or not by Lemma 7.6. Note also that $[i,t] = 1$ by the definition of ζ_0^t.
Step 3: By Lemma 7.4, we construct the components of $C_G(i)'' = K_0 \circ_2 K_2$ where $K_0 \cong K_2 \cong \mathrm{SL}_2(q)$. Note that the subgroup K_1 stabilises a maximal totally isotropic subspace so $N_G(K_1)$ is a maximal subgroup of G [3] and $|N_G(K_1)/K_1| = 2(q \pm 1)$. Clearly $K_0 \not\leqslant N_G(K_1)$ and $K_2 \not\leqslant N_G(K_1)$. Hence $\langle K_1, K_0 \rangle = \langle K_1, K_2 \rangle = G$.

8.3.2 General case: $\mathrm{PSp}_{2n}(q)$, $n \geqslant 3$

We can now present the algorithm for the general case.

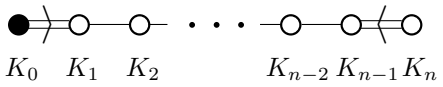

Figure 5: Extended Dynkin diagram of C_n

Algorithm: `CPT_Cn`
1. Construct an element $g \in G$ which has a maximal primitive divisor rank.
2. Construct the involution $i = \mathrm{i}(g)$.
3. Check whether i is an involution of type t_n. If not, repeat Steps 1 and 2.
4. Construct $C = C_G(i)'' \cong \frac{1}{(2,n)}\mathrm{SL}_n^{\varepsilon}(q)$.
5. Construct Curtis-Phan-Tits system for C, that is, $K_1, K_2, \ldots, K_{n-1}$.
6. Construct K_n and K_0.

Step 1. Let T be a maximally twisted torus of order $(q^n \pm 1)/2$. Then $|N_G(T)/T| = 2n$ by [1, Lemma 2.3]. Therefore, we can find an element $g \in G$ such that $\mathrm{pdrank}(g) = n$ or $2n$ in $O(n)$ random selections from G.
Step 2. It is easy to see that involutions which belong to a torus of order $(q^n + 1)/2$ are of type t_n, see [1, Lemma 2.13].

If $q^n \equiv -1 \bmod 4$, then we use elements of maximal primitive divisor rank $2n$ to construct involution of type t_n. Note that the elements $g \in G$ with $\mathrm{pdrank}(g) = 2n$ belong to tori of order $(q^n+1)/2$, which is even.

If $q^n \equiv 1 \bmod 4$, then $(q^n+1)/2$ is odd. Therefore the elements of maximal primitive divisor rank $2n$ have odd order since they belong to some torus of order $(q^n+1)/2$. In this case, we construct an element $g \in G$ of pdrank n, which has even order, and the involution $i = \mathrm{i}(g)$. By [1, Section 4.3], if n is odd, then i is an involution of type t_n. It might happen to be a different type, if n is even.

Step 3. We check whether i is of type t_n in the following way. If i is an involution of type t_n, then, for $20n$ random elements $g \in G$, one of the elements ii^g has pdrank $2n$ with probability at least $1 - 1/e$, see Section 3.4 in the corrected version of [1]. If i is not an involution of type t_n, then the $\mathrm{pdrank}(ii^g) < 2n$ for any $g \in G$.

Note that if $q^n \equiv -1 \bmod 4$ or n is odd, then i is of type t_n by the arguments in Step 2.

Step 4. For an involution i of type t_n, if $q \equiv 1 \bmod 4$, then $C_G(i)'' \cong \frac{1}{2}\mathrm{SL}_n(q)$, whereas, if $q \equiv -1 \bmod 4$, then $C_G(i)'' \cong \frac{1}{2}\mathrm{SU}_n(q)$.

Step 5. In either case $q \equiv \pm 1 \bmod 4$, we run the algorithm in Subsection 8.1 to construct the subgroups $K_1, K_2, \ldots, K_{n-1}$. By the description of the centralisers of involutions, see for example [21, Definition 4.1.8(A) and Table 4.5.1], $C_G(i)''$ is generated by the all fundamental short root $\mathrm{SL}_2(q)$-subgroups corresponding to a fixed fundamental root system. Hence, we construct all the short root $\mathrm{SL}_2(q)$-subgroups corresponding to the nodes in the Dynkin diagram of G, see Figure 5.

Step 6. Let i_{n-1} be the unique involution in K_{n-1}. Observe that $C = C_G(i_{n-1})'' \cong L_1 \times L_2$ where $L_1 \cong \mathrm{Sp}_4(q)$ and $L_2 \cong \mathrm{Sp}_{2n-4}(q)$. Moreover, $i_{n-1} \in Z(L_1)$ and $K_{n-1} \leqslant L_1$. Now, we construct a long root $\mathrm{SL}_2(q)$-subgroup K_n in L_1 by using [47, Theorem 1.1]. By the arguments in Step 3 in Subsection 8.3.1, we have $\langle K_{n-1}, K_n \rangle = L_1 \cong \mathrm{Sp}_4(q)$. To construct K_0, we use K_1 instead of K_{n-1} and apply the same method.

Acknowledgements

The second author is supported in part by TÜBİTAK, MATHLOGAPS project 504029 and Australian Research Council Federation Fellowship grant FF0776186

References

[1] C. Altseimer and A. V. Borovik, *Probabilistic recognition of orthogonal and symplectic groups*, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 1–20; Corrections: math.GR/0110234.

[2] M. Aschbacher, *A characterization of Chevalley groups over fields of odd order. I, II*, Ann. of Math. (2) **106** (1977), no. 3, 353–468.

[3] ———, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), no. 3, 469–514.

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

[5] L. Babai, W. M. Kantor, P. P. Pálfy, and Á. Seress, *Black-box recognition of finite simple groups of Lie type by statistics of element orders*, J. Group Theory **5** (2002), no. 4, 383–401.

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

[7] C. Bennett, R. Gramlich, C. Hoffman, and S. Shpectorov, *Odd-dimensional orthogonal groups as amalgams of unitary groups. I. General simple connectedness*, J. Algebra **312** (2007), no. 1, 426–444.

[8] C. D. Bennett, R. Gramlich, C. Hoffman, and S. Shpectorov, *Curtis-Phan-Tits theory*, Groups, combinatorics & geometry (Durham, 2001), World Sci. Publ., River Edge, NJ, 2003, pp. 13–29.

[9] C. D. Bennett and S. Shpectorov, *A new proof of a theorem of Phan*, J. Group Theory **7** (2004), no. 3, 287–310.

[10] 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.

[11] A.V. Borovik and Ş. Yalçınkaya, *Construction of Curtis-Phan-Tits system for black box exceptional groups of Lie type odd characteristic*, in preparation.

[12] ———, *The Curtis-Tits theorem and its generalizations*, in preparation.

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

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

[15] P. A. Brooksbank and W. M. Kantor, *On constructive recognition of a black box* $\mathrm{PSL}(d, q)$, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 95–111.

[16] ———, *Fast constructive recognition of black box orthogonal groups*, J. Algebra **300** (2006), no. 1, 256–288.

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

[18] R. W. Carter, *Simple groups of Lie type*, John Wiley & Sons, London-New York-Sydney, 1972, Pure and Applied Mathematics, Vol. 28.

[19] 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.

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

[21] 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.

[22] R. Gramlich, *Weak Phan systems of type C_n*, J. Algebra **280** (2004), no. 1, 1–19.

[23] R. Gramlich, C. Hoffman, W. Nickel, and S. Shpectorov, *Even-dimensional orthogonal groups as amalgams of unitary groups*, J. Algebra **284** (2005), no. 1, 141–173.

[24] R. Gramlich, C. Hoffman, and S. Shpectorov, *A Phan-type theorem for* $\mathrm{Sp}(2n, q)$, J. Algebra **264** (2003), no. 2, 358–384.

[25] Ralf Gramlich, Max Horn, and Werner Nickel, *The complete Phan-type theorem for* $\mathrm{Sp}(2n, q)$, J. Group Theory **9** (2006), no. 5, 603–626.

[26] R. M. Guralnick and F. Lübeck, *On p-singular elements in Chevalley groups in characteristic p*, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 169–182.

[27] 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.

[28] W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), no. 1, 67–87.

[29] W. M. Kantor and Á. Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708, viii+168.

[30] ———, *Prime power graphs for groups of Lie type*, J. Algebra **247** (2002), no. 2, 370–434.

[31] ———, *Large element orders and the characteristic of Lie-type simple groups*, J. Algebra **322** (2009), no. 3, 802–832.

[32] Martin W. Liebeck and E. A. O'Brien, *Finding the characteristic of a group of Lie type*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 741–754.

[33] Frank Lübeck, Alice C. Niemeyer, and Cheryl E. Praeger, *Finding involutions in finite Lie type groups of odd characteristic*, J. Algebra **321** (2009), no. 11, 3397–3417.

[34] A. C. Niemeyer and C. E. Praeger, *A recognition algorithm for classical groups over finite fields*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 117–169.

[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] Igor Pak, *What do we know about the product replacement algorithm?*, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 301–347.

[37] C. Parker and R. Wilson, *Recognising simplicity of black box groups*, 2005, preprint.

[38] K. W. Phan, *On groups generated by three-dimensional special unitary groups. I, II*, J. Austral. Math. Soc. Ser. A **23** (1977), no. 1, 67–77, 129–146.

[39] C. Praeger and Á Seress, *Probabilistic generation of finite classical groups in odd characteristic by involutions*, 2009, preprint.

[40] ———, *Balanced involutions in centralisers of balanced involutions for finite classical groups*, In preparation.

[41] G. M. Seitz, *The root subgroups for maximal tori in finite groups of Lie type*, Pacific J. Math. **106** (1983), no. 1, 153–244.

[42] Á. Seress, *Permutation group algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003.

[43] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968, Notes prepared by John Faulkner and Robert Wilson.

[44] F. G. Timmesfeld, *The Curtis-Tits-presentation*, Adv. Math. **189** (2004), no. 1, 38–67.

[45] J. Tits, *Groupes semi-simples isotropes*, Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962), Librairie Universitaire, Louvain, 1962, pp. 137–147.

[46] Ş. Yalçınkaya, *Black box groups*, Suppl. Turkish Journal of Mathematics **31** (2007), 171–210.

[47] ———, *Construction of long root $SL_2(q)$-subgroups in black-box groups*, arXiv:1001.3184, p. 37 pp.