Constructive recognition of classical groups in odd characteristic

C.R. Leedham-Green and E.A. O'Brien

Abstract

Let $G = \langle X \rangle \leq \mathrm{GL}(d, F)$ be a classical group defined over a finite field F of odd characteristic. We present algorithms to construct standard generators for G which permit us to write an element of G as a straight-line program in X. The algorithms run in Las Vegas polynomial-time, subject to the existence of a discrete log oracle for F.

1 Introduction

The goal of the 'matrix recognition project' is the development of efficient algorithms for the investigation of subgroups of $\mathrm{GL}(d, F)$ where F is a finite field. We refer to the recent survey [29] for background related to this work. A particular aim is to identify the composition factors of $G \leq \mathrm{GL}(d, F)$. If a problem can be solved for the composition factors, then it can be frequently be solved for G.

One may intuitively think of a *straight-line program* (SLP) for $g \in G = \langle X \rangle$ as an efficiently stored group word on X that evaluates to g. For a formal definition, we refer the reader to Section 16. A critical property of an SLP is that its length is proportional to the number of multiplications and exponentiations used in constructing the corresponding group element. Babai & Szemerédi [2] prove that every element of G has an SLP in X of length at most $O(\log^2 |G|)$.

Informally, a *constructive recognition algorithm* constructs an explicit isomorphism between a group G and a 'standard' (or natural) copy of G, and exploits this isomorphism to write an arbitrary element of G as an SLP in its defining generators. For a more formal definition, see [33, p. 192].

In the case under consideration G is given in its natural representation, so one might regard the construction of the identity map as an easy exercise. However, G is, from the computational point of view, the group generated by X: so constructing an

This work was supported in part by the Marsden Fund of New Zealand via grant UOA 412. We thank Peter Brooksbank, John Bray, Cheryl Praeger, and Robert Wilson for helpful discussions on its content. 2000 *Mathematics Subject Classification.* Primary 20C20, 20C40.

explicit isomorphism from the classical group to G requires one, in particular, to write a canonical generating set for the classical group as SLPs in X; and that is the problem considered in this paper.

1.1 The groups

We divide the groups of principal interest into three overlapping classes.

The first class consists of the following groups. In all cases q is odd, and V denotes the underlying vector space.

- $\mathrm{GL}(d,q)$, the group of all invertible $d \times d$ matrices of $\mathrm{GF}(q)$.
- $\mathrm{Sp}(d,q)$, the group of all elements of $\mathrm{GL}(d,q)$ that preserve a given non-degenerate alternating bilinear form on V. The existence of such a form implies that d is even.
- $\mathrm{U}(d,q)$, the group of all elements of $\mathrm{GL}(d,q^2)$ that preserve a given non-degenerate hermitian form on V.
- $\mathrm{O}^+(d,q)$, the group of all elements of $\mathrm{GL}(d,q)$ that preserve a given non-degenerate symmetric bilinear form on V of $+$ type. This implies that d is even.
- $\mathrm{O}^-(d,q)$ is defined in the same way, except that the form is of - type; again d is even.
- $\mathrm{O}^0(d,q)$, the group of all elements of $\mathrm{GL}(d,q)$ that preserve a given non-degenerate symmetric bilinear form on V, where d is odd.

The definition of all of these groups, except for the first, depends on the choice of form. However, the groups defined by two different forms of the same stated type are conjugate in $\mathrm{GL}(d,q)$. The resulting ambiguity should not cause problems. We use the notation $\mathrm{GX}(d,q)$ to represent any one of the above groups.

The second class of groups is obtained from the first class by replacing each group by the subgroup consisting of the elements of determinant 1. All elements of $\mathrm{Sp}(d,q)$ have determinant 1. The subgroups of the other groups thus defined are denoted respectively by $\mathrm{SL}(d,q)$, $\mathrm{SU}(d,q)$, $\mathrm{SO}^+(d,q)$, $\mathrm{SO}^-(d,q)$ and $\mathrm{SO}^0(d,q)$. Thus $\mathrm{Sp}(d,q)$ belongs to both classes. We use the notation $\mathrm{SX}(d,q)$ to represent any group in the second class. However, when we discuss only the orthogonal groups, we use the conventational notation $\mathrm{SO}^\epsilon(d,q)$ where $\epsilon \in \{-1,0,1\}$.

All the groups in the second class are perfect with the exception of the orthogonal groups; these containing a unique subgroup of index 2, denoted respectively by $\Omega^+(d,q)$, $\Omega^-(d,q)$ and $\Omega^0(d,q)$; with one exception, $\Omega^+(4,3)$, these groups are perfect for $d > 2$. The third class consists of these three families together with the perfect groups in the second class. We sometimes use the notation $\Omega\mathrm{X}(d,q)$ to represent any group in the third class. Let $\mathcal{C}$ denote the union of the second and third class.

Recall that the spinor norm is a homomorphism from $\mathrm{SO}^\epsilon(d,q)$ to $\{\pm 1\}$ with kernel $\Omega^\epsilon(d,q)$. For details of this map, see for example [35, p. 163].

We may regard any of the above groups as a group of automorphisms of a vector space V of dimension d over $\mathrm{GF}(q)$ (or over $\mathrm{GF}(q^2)$ in the case of unitary groups); and we replace (d,q) by V when we wish to specify the vector space; thus writing, for example, $\mathrm{Sp}(V)$ for $\mathrm{Sp}(d,q)$. In this situation V will be equipped with a non-degenerate form (except in the case of $\mathrm{SL}(V)$ and $\mathrm{GL}(V)$), so we write $\mathrm{O}(V)$ rather than, for example $\mathrm{O}^-(V)$, and similarly for $\mathrm{SO}(V)$ and $\Omega(V)$, allowing the type of the form to determine the type of the group.

1.2 The primary result

We present and analyse two algorithms that take as input a generating subset X of a group in $\mathcal{C}$ and return as output *standard generators* of this group as SLPs in X. Usually, these generators are defined with respect to a basis different to that for which X was defined, and a change-of-basis matrix is also returned to relate these bases.

The second algorithm does not apply directly to orthogonal groups that are not of + type; but when dealing with the other orthogonal groups in large dimensions most of the work is carried out in an orthogonal subgroup of + type, and this subgroup can be processed using the second algorithm.

Classical groups in characteristic 2 can also be addressed in the same style, but the resulting algorithms are more complex. We shall consider these groups in a later paper.

If a non-degenerate form is to be preserved by a group, then the standard generators are defined with respect to a specific form. However, the input is a generating set for the group in question, and no form is specified. Naturally the group defines the form that it preserves *up to a scalar multiple*. Thus the standard generators need to be modified (in a very simple way) if they are to preserve a specified form. [WHAT ARE WE SAYING HERE?]

A non-degenerate form preserved by a classical group may be readily determined by an application of module isomorphism (see [18, Section 7.5.4]). Once a form is known, we can identify that the group is of a particular classical type by applying the 'naming' algorithm of [26].

Let ξ denote the number of field operations to construct an independent (nearly) uniformly distributed random element of a group, and let χ denote the number of field operations for a call to a discrete log oracle for $\mathrm{GF}(q)$.

Our principal result is the following.

Theorem 1.1 *There is a Las Vegas algorithm that takes as input a subset X of bounded cardinality of $\mathrm{GL}(d,q)$, where X generates a group in $\mathcal{C}$, and returns standard generators for $\langle X\rangle$ as* SLPs *in X. Given an oracle to solve the discrete logarithm problem in $\mathrm{GF}(q)$ (and in $\mathrm{GF}(q^2)$ in the case of orthogonal groups of $-$ type) the algorithm requires $O(d(\xi+d^3\log q+\chi))$ field operations, and returns the standard generators as* SLPs *of length $O(\log^3 d)$ in X.*

We prove this theorem by exhibiting an algorithm with the given complexity; more precisely, we exhibit two algorithms for each of the given types of group. For each type, the first algorithm is designed to run fast, and the second to produce shorter straight line programs. The first algorithm spends less time in the parent group; the second spends more time in the parent group, but generates far fewer recursive calls. The bound of $O(\log^3 d)$ for the length of the straight line programs is achieved by the second algorithm. If we assume that a random element can be constructed in $O(d^3)$ field operations, then, for fixed q, and subject to the existence of a discrete log oracle, both algorithms require $O(d^4 \log q)$ field operations to construct the standard generators.

Brooksbank's algorithms [7] for the natural representation of $\mathrm{Sp}(d,q)$, $\mathrm{SU}(d,q)$, and $\Omega^\epsilon(d,q)$ have complexity $O(d^5)$ for fixed q. More precisely, the complexity of his algorithm to construct standard generators for the classical group is

$$O(d^3 \log q(d + \log d \log^3 q) + (d + \log\log q)\xi + d^5 \log^2 q + (\log q)\chi)$$

and again assumes the existence of a discrete log oracle. The algorithm of Celler & Leedham-Green [11] for $\mathrm{SL}(d,q)$ has complexity $O(d^4 q)$.

Once we have constructed these standard generators for G, a generalised echelonisation algorithm can be used to write a given element of G as an SLP in terms of these generators. We do not consider this task here, but refer the interested reader to the algorithm of [7, Section 5], which performs this task in $O(d^3 \log q + \log^2 q)$ field operations.

It has become standard practice to describe the time complexity of algorithms of this type in terms of the number of field operations (or time) required to carry out various basic operations, such as constructing a suitable random element, or multiplying two matrices. This practice is not so appropriate for our algorithms. The reason is that our algorithms rely on recursive calls to cases of approximately half the original dimension, and we need to prove that the time spent in these calls only affects the total time by at most a fixed constant factor. This requires assumptions about the cost of these operations as functions of d. In an algorithm that moves from dimension d to dimension $d-1$ the only assumption required to estimate the complexity (up to a constant factor) is the unwritten assumption that these operations do not become slower as d becomes smaller. If we ignore these issues and write the complexity of our algorithms in the standard style for the sake of comparison, the complexity of our algorithms is $O(d(\xi(d) + d^3 \log q + \chi))$ field operations, where $\xi(d)$ is the number of field operations required to produce a sufficiently independent random element of a classical group in dimension d, and χ is the time required for a call to a discrete logarithm algorithm, divided by the time required by a field operation. This formulation of the complexity simply records the fact that the number of random elements required *outside* the recursive calls is $O(d)$, and the total number of calls to the discrete logarithm oracle is also $O(d)$. We shall use ξ and χ with

the above meanings, writing ξ for $\xi(d)$ where the value of d is clear from the context.

1.3 The content of the paper

A central component of both algorithms is the use of involution centralisers. In Section 2 we review some background material on forms and summarise the structure of involution centralisers for elements of classical groups in odd characteristic. In Section 3 we define standard generators for the classical groups. In Sections 4 to 7 the two algorithms are described: the non-orthogonal groups are first presented uniformly. The algorithms rely on finding involutions whose -1-eigenspaces have dimensions in a prescribed range. The cost of constructing such involutions is analysed in Sections 9 and 10. We frequently compute high powers of elements of linear groups; an algorithm for doing this efficiently is described in Section 11. In Section 12 we discuss how to construct the factors of a direct product of two classical groups. The centraliser of an involution is constructed using an algorithm of Bray [5]; this is considered in Section 13. The base cases of the algorithms (when $d \leq 6$) are discussed in Section 14. The complexity of the algorithms and the length of the resulting SLPs for the standard generators are discussed in Section 15 and 16. Finally we report on our implementation of the algorithm, publicly available in Magma [6].

2 Notation and background

We assume familiarity with the most basic results in the theory of classical groups; all can be found in [35]. In particular, we use Witt's Theorem in the following form,

Theorem 2.1 *Let V be a finite dimensional vector space that supports a non-degenerate bilinear form. Let U and W be subspaces of V, and let g be a linear isometry from U to W. Then there is a linear isometry f from V to V such that $uf = ug$ for all $u \in U$.*

For a proof see [35, Theorem 7.4]; we specialise to the case where $\mathrm{rad}(V) = 0$. EOB -- If the bilinear form restricted to U is non-degenerate, then f can be chosen to have determinant 1. If the form is symmetric, f had determinant 1, and U has codimension at least 2 in V, we can choose f to have spinor norm 1. This is because $V = W \oplus W^\perp$, and a linear isometry h can be constructed from V to V that maps W to W as the identity, and that maps $W^\perp$ to $W^\perp$ with the same determinant and (when relevant) the same spinor norm as h, and then fh^{-1} will be the required isometry of V.

If V has a bilinear form we denote the image of the ordered pair of vectors (u, v) in $V \times V$ under the form by $u.v$.

We establish some notation. Let $g \in G \leq \mathrm{GL}(d, q)$, let $\bar{G}$ denote $G/G \cap Z$ where Z denotes the centre of $\mathrm{GL}(d, q)$, and let $\bar{g}$ denote the image of g in $\bar{G}$. The *projective centraliser* of $g \in G$ is the preimage in G of $C_{\bar{G}}(\bar{g})$. Further, $g \in G$ is a *projective involution* if g^2 is scalar, but g is not.

We briefly review what we need of the structure of involution centralisers in (projective) classical groups defined over fields of odd characteristic. A detailed account can be found in [16, 4.5.1]. If h is an involution in a classical group G, then we denote its $+1$ and -1 eigenspaces by E_+ and E_- respectively. Observe that the dimension of the -1-eigenspace of an involution in $\mathrm{SX}(d,q)$ is always even.

If G preserves a non-degenerate form, it follows that E_+ and E_- are mutually orthogonal, and the form restricted to each of these spaces is non-degenerate. If $G \in \mathcal{C}$, then $C_G(u) = (\mathrm{GX}(E_+) \times \mathrm{GX}(E_-)) \cap G$. The centraliser of the image of u in the central quotient $\overline{G}$ of G is the image of $C_G(u)$ in $\overline{G}$ if E_+ and E_- are of different dimensions or (in the orthogonal case) of different types. Otherwise E_+ and E_- are isometric and the centraliser is the image of $(\mathrm{GX}(E_+) \wr C_2) \cap G$ in $\overline{G}$.

A subgroup of $\mathrm{GL}(U)$, where U is a subspace of V that supports a non-degenerate form, is regarded as a subgroup of $\mathrm{GL}(V)$ centralising $U^\perp$. With this convention, the base of the wreath product $\mathrm{GX}(E_+) \wr C_2$ is $\mathrm{GX}(E_+) \times \mathrm{GX}(E_-)$. Similarly, if E_+ and E_- are the eigenspaces of an involution in $\mathrm{GL}(V)$, a subgroup of $\mathrm{GL}(E_+)$ is regarded as a subgroup of $\mathrm{GL}(V)$ that centralises $\mathrm{GL}(E_-)$; and *mutatis mutandis* the same applies to a subgroup of $\mathrm{GL}(E_-)$.

We denote the subgroup of $\mathrm{SO}^\epsilon(n,q) \times \mathrm{SO}^\epsilon(m,q)$ consisting of those pairs of elements whose spinor norms are equal by $\mathrm{SO}^\epsilon(n,q) \times_{C_2} \mathrm{SO}^\epsilon(m,q)$.

We summarise some observations about symmetric bilinear forms of + and - type.

Lemma 2.2 *Let E_+ and E_- denote the $+1$ and -1 eigenspaces of an involution $h \in \Omega^\epsilon(d,q)$, where E_- has dimension e.*

(i) The form supported by E_- is of $-$ type if and only if both $q \equiv 3 \bmod 4$ and $e \equiv 2 \bmod 4$.

(ii) The restrictions of the symmetric bilinear form preserved by $\Omega^\epsilon(d,q)$ to the two eigenspaces of h are of the same type if $\epsilon = +1$, and are of opposite types if $\epsilon = -1$.

The proof of these assertions is elementary: $-I_2 \in \mathrm{O}^+(2,q)$ has spinor norm $+1$ if $q \equiv 1 \bmod 4$, and has spinor norm -1 if $q \equiv 3 \bmod 4$; whereas $-I_2 \in \mathrm{O}^-(2,q)$ has spinor norm -1 if $q \equiv 1 \bmod 4$, and has spinor norm $+1$ if $q \equiv 3 \bmod 4$.

To distinguish readily between symmetric bilinear forms of + and - type, we use the following observation.

Lemma 2.3 *If A is the $2n$-dimensional matrix of a symmetric bilinear form, then the form is of + type if $(-1)^n \det(A)$ is a square, otherwise the form is of - type.*

2.1 Cost and complexity

We use the 'big O' notation in the following way. If f and g are real valued functions, defined on all sufficiently large integers, we write $f(n) = O(g(n))$ to mean $|f(n)| <$

$c|g(n)|$ for some constant c and all sufficiently large n. The modulus here will be relevant only when $g(n)$ tends to 0 with n, as in $f(n) = O(1/n)$.

We record an elementary observation that is frequently used to estimate the cost of our 'divide-and-conquer' algorithms.

Lemma 2.4 *Let f be a real valued function defined on the set of integers greater than 1. Suppose that*

$$\exists k > 1 \quad \exists c > 0 \quad \forall d \geq 4 \quad \exists e \in (d/3, 2d/3] \quad f(d) \leq f(e) + f(d-e) + cd^k.$$

Then $f(d) = O(d^k)$.

PROOF: Let $m = \max(c/(1-(1/3)^k-(2/3)^k), f(2)/2^k, f(3)/3^k)$. We prove, by induction on $d > 1$, that $f(d) \leq md^k$ for all d. So suppose that $d \geq 4$, that e is as in the statement of the lemma, and that $f(n) \leq mn^k$ for all $n < d$. Then

$$\begin{aligned} f(d) &\leq f(e) + f(d-e) + cd^k \\ &\leq me^k + m(d-e)^k + cd^k \\ &= md^k \left(\left(\frac{e}{d}\right)^k + \left(\frac{d-e}{d}\right)^k \right) + cd^k \\ &\leq md^k \left(\left(\frac{1}{3}\right)^k + \left(\frac{2}{3}\right)^k \right) + cd^k \\ &\leq md^k. \end{aligned}$$

□

This lemma demonstrates that the cost of the recursive calls in a 'divide-and-conquer' algorithm of the type we employ does not affect the degree of complexity of the overall algorithm. The condition $k > 1$ is required to ensure that $1 - (1/3)^k - (2/3)^k > 0$.

3 Standard generators for classical groups

We now describe *standard generators* for the groups $\mathrm{SX}(d, q)$, where q is odd in all cases.

Recall that V is the natural module for $G = \mathrm{SX}(d, q)$. The standard generators for G are defined with respect to a hyperbolic basis for V, which will in turn be defined in terms of the given basis by a change-of-basis matrix. We define a *hyperbolic* basis for V as follows.

1. If V does not support a classical form, then any ordered basis, say $(e_1, \ldots, e_d)$, is hyperbolic.

2. If the form supported by V is symplectic of rank $2n$, then a hyperbolic basis for V is an ordered basis $(e_1, f_1, \ldots, e_n, f_n)$, where $e_i.e_j = f_i.f_j = 0$ for all i, j (including the case $i = j$), and $e_i.f_j = 0$ for $i \neq j$, and $e_i.f_i = -f_i.e_i = 1$ for all i.

3. If the form supported by V is hermitian and of rank $2n$, then a hyperbolic basis for V is exactly as for $\mathrm{Sp}(2n, q)$ except that, the form being hermitian, the condition $e_i.f_i = -f_i.e_i = 1$ for all i is replaced by the condition $e_i.f_i = f_i.e_i = 1$ for all i.

4. If the form supported by V is hermitian and of rank $2n + 1$, then a hyperbolic basis for V is an ordered basis of the form $(e_1, f_1, \ldots, e_n, f_n, w)$, where the above equations hold, and in addition $e_i.w = f_i.w = 0$ for all i, and $w.w = 1$.

5. If the form supported by V is symmetric bilinear of $+$ type and of rank $2n$, then a hyperbolic basis for V is an ordered basis of the form $(e_1, f_1, \ldots, e_n, f_n)$, where the equations used to define the form for $\mathrm{SU}(2n, q)$ again apply.

6. If the form supported by V is symmetric bilinear of $-$ type and of rank $2n$, then a hyperbolic basis for V is an ordered basis of the form $(e_1, f_1, \ldots, e_{n-1}, f_{n-1}, w_1, w_2)$, where the above relations hold for $i < n$, and in addition $w_1.e_i = w_1.f_i = w_2.e_i = w_2.f_i = w_1.w_2 = 0$, and $w_1.w_1 = -2$, and $w_2.w_2 = 2\omega$, where ω is a primitive element of $\mathrm{GF}(q)$. It is easy to see that, since ω is not a square in $\mathrm{GF}(q)$, this defines a form of $-$ type.

7. If the form supported by V is symmetric bilinear of 0 type and of rank $2n + 1$, then a hyperbolic basis for V is an ordered basis of the form $(e_1, f_1, \ldots, e_n, f_n, w)$, where again the relations in 3 hold, and in addition $w.e_i = w.f_i = 0$, and $w.w = -1/2$. Note that in this case multiplying the form by a non-square scalar produces a form that is inequivalent to the given form, but which is preserved by the same group. Thus the conditions imposed on a hyperbolic basis specify the equivalence class of the form.

For uniformity of exposition, we sometimes label the ordered basis for $\mathrm{SL}(2n, q)$ as $(e_1, f_1, \ldots, e_n, f_n)$ and that for $\mathrm{SL}(2n + 1, q)$ as $(e_1, f_1, \ldots, e_n, f_n, w)$.

A hyperbolic basis for a vector space with a given non-degenerate bilinear form can be constructed in $O(d^3)$ field operations (see [7] for an algorithm to perform this task).

Lemma 3.1 *If the form $\mathcal{F}$ supported by V is symmetric bilinear of 0 type and of rank $2n + 1$, then the determinant of $\mathcal{F}$, when multiplied by $(-1)^{n+1}2$, is a square.*

Hence if the form that is supported by V does not have this property, we multiply the form by a non-square scalar.

Subject to the following conventions, the standard generators for the non-orthogonal groups $\mathrm{SX}(d, q)$ are defined in Table 1, and for $\mathrm{SO}^\epsilon(d, q)$ in Table 2.

1. γ is a specified primitive element for $\mathrm{GF}(q^2)$, and $\alpha = \gamma^{(q+1)/2}$, and $\omega = \alpha^2$ is a primitive element for $\mathrm{GF}(q)$.

2. In all but one case, we describe v as a signed permutation matrix acting on the hyperbolic basis for V. We adopt the following notation. Given a basis for V, a signed permutation matrix with respect to this basis will be given as

a product of disjoint signed cyclic permutations of the basis elements. Such a cycle either permutes the vectors in the cycle, no sign being involved, or it sends each vector in the cycle to the next, except for the last vector which is sent to minus the first vector. In this case the cycle is adorned with the superscript $-$, as in $(e_1, e_2, \ldots, e_n)^-$. The superscript $+$ has no effect, so that $(e_1, e_2, \ldots, e_n)^+ = (e_1, e_2, \ldots, e_n)$. If we use the notation $(e_1, e_2, \ldots, e_n)^{\epsilon_n}$, then $\epsilon_n = +$ if n is odd, and $\epsilon_n = -$ if n is even.

3. For $\mathrm{SU}(2n+1, q)$, the matrices x and y normalise the subspace U having ordered basis $B = (e_1, w, f_1)$ and centralise $\langle e_2, f_2, \ldots, e_n, f_n \rangle$. We list their action on U with respect to basis B.

4. The remaining generators, other than v, of groups in Table 1 normalise a subspace U having ordered basis B, where $B = (e_1, f_1)$ or $B = (e_1, f_1, e_2, f_2)$, and centralise the space spanned by the remaining basis vectors. We write the action of a generator on U with respect to basis B.

5. In Table 2 the generators of $\mathrm{SO}^+(2n, q)$ that are given as 4×4 matrices normalise a subspace U having ordered basis B, where $B = (e_1, f_1, e_2, f_2)$, and centralise the subspace spanned by the remaining basis vectors. We write the action of a generator on U with respect to basis B. For $\mathrm{SO}^-(2n, q)$ the same applies, but with $B = (e_1, f_1, w_1, w_2)$, and for $\mathrm{SO}(2n+1, q)$ we take $B = (e_1, f_1, w)$, or $B = (e_1, f_1, e_2, f_2)$. We assume $n > 1$ for the groups $\mathrm{SO}^\epsilon(2n, q)$.

6. In the definition for $\Omega^-(2n, q)$, the variables A, B, C have the following values:

$$\begin{aligned} A &= \frac{1}{2}(\gamma^{q-1} + \gamma^{-q+1}) \\ B &= \frac{1}{2}\alpha(\gamma^{q-1} - \gamma^{-q+1}) \\ C &= \frac{1}{2}\alpha^{-1}(\gamma^{q-1} - \gamma^{-q+1}). \end{aligned}$$

7. For $SO^\epsilon(d, q)$, a unique generator σ is given that lies in the special orthogonal group, but has spinor norm -1; removing this generator gives the standard generating set for the corresponding $\Omega^\epsilon(d, q)$. For $\epsilon = 0, 1$, the value of b is determined by $q - 1 = 2^a \cdot b$; for $\epsilon = -1$ we have $\lambda = (-1)^{(q-1)/2}$.

8. To facilitate uniform exposition, we introduce trivial generators. If the dimension required to define a generator is greater than the dimension of the group, then the generator is assumed to be trivial.

By analogy with the general case, we assume that $\mathrm{SO}^+(2, q)$ has the same sequence of nine standard generators, where the only non-trivial elements are:

$$\delta = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{-2} \end{pmatrix} \quad \sigma = \begin{pmatrix} \omega^b & 0 \\ 0 & \omega^{-b} \end{pmatrix};$$

of course, $\Omega^+(2,q) = \langle \delta \rangle$.

Once a hyperbolic basis has been chosen for V, the Weyl group of G can be defined as a section of G, namely as the group of monomial matrices in G modulo diagonal matrices, thus defining a subgroup of the symmetric group S_d. The Weyl group of $G = \mathrm{SL}(d,q)$ is S_d. The Weyl group of $\mathrm{Sp}(2n,q)$ is the subgroup of S_{2n} that preserves the system of imprimitivity with blocks $\{e_i, f_i\}$ for $1 \le i \le n$, and is thus $C_2 \wr S_n$. The Weyl group of each of $\mathrm{SU}(2n,q)$ and $\mathrm{SU}(2n+1,q)$ is also $C_2 \wr S_n$. The Weyl group of $\Omega^+(2n,q)$ is the subgroup $(C_2 \wr S_n)^+$ of $C_2 \wr S_n$ consisting of even permutations. The Weyl group of $\Omega^-(2n,q)$ is $C_2 \wr S_{n-1}$, and the Weyl group of $\Omega(2n+1,q)$ is $C_2 \wr S_n$. `EOB -- Does Weyl group make sense for` SO`?`

If G is $\mathrm{SL}(d,q)$ or $\mathrm{Sp}(d,q)$, then the standard generators of $\mathrm{SX}(d,q)$ have the property that it is easy to construct from them any root group, and consequently they generate $\mathrm{SX}(d,q)$. The root groups are defined with respect to a maximal split torus, the group of diagonal matrices in $\mathrm{SX}(d,q)$; for a detailed description see [8]. The situation is similar for $\mathrm{SU}(d,q)$ and the orthogonal groups, as shown below.

Lemma 3.2 *Let $G = \mathrm{SU}(d,q)$ for $d \ge 2$. Then $G = \langle s, t, \delta, u, v, x, y \rangle$.*

Proof: If $d = 2n+1$, then a direct computation shows that

$$x^y = \begin{pmatrix} 1 & \omega^{q-2} & -\omega^{-(q+1)}/2 \\ 0 & 1 & \omega^{-2q+1} \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe that y has order q^2-1. Thus $S = \langle x^{y^k} : 1 \le k \le q^2-1 \rangle$ is a non-abelian group of order q^3, having derived group and centre of order q. A similar calculation for $d = 2n$ shows that $\langle x^{y^k} : 0 \le k < q^2-1 \rangle$ is a group of order q^2. These groups correspond to the subgroups X_S^1 of [8]; the result now follows from [8, Proposition 13.6.5]. □

Lemma 3.3 *Let $G = \Omega^+(2n,q)$ for $n \ge 2$. Then $G = \langle s, s', t, t', \delta, \delta', v \rangle$.*

Proof: If $n = 2$ then G is the central product of two copies of $\mathrm{SL}(2,q)$ (see [35, Corollary 12.39]). Let the natural modules for these copies of $\mathrm{SL}(2,q)$ be U_1 and U_2, and let these modules have ordered bases (a_1, b_1) and (a_2, b_2) respectively. Define an alternating bilinear form on U_i by $a_i.b_i = 1$ for $i = 1, 2$. This form is preserved by the respective copies of $\mathrm{SL}(2,q)$. Now define a bilinear form on $V = U_1 \otimes U_2$ by $(u_1 \otimes u_2).(v_1 \otimes v_2) = u_1.v_1 \times u_2.v_2$. This defines a non-degenerate symmetric form on V. A hyperbolic basis is then given by $(a_1 \otimes a_2, b_1 \otimes b_2, a_1 \otimes b_2, -b_1 \otimes a_2)$. Let s, t, δ in $\mathrm{SL}(U_1)$ be defined, with respect to the basis (a_1, b_1), by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix},$$

and let s', t', δ' denote the corresponding elements of $\mathrm{SL}(U_2)$. Now $\Omega^+(4,q)$ is the central product of these two copies of $\mathrm{SL}(2,q)$, and abusing notation by writing s, t

and δ for the images of (s, I_2), (t, I_2) and (δ, I_2) in $\Omega^+(4,q)$, and s', t', δ' for the images of (I_2, s'), (I_2, t') and (I_2, δ'), we obtain the first six given generators. Note that

$$s' = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}.$$

We also need to prove that the spinor norm of v is $+1$. If n is odd this follows since v is of odd order. It then suffices to consider the case $n = 2$ since

$$(e_{n-1}, e_n)^-(f_{n-1}, f_n)^-(e_1, \ldots, e_{n-1})^{\epsilon_{n-1}}(f_1, \ldots, f_{n-1})^{\epsilon_{n-1}} = (e_1, \ldots, e_n)^{-\epsilon_n}(f_1, \ldots f_n)^{-\epsilon_n}.$$

Thus the proof can take place in $\Omega(e_1, f_1, e_2, f_2)$. Then

$$\begin{aligned} (e_1, e_2)^-(f_1, f_2)^- &= (a_1 \otimes a_2, a_1 \otimes b_2)^-(b_1 \otimes b_2, -b_1 \otimes a_2)^- \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

and this product is in $\mathrm{SL}(U_1) \otimes \mathrm{SL}(U_2) = \Omega^+(4,q)$. The lemma follows. □

Lemma 3.4 *Let $G = \Omega^-(2n,q)$ for $n \geq 2$. Then $G = \langle s, t, \delta, u, v \rangle$.*

PROOF: If $n = 2$ then G is isomorphic to $\mathrm{PSL}(2, q^2)$ (see [35, Corollary 12.43]). This isomorphism arises as follows. Take the natural module U for $\mathrm{SL}(2, q^2)$, and let W be U twisted by the automorphism of $\mathrm{GF}(q^2)$ given by $a \mapsto a^q$. Then $U \otimes W$ gives rise to a representation of $\mathrm{PSL}(2, q^2)$ over $\mathrm{GF}(q^2)$. If (a_1, b_1) is a basis for U, and (a_2, b_2) is a basis for W, then the resulting representation of $\mathrm{PSL}(2, q^2)$ on $U \otimes W$ with respect to the ordered basis $(a_1 \otimes a_2, a_1 \otimes b_2, b_1 \otimes a_2, b_1 \otimes b_2)$ preserves the symmetric non-degenerate bilinear form

$$\begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix},$$

where

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Now let γ be a primitive element of $\mathrm{GF}(q^2)$, and let $\alpha = \gamma^{\frac{1}{2}(q+1)}$, so that α^2 is a primitive element ω of $\mathrm{GF}(q)$. Conjugating by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & -\alpha & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

transforms the above image of $\mathrm{PSL}(2, q^2)$ into a subgroup of $\mathrm{SL}(4, q)$. Interchanging the second and fourth basis vectors now transforms this image into a group that preserves the form

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 2\omega \end{pmatrix},$$

and thus into our chosen copy of $\Omega^-(4,q)$. It is straightforward to check that the given given generators s, t, δ are the images of the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix},$$

and hence generate $\Omega^-(4,q)$. It follows, as with the case of $\Omega^+(2n,q)$, that these generators, together with u and v, generate $\Omega^-(2n,q)$. □

Lemma 3.5 *Let $G = \Omega(2n+1,q)$ for $n \geq 1$. Then $G = \langle s, t, \delta, u, v \rangle$.*

PROOF: If $n = 1$ then G is isomorphic to $\mathrm{PSL}(2,q)$ (see [35, Theorem 11.6]). This isomorphism arises as follows. Take the natural module U for $\mathrm{SL}(2,q)$, and let V be the symmetric square of U. If (a,b) is a basis for U then, with respect to the ordered basis (a^2, b^2, ab) of V, the form

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}$$

is preserved by G. This exhibits $\mathrm{PSL}(2,q)$ as $\Omega(3,q)$. The generators s, t, δ then correspond to the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}.$$

Thus the given matrices generate $\Omega(2n+1,q)$. □

Lemma 3.6 *The standard generator $\sigma \in \mathrm{SO}^\epsilon(d,q) \setminus \Omega^\epsilon(d,q)$.*

PROOF: It is clear that in all cases $\sigma \in \mathrm{SO}^\epsilon(d,q)$, so it remains to compute the spinor norm of σ.

Consider first the case where $q \equiv 3 \bmod 4$. Now σ acts as an involution on a 2-dimensional space of + type, and centralises its orthogonal complement. Thus it suffices to prove that $\Omega^+(2,q)$ is of odd order; but the order of this group is $(q-1)/2$.

`EOB -- Rest of argument needs attention. A similar argument applies when` $q \equiv 1 \bmod 4$: `now` σ `acts as an involution on a 2-dimensional space of` $-$ `type and` $\Omega^-(2,q)$ `has order` $(q+1)/2$. □

We conclude this section with the following observation.

Lemma 3.7 *If $d = 2n$ is even and $G = \langle s, t, \delta, u, v, x, y \rangle$ is not an orthogonal group, and if $H = \langle s, t, \delta, u, v \rangle$, then $H = \mathrm{SL}(2,q) \wr C_n$, or $H = \mathrm{SL}(2,q) \wr S_n$ or $H = \mathrm{SU}(2,q) \wr S_n$ according as G is a special linear, symplectic or special unitary group.*

For non-orthogonal groups in even dimensions, we postpone the construction of the generator x (and y in the case of unitary groups) to reduce the time spent in the more difficult base cases, and instead construct the wreath product identifed in Lemma 3.7. Observe that vx acts as a $2n$-cycle on the hyperbolic basis for $\mathrm{SL}(2n,q)$.

Group	s	t	δ	u	v	x	y
$\mathrm{SL}(2n,q)$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$	I_2	$(e_1,e_2,\ldots,e_n)(f_1,f_2,\ldots,f_n)$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$	I_4
$\mathrm{SL}(2n+1,q)$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$	I_2	$\begin{pmatrix} 0 & 1 \\ -I_{2n} & 0 \end{pmatrix}$	I_4	I_4
$\mathrm{Sp}(2n,q)$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$(e_1,e_2,\ldots,e_n)(f_1,f_2,\ldots,f_n)$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$	I_4
$\mathrm{SU}(2n,q)$	$\begin{pmatrix} 0 & \alpha \\ \alpha^{-q} & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \gamma^{q+1} & 0 \\ 0 & \gamma^{-(q+1)} \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$(e_1,e_2,\ldots,e_n)(f_1,f_2,\ldots,f_n)$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \gamma & 0 & 0 & 0 \\ 0 & \gamma^{-q} & 0 & 0 \\ 0 & 0 & \gamma^{-1} & 0 \\ 0 & 0 & 0 & \gamma^{q} \end{pmatrix}$
$\mathrm{SU}(2n+1,q)$	$\begin{pmatrix} 0 & \alpha \\ \alpha^{-q} & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \gamma^{q+1} & 0 \\ 0 & \gamma^{-(q+1)} \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$(e_1,e_2,\ldots,e_n)(f_1,f_2,\ldots,f_n)$	$\begin{pmatrix} 1 & 1 & -1/2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \gamma & 0 & 0 \\ 0 & \gamma^{q-1} & 0 \\ 0 & 0 & \gamma^{-q} \end{pmatrix}$

Table 1: Standard generators for non-orthogonal classical groups

Group	s	t	δ	u	v	σ
$\mathrm{SO}^+(2n,q)$	$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega^{-1} \end{pmatrix}$	I_4	$(e_1,e_2,\ldots,e_n)^{\epsilon_n}(f_1,f_2,\ldots,f_n)^{\epsilon_n}$	$\begin{pmatrix} \omega^b & 0 & 0 & 0 \\ 0 & \omega^{-b} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
	s'	t'	δ'			
	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & \omega^{-1} & 0 \\ 0 & 0 & 0 & \omega \end{pmatrix}$			
Group	s	t	δ	u	v	σ
$\mathrm{SO}^-(2n,q)$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & A & B \\ 0 & 0 & C & A \end{pmatrix}$	$\begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$	$(e_1,\ldots,e_{n-1})^{\epsilon_{n-1}}(f_1,\ldots,f_{n-1})^{\epsilon_{n-1}}$	$\begin{pmatrix} \lambda I_2 & 0 \\ 0 & -\lambda I_2 \end{pmatrix}$
Group	s	t	δ	u	v	σ
$\mathrm{SO}(2n+1,q)$	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega^2 & 0 & 0 \\ 0 & \omega^{-2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$	I_4	$(e_1,\ldots,e_n)^{\epsilon_n}(f_1,\ldots,f_n)^{\epsilon_n}$	$\begin{pmatrix} \omega^b & 0 & 0 \\ 0 & \omega^{-b} & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Table 2: Standard generators for orthogonal groups

4 Algorithm `One` for non-orthogonal groups

Let $G = \mathrm{SX}(d, q)$ denote a non-orthogonal group in $\mathcal{C}$. Algorithm `One` takes as input a generating set X for G, and returns standard generators for G as SLPs in X. The generators are in standard form with respect to a hyperbolic basis for the natural module V. The change-of-basis matrix from the given basis to the hyperbolic basis is also returned.

The algorithm employs a 'divide-and-conquer' strategy.

Definition 4.1 *A strong involution in* $\mathrm{SX}(d, q)$ *for* $d > 4$ *is an involution whose* -1*-eigenspace has dimension in the range* $(d/3, 2d/3]$.

The main algorithm `OneMain` has two subcases, according to the parity of the input dimension. Algorithm `OneEven` addresses the case of even d, and algorithm `OneOdd` the case of odd d. Recall, from Lemma 3.7, that, for $d = 2n$, $Y_0 = \{s, t, \delta, u, v\}$ generates $\mathrm{SX}(2, q) \wr C_n$ or $\mathrm{SX}(2, q) \wr S_n$ according to the type of the input group. This observation has important consequences, which we will consider in more detail in Section 14. If d is even, then, as the first and major part of the main algorithm, `OneEven` constructs Y_0; as a final step, `OneMain` constructs the additional elements x, y.

Algorithm 1: `OneEven` $(X, type, \mathcal{F})$ for non-orthogonal groups

/* X is a generating set for the perfect classical group G in odd characteristic, of type SL or Sp or SU, in even dimension. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set Y_0 for $\mathrm{SL}(2,q) \wr C_{d/2}$ if *type* is SL, otherwise for $\mathrm{SL}(2,q) \wr S_{d/2}$, as subgroup of G, the SLPs for the elements of Y_0 and the change-of-basis matrix. */

1 **begin**
2 $d :=$ the rank of the matrices in X;
3 if $d = 2$ then return `BaseCase` $(X, type, \mathcal{F})$;
4 Find by random search $g \in G := \langle X \rangle$ of even order such that g powers to a strong involution h;
5 Let E_+ of dimension $2k$ and E_- be the eigenspaces of h;
6 Find generators for the centraliser C of h in G;
7 Rewrite with respect to the concatenation of hyperbolic bases for E_+ and E_-;
8 In C find generating sets X_1 and X_2 for $\mathrm{SX}(E_+)$ and $\mathrm{SX}(E_-)$;
9 $((s_1, t_1, \delta_1, u_1, v_1), B_1) :=$ `OneEven` $(X_1, type, \mathcal{F}|_{E_+})$;
10 $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ `OneEven` $(X_2, type, \mathcal{F}|_{E_-})$;
11 Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{d/2}, f_{d/2})$ be the concatenation of the hyperbolic bases defined by B_1 and B_2;
12 $a := (s_1^2)^{v_1^{-1}}(s_2^2)$;
13 Find generators for the centraliser D of a in G;
14 In D find a generating set X_3 for $\mathrm{SX}(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$;
15 In $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
16 $v := v_2 b v_1$;
17 return $(s_1, t_1, \delta_1, u_1, v)$ and the change-of-basis matrix for B;
18 **end**

If the type is SL, then the centraliser of h is $(\mathrm{GL}(E_+) \times \mathrm{GL}(E_-)) \cap \mathrm{SL}(d,q)$ where E_+ and E_- are the eigenspaces of h. If the type is Sp, it is $\mathrm{Sp}(E_+) \times \mathrm{Sp}(E_-)$; and if the type is SU, it is $(U(E_+) \times U(E_-)) \cap \mathrm{SU}(d,q)$. Thus, if the eigenspaces have dimensions e and $d-e$, then the derived subgroup of the centraliser of u in $\mathrm{SX}(d,q)$ is $\mathrm{SX}(e,q) \times \mathrm{SX}(d-e,q)$.

We make the following observations on Algorithm `OneEven`.

1. The SLPs that express the standard generators in terms of X are also returned.

2. Generators for the involution centralisers in lines 8 and 15 are constructed using the algorithm of Bray [5], see Section 13. We need only a subgroup of the centraliser that contains the derived subgroup.

3. The generators for the direct factors in line 8 are constructed using the algorithm described in Section 12.

4. The algorithms for the `BaseCase` call in line 3 are discussed in Section 14. In summary, `BaseCase` $(X, type, \mathcal{F})$ returns the standard generating set Y and the associated SLPs for the classical group $\langle X \rangle$ of the specified type having associated form $\mathcal{F}$.

5. The search in line 4 for an element that powers to a strong involution is discussed in Section 9.

6. The recursive calls in lines 11 and 12 are in smaller dimension. As shown in Lemma 2.4, these calls only affect the time or space complexity of the algorithm up to a constant multiple; however they contribute more seriously to the length of the SLPs produced. We consider these issues in Sections 15 and 16.

7. In line 14, a is an involution with -1-eigenspace $\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle$.

8. `EOB -- Needs attention in light of decision to pass form as argument. For` $\mathrm{Sp}(d, q)$ `and` $\mathrm{SU}(d, q)$ `the eigenspaces of an involution are mutually orthogonal, and the form restricted to either eigenspace is non-degenerate. The form is only defined, by the group, up to a scalar multiple. However the hyperbolic bases returned by the two recursive calls must be with respect to the same form. We use hyperbolic bases to encode forms. Given a hyperbolic basis there is a unique form with respect to which the basis is hyperbolic. The forms used in line 7 are the restrictions to` $E_+$ `and` $E_-$ `of a form on` $V$ `preserved by` $G$`. This form is chosen to be the unique form with respect to which the given basis for` $V$ `is hyperbolic, provided that this form is preserved by` $G$`, which will be the case in recursive calls.`

The element b is referred to as the 'glue' element, since it is used in the assignment $v := v_2 b v_1$ to 'glue' the elements v_1 and v_2 to produce v. We discuss how to find b as an element of $\langle X_3 \rangle$ in Section 14.2.

Algorithm `OneOdd`, which considers the case of odd degree d, is similar to Algorithm `OneEven`. Most of our commentary on the even degree case also applies to the odd case.

Algorithm 2: `OneOdd` $(X, type, \mathcal{F})$ for non-orthogonal groups

/* X is a generating set for the perfect classical group G in odd characteristic and odd dimension, of type SL or SU. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set for G, the SLPs for elements of this generating set, and the change-of-basis matrix. */

1 **begin**
2 $d :=$ the rank of the matrices in X;
3 if $d = 3$ then return `BaseCase` $(X, type, \mathcal{F})$;
4 Find by random search $g \in G := \langle X \rangle$ of even order such that g powers to a strong involution h;
5 Let E_+ and E_- be the eigenspaces of h;
6 Find generators for the centraliser C of h in G;
7 Rewrite with respect to the concatenation of hyperbolic bases for E_+ and E_-;
8 In C find generating sets X_1 and X_2 for $\mathrm{SX}(E_+)$ and $\mathrm{SX}(E_-)$;
9 $((s_1, t_1, \delta_1, u_1, v_1, x, y), B_1) :=$ `OneOdd` $(X_1, type, \mathcal{F}|_{E_+})$;
10 $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ `OneEven` $(X_2, type, \mathcal{F}|_{E_-})$;
11 If $B_1 = (e_1, f_1, \ldots, e_k, f_k, w)$ and $B_2 = (e_{k+1}, f_{k+1}, \ldots, e_{(d-1)/2}, f_{(d-1)/2})$ let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{(d-1)/2}, f_{(d-1)/2}, w)$;
12 $a := (s_1^2)^{v_1^{-1}}(s_2^2)$;
13 Find generators for the centraliser D of a in G;
14 In D find a generating set X_3 for $\mathrm{SX}(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$;
15 In $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
16 $v := v_2 b v_1$;
17 return $(s_1, t_1, \delta_1, u_1, v, x, y)$ and the change-of-basis matrix for B;
18 **end**

We summarise the main algorithm in the case of non-orthogonal groups as Algorithm `OneMain`.

The correctness and complexity of this algorithm, and the lengths of the resulting SLPs for the standard generators, are discussed in Sections 9 and 15–16. The construction of x and y are discussed in Section 14.

5 Algorithm `Two` for non-orthogonal groups

We present a variant of the algorithms in Section 4 based on one recursive call rather than two. Again we denote the groups $\mathrm{SL}(d, q)$, $\mathrm{Sp}(d, q)$ and $\mathrm{SU}(d, q)$ by $\mathrm{SX}(d, q)$, and the corresponding projective group by $\mathrm{PX}(d, q)$.

The key idea is as follows. Suppose that d is a multiple of 4. We find $g \in \mathrm{SX}(d, q)$ of order $2m$ and an involution $h := g^m$, as in line 6 of `OneEven`, but insist that both eigenspaces of h have dimension $d/2$.

Let $\bar{h}$ be the image of h in $\mathrm{PX}(d, q)$. The centraliser of $\bar{h}$ in $\mathrm{PX}(d, q)$ interchanges the

Algorithm 3: `OneMain` $(X, type, \mathcal{F})$ for non-orthogonal groups

```
/* X is a generating set for the perfect classical group G in odd characteristic,
   of type SL or Sp or SU. The classical form preserved by G is F. Return the
   standard generators for G, the SLPs for these generators, and change-of-basis
   matrix.                                                                  */
1  begin
2      d := the rank of the matrices in X;
3      if d is odd then
4          ((s, t, δ, u, v, x, y), B) := OneOdd (X, type, F);
5      else
6          ((s, t, δ, u, v), B) := OneEven (X, type, F);
7          Construct additional elements x and y;
8      end
9      return (s, t, δ, u, v, x, y) and the change-of-basis matrix B;
10 end
```

eigenspaces E_+ and E_- of h. We construct the projective centraliser of h by applying the algorithm of [5] to $\bar{h}$ and $\mathrm{PX}(d, q)$.

If we now find recursively the subset Y_0 of standard generators for $\mathrm{SX}(E_+)$ with respect the basis $\mathcal{B}$, then Y_0^g is a set of standard generators for $\mathrm{SX}(E_-)$ with respect to the basis $\mathcal{B}^g$. We now use these to construct standard generators for $\mathrm{SX}(d, q)$ exactly as in Algorithm `One`.

If d is an odd multiple of 2, we find an involution with one eigenspace of dimension exactly 2. The centraliser of this involution allows us to construct $\mathrm{SX}(2, q)$ and $\mathrm{SX}(d-2, q)$. The $d-2$ factor is now processed as above, since $d-2$ is a multiple of 4, and the 2 and $d-2$ factors are combined as in the first algorithm. Thus the algorithm deals with $\mathrm{SX}(d, q)$, for even values of d, in a way that is similar in outline to the familiar method of powering, that computes a^n, by recursion on n, as $(a^2)^{n/2}$ for even n and as $a(a^{n-1})$ for odd n.

Algorithms `TwoTimesFour` and `TwoTwiceOdd` describe the case of even d. Algorithm `TwoTimesFour` calls no new procedures except in line 5, where we construct an involution with eigenspaces of equal dimension. This construction is discussed in Section 10. Algorithm `TwoEven`, which summarises the even degree case, returns the generating set Y_0 defined in Section 3. We complete the construction of Y exactly as in Section 4.

If d is odd, then we find an involution whose -1-eigenspace has dimension 3, thus splitting d as $(d-3)+3$. Since $d-3$ is even, we apply the odd case *precisely once*.

The resulting `TwoOdd` is otherwise the same as `OneOdd`, except that it calls `TwoEven` rather than `OneEven`; similarly `TwoMain` calls `TwoOdd` and `TwoEven` if $d \geq 8$, and otherwise calls `OneMain`.

The primary advantage of the second algorithm lies in its one recursive call. As we show in Section 16, this reduces the lengths of the SLPs for the standard generators.

Algorithm 4: `TwoTimesFour`$(X, type, \mathcal{F})$ for non-orthogonal groups

/*X is a generating set for the perfect classical group G in odd characteristic, of type SL or Sp or SU, in dimension a multiple of 4. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set for G, and the change-of-basis matrix. */

begin
  $d :=$ the rank of the matrices in X;
  if $d = 4$ return `OneMain` $(X, type, \mathcal{F})$;
  $k := d/4$;
  Find an involution h with eigenspaces of dimension $2k$;
  Let E_+ and E_- be the eigenspaces of h;
  Find generators for the projective centraliser C of h in G and identify an element c of C that interchanges the two eigenspaces;
  In C find a generating set X_1 for $\mathrm{SX}(E_+)$;
  $((s_1, t_1, \delta_1, u_1, v_1, x_1, y_1), B_1) :=$ `TwoEven`$(X_1, type, \mathcal{F}|_{E_+})$;
  $s_2 := s_1^c$;
  Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{2k}, f_{2k})$ be the concatenation of the bases defined by B_1 and B_1^c;
  $a := (s_1^2)^{v_1^{-1}}(s_2^2)$;
  Find generators for the centraliser D of a in G;
  In D find a generating set X_3 for $\mathrm{SX}(\langle e_k, f_k, e_{k+1}, f_{k+1}\rangle)$;
  In $\langle X_3\rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
  $v := v_2 b v_1$;
  return $(s_1, t_1, \delta_1, u_1, v, x, y)$ and the change-of-basis matrix for B;
end

Algorithm 5: `TwoTwiceOdd`$(X, type, \mathcal{F})$ for non-orthogonal groups

/* X is a generating set for the perfect classical group G in odd characteristic, of type SL or Sp or SU, in dimension $d = 2(k+1)$ for even k. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set for G, and the change-of-basis matrix. */

begin
  $d :=$ the rank of the matrices in X;
  If $d < 10$ return `OneMain` $(X, type, \mathcal{F})$;
  Find $g \in G := \langle X \rangle$ of even order such that g powers to an involution h with eigenspaces of dimensions 2 and $d-2$;
  Find generators for the centraliser C of h in G;
  Let E_1 and E_2 be the eigenspaces of h, of dimensions $d-2$ and 2 respectively;
  Rewrite with respect to the concatenation of hyperbolic bases for E_1 and E_2;
  In C find generating sets X_1 and X_2 for $\mathrm{SX}(E_1)$ and $\mathrm{SX}(E_2)$ respectively;
  $((s_1, t_1, \delta_1, u_1, v_1, , x_1, y_1), B_1) :=$ `TwoTimesFour` $(X_1, type, \mathcal{F}|_{E_1})$;
  $((s_2, t_2, \delta_2), B_2) :=$ `OneMain` $(X_2, type, \mathcal{F}|_{E_2})$;
  Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1})$ be the concatenation of the hyperbolic bases B_1 and B_2;
  $a := (s_1^2)^{v_1^{-1}}(s_2^2)$;
  Find generators for the centraliser D of a in G;
  In D find a generating set X_3 for $\mathrm{SX}(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$;
  In $\langle X_3 \rangle$ find the signed permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
  $v := bv_1$;
  return $(s_1, t_1, \delta_1, u_1, v, x_1, y_1)$ and the change-of-basis matrix for B.
end

Algorithm 6: `TwoEven`$(X, type, \mathcal{F})$ `for non-orthogonal groups`

/* X is a generating set for the perfect classical group G in odd characteristic, of type SL or Sp or SU, in even dimension d. The classical form preserved by G is $\mathcal{F}$. Return standard generating set for G, and the change-of-basis matrix. */

begin
  $d :=$ the rank of the matrices in X;
  if $d \bmod 4 = 2$ **then**
    return `TwoTwiceOdd`$(X, type, \mathcal{F})$;
  else
    return `TwoTimesFour`$(X, type, \mathcal{F})$;
  end
end

6 Algorithm `One` for orthogonal groups

The algorithms for orthogonal groups are more complex in design than those for other classical groups. In particular, the algorithm for $\Omega^\epsilon(d,q)$ depends both on the type of form preserved and on the residue of q mod 4.

For each of the form types, we present three algorithms: for $\Omega^\epsilon(d,q)$ where $q \equiv 1 \bmod 4$, then $\mathrm{SO}^\epsilon(d,q)$, and finally for $\Omega^\epsilon(d,q)$ where $q \equiv 1 \bmod 3$.

6.1 Groups preserving forms of + type

6.1.1 $\Omega^+(2n,q)$ for $q \equiv 1 \bmod 4$

This case is very similar to Algorithm `One` for the other classical groups.

Let $G = \Omega^+(2n,q)$ where $q \equiv 1 \bmod 4$ and let V denote the underlying vector space.

We say that an involution h of G is *suitable* if it is strong and has the additional property that the symmetric bilinear form preserved by G, when restricted to each of its eigenspaces, is of + type.

We summarise the resulting algorithm.

Algorithm 7: `OneOmegaPlus` $(X, \mathcal{F})$

/* X is a generating set for the orthogonal group G of type + defined over a field of odd characteristic and size $q \equiv 1 \bmod 4$. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set Y for G, the SLPs for the elements of Y and the change-of-basis matrix. */

begin
  $d :=$ the rank of the matrices in X;
  if $d \leq 4$ then return `PlusBaseCase` $(X, \mathcal{F})$;
  Find by random search $g \in G := \langle X \rangle$ of even order such that g powers to a suitable involution h;
  Let E_+ be the $+1$-eigenspace of h having dimension $2k$ and let E_- be its -1-eigenspace;
  Find generators for the centraliser C of h in G;
  Rewrite with respect to the concatenation of hyperbolic bases for E_+ and E_-;
  In C find generating sets X_1 and X_2 for $\Omega^+(E_+)$ and $\Omega^+(E_-)$;
  $((s_1, t_1, \delta_1, u_1, v_1, s_1', t_1', \delta_1'), B_1) :=$ `OneOmegaPlus` $(X_1, \mathcal{F}|_{E^+})$;
  $((s_2, t_2, \delta_2, u_2, v_2, s_2', t_2', \delta_2'), B_2) :=$ `OneOmegaPlus` $(X_2, \mathcal{F}|_{E^-})$;
  Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{d/2}, f_{d/2})$ be the concatenation of the hyperbolic bases defined by B_1 and B_2;
  $n := (q-1)/4$;
  $a = ((\delta_1\delta_1')^n)^{v_1^{-1}}(\delta_2\delta_2')^n$;
  Find generators for the centraliser D of a in G;
  In D find a generating set X_3 for $\Omega^+(\langle e_k, f_k, e_{k+1}, f_{k+1}\rangle)$;
  In $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
  $v := v_2 b v_1$;
  return $(s_1, t_1, \delta_1, u_1, v, s_1', t_1', \delta_1')$ and the change-of-basis matrix for B;
end

6.1.2 $\mathrm{SO}^+(2n, q)$

The algorithm for this case is independent of the value of $q \bmod 4$. The definition of a suitable involution is as in Section 6.1.1. The centraliser in $\mathrm{SO}^+(2n, q)$ of a suitable involution contains the direct product of $\mathrm{SO}(E_+)$ and $\mathrm{SO}(E_-)$. We construct each group as a subgroup of the centraliser, and proceed recursively. The resulting algorithm, `OneSpecialPlus`, differs in one respect only from `OneOmegaPlus`: the recursive calls are to `OneSpecialPlus`, and so construct the additional standard generator σ needed to generate $\mathrm{SO}^+(2n, q)$.

6.1.3 $\Omega^+(2n, q)$ when $q \equiv 3 \bmod 4$

The algorithm for $G = \Omega^+(2n, q)$ and $q \equiv 3 \bmod 4$ is more elaborate than that when $q \equiv 1 \bmod 4$: now $\Omega^+(2, q)$ has odd order $(q-1)/2$ and so does not contain $-I_2$. In

order to construct the involution whose centraliser contains the 'glue' element, we must move outside $\Omega(E)$ to $\mathrm{SO}(E)$ where E is a relevant eigenspace.

We outline the steps of the algorithm, `OneOmegaPlus3`, which applies when $n > 2$.

1. Find, by random search, an element of G that powers up to an strong involution i having eigenspaces E and F, with the additional property that the symmetric bilinear form preserved by G, when restricted to these eigenspaces, is of + type.

2. Construct a generating set of $H = \mathrm{SO}(E) \times_{C_2} \mathrm{SO}(F)$, and hence generating sets X and Y for $\Omega(E)$ and $\Omega(F)$ as subgroups of G.

3. Find by random search within H an element $g = (g_1, g_2)$, where $g_1 \in \mathrm{SO}(E)$, and $g_2 \in \mathrm{SO}(F)$, and the spinor norms of g_1 and of g_2 are both -1. We also require one of the g_j, say g_2, to be of twice odd order. By powering up, we may now assume that g has order a power of 2, and g_2 is an involution. `EOB -- WHERE DO WE ADDRESS COST OF THIS?`

4. Let $A = \langle X, g \rangle$. Its projection onto E is $\mathrm{SO}(E)$. Using `OneSpecialPlus`, construct words in the generators of A that map onto standard generators for $\mathrm{SO}(E)$.

5. Evaluate these generators in their action on V.

   Recall that g is an element of spinor norm -1 and g_2 is an involution. Hence the standard generators for $\Omega(E)$, which have been found as words in the generating set for A, all involve g to an even multiplicity, and so restrict to the identity on F. Thus, in their action on V, the standard generators for $\Omega(E)$ centralise F. Let σ be the standard generator for $\mathrm{SO}(E)$ that, as shown in Lemma 3.6, has spinor norm -1. In its action on V, σ has form $h = (g_3, g_2)$, where g_3 is an involution.

6. Let $B = \langle Y, h \rangle$. Its projection onto F is $\mathrm{SO}(F)$. Using `OneSpecialPlus`, construct words in the generators of B that map onto standard generators for $\mathrm{SO}(F)$ and evaluate these generators in their action on V. Let σ be the standard generator for $\mathrm{SO}(F)$ having spinor norm -1. In its action on V, σ has form (g_3, g_4), where g_4 is an involution.

7. Hence (g_3, g_4) is an involution and conjugating by v_1 we can construct the involution σ with a -1-eigenspace of dimension 4.

The remaining steps of the algorithm are identical to those described in `OneOmegaPlus` where $q \equiv 1 \bmod 4$. Namely, we find generators for the centraliser D of a in G, construct a generating set X_3 for $\Omega^+(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$; in $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$; and finally construct the last standard generator $\sigma := v_2 b v_1$.

6.2 Groups preserving forms of − type

6.2.1 $\Omega^-(2n, q)$ when $q \equiv 1 \bmod 4$

In summary, we construct an involution whose centraliser contains a direct product of $\Omega^+(2n-4, q)$ and $\Omega^-(4, q)$. We then recursively construct standard generators for each. Within the centraliser of an involution of + type, we find the 'glue' element.

An involution of $\Omega^-(2n, q)$ is *suitable* if it has one eigenspace of dimension 4 supporting a form of − type; and its other eigenspace, consequently of dimension $2n-4$, supports a form of + type.

Algorithm 8: `OneOmegaMinus` $(X, \mathcal{F})$

/* X is a generating set for the orthogonal group G of type − defined over a field of odd characteristic and size $q \equiv 1 \bmod 4$. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set Y for G, the SLPs for the elements of Y and the change-of-basis matrix. */

begin
- $d :=$ the rank of the matrices in X;
- if $d = 4$ then return `MinusBaseCase` (X, F);
- Find by random search $g \in G := \langle X \rangle$ of even order such that g powers to a suitable involution h;
- Let E be the eigenspace of h of dimension $2n-4$ and let F be the eigenspace of h having dimension 4;
- Find generators for the centraliser C of h in G;
- Rewrite with respect to the concatenation of hyperbolic bases for E and F;
- In C find generating sets X_1 and X_2 for $\Omega^+(E)$ and $\Omega^-(F)$;
- $((s_1, t_1, \delta_1, u_1, v_1, s_1', t_1', \delta_1'), B_1) :=$ `OneOmegaPlus` $(X_1, \mathcal{F}|_E)$;
- $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ `OneOmegaMinus` $(X_2, \mathcal{F}|_F)$;
- Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{d/2}, f_{d/2})$ be the concatenation of the hyperbolic bases defined by B_1 and B_2;
- $n := (q-1)/4$;
- $a := ((\delta_1 \delta_1')^n)^{v_1^{-1}} \delta_2^{n(q+1)}$;
- Find generators for the centraliser D of a in G;
- In D find a generating set X_3 for $\Omega^+(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$;
- In $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
- $v := bv_1$;
- return $(s_1, t_1, \delta_1, u_1, v)$ and the change-of-basis matrix for B;

end

6.2.2 $\mathrm{SO}^-(d, q)$

The algorithm for this case is independent of the value of $q \bmod 4$. The definition of a suitable involution is as in Section 6.2.1. The centraliser in $\mathrm{SO}^-(2n, q)$ of a suitable involution contains the direct product of $\mathrm{SO}^+(E)$ and $\mathrm{SO}^-(F)$. We construct each

group as a subgroup of the centraliser, and proceed recursively. The resulting algorithm, `OneSpecialMinus`, differs in one respect only from `OneOmegaMinus`: the calls are to `OneSpecialPlus` and `OneSpecialMinus`, and so construct the additional standard generator σ needed to generate $\mathrm{SO}^-(2n, q)$.

6.2.3 $\Omega^-(2n, q)$ when $q \equiv 3 \bmod 4$

In summary, we construct an involution in $G = \Omega^-(2n, q)$ whose centraliser contains a direct product of $\Omega^+(2n - 2k, q)$ and $\Omega^-(2k, q)$, where k is 2 or 3, depending on the parity of n. We then recursively construct standard generators for each. As in the corresponding case of $\Omega^+(2n, q)$, we must move from Ω^ϵ to the corresponding SO^ϵ to find the involution whose centraliser contains the 'glue' element.

However, the definition of a suitable involution is now more complex.

- If $n > 3$ is even, then an involution is *suitable* if its $+1$-eigenspace has dimension 4 and supports a form of $-$ type, and its -1-eigenspace of dimension $2n - 4$ supports a form of $+$ type.
- If $n > 3$ is odd, then an involution is *suitable* if it has one eigenspace of dimension 6 that supports a form of $-$ type, and its other eigenspace of dimension $2n - 6$ supports a form of $+$ type.

We now outline the steps of the algorithm, `OneOmegaMinus3`. Similar in structure to `OneOmegaPlus3`, it applies only when $n > 3$.

1. Find, by random search, an element of G that powers up to an suitable involution i. Let E and F denote the eigenspaces of i which support the forms of $-$ and $+$ type respectively.
2. Construct a generating set of $H = \mathrm{SO}^+(E) \times_{C_2} \mathrm{SO}^-(F)$, and hence generating sets X and Y for $\Omega(E)$ and $\Omega(F)$ as subgroups of G.
3. Find by random search within H an element $g = (g_1, g_2)$, where $g_1 \in \mathrm{SO}^+(E)$, and $g_2 \in \mathrm{SO}^-(F)$, and the spinor norms of g_1 and of g_2 are both -1. We also require one of the g_j, say g_2, to be of twice odd order. By powering up we may then assume that g is of order a power of 2, and that g_2 is an involution. `EOB -- COST OF THIS?`
4. Let $A = \langle X, g \rangle$. Its projection onto E is $\mathrm{SO}^+(E)$. Using `OneSpecialPlus`, construct words in the generators of A that map onto standard generators for $\mathrm{SO}^+(E)$.
5. Evaluate these generators in their action on V.

   Recall that g is an element of spinor norm -1 and g_2 is an involution. Hence the standard generators for $\Omega^+(E)$, which have been found as words in the generating

set for A, all involve g to an even multiplicity, and so restrict to the identity on F. Thus, in their action on V, the standard generators for $\Omega^+(E)$ centralise F.

Let σ be the standard generator for $\mathrm{SO}^+(E)$ having spinor norm -1. In its action on V, σ has form $h = (g_3, g_2)$, where g_3 is an involution.

6. Let $B = \langle Y, h \rangle$. Its projection onto F is $\mathrm{SO}^-(F)$. Using `OneSpecialMinus`, construct words in the generators of B that map onto standard generators for $\mathrm{SO}^-(F)$, and evaluate these generators in their action on V. Let σ be the standard generator for $\mathrm{SO}^-(F)$ having spinor norm -1. In its action on V, σ has form (g_3, g_4), where g_4 is an involution.

7. Hence (g_3, g_4) is an involution and by conjugation we can construct the involution σ with a -1-eigenspace of dimension 4.

The remaining steps of the algorithm are identical to those described in `OneOmegaPlus` where $q \equiv 1 \bmod 4$.

If $n = 3$ then the non-central involutions in $\Omega^-(6, q)$ have centralisers containing $\Omega^+(4, q) \times \Omega^-(2, q)$. Algorithms for this case and for $\Omega^-(4, q)$ are presented in Section 8.

6.3 Groups preserving forms of 0 type

6.3.1 $\Omega(2n + 1, q)$ when $q \equiv 1 \bmod 4$

In summary, we construct an involution in G whose centraliser contains $\Omega^+(2n - 2, q) \times \Omega(3, q)$. We then recursively construct standard generators for each. Within the centraliser of an involution of + type, we find the 'glue' element.

An involution is *suitable* if its -1-eigenspace has dimension $2n - 2$ and supports a form of + type.

Algorithm 9: `OneOmegaCircle` $(X, \mathcal{F})$

/* X is a generating set for the orthogonal group G of type 0 defined over a field of odd characteristic and size $q \equiv 1 \bmod 4$. The classical form preserved by G is $\mathcal{F}$. Return the standard generating set Y for G, the SLPs for the elements of Y and the change-of-basis matrix. */

begin
  $d :=$ the rank of the matrices in X;
  if $d = 3$ then return `CircleBaseCase` $(X, \mathcal{F})$;
  Find by random search $g \in G := \langle X \rangle$ of even order such that g powers to a suitable involution h;
  Let E be the eigenspace of h of dimension $2n-2$ and let F be the eigenspace of i having dimension 3;
  Find generators for the centraliser C of h in G;
  Rewrite with respect to the concatenation of hyperbolic bases for E and F;
  In C find generating sets X_1 and X_2 for $\Omega^+(E)$ and $\Omega^0(F)$;
  $((s_1, t_1, \delta_1, u_1, v_1, s_1', t_1', \delta_1'), B_1) :=$ `OneOmegaPlus` $(X_1, \mathcal{F}|_E)$;
  $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ `OneOmegaCircle` $(X_2, \mathcal{F}|_F)$;
  Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{d/2}, f_{d/2})$ be the concatenation of the hyperbolic bases defined by B_1 and B_2;
  $n := (q-1)/4$;
  $a := ((\delta_1 \delta_1')^n)^{v_1^{-1}} \delta_2^n$;
  Find generators for the centraliser D of a in G;
  In D find a generating set X_3 for $\Omega^+(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$;
  In $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
  $v := bv_1$;
  return $(s_1, t_1, \delta_1, u_1, v)$ and the change-of-basis matrix for B;
end

6.3.2 $\mathrm{SO}(2n+1, q)$

The algorithm for this case is independent of the value of $q \bmod 4$. The definition of a suitable involution is as in Section 6.3.1. The centraliser in $\mathrm{SO}(2n+1, q)$ of a suitable involution contains the direct product of $\mathrm{SO}^+(E)$ and $\mathrm{SO}^-(F)$. We construct each group as a subgroup of the centraliser, and proceed recursively. The resulting algorithm, `OneSpecialCircle`, differs in one respect only from `OneOmegaCircle`: the calls are to `OneSpecialPlus` and `OneSpecialCircle`, and and so construct the additional standard generator σ needed to generate $\mathrm{SO}(2n+1, q)$.

6.3.3 $\Omega(2n+1, q)$ when $q \equiv 3 \bmod 4$

In summary, we construct an involution in $\Omega(2n+1, q)$ whose centraliser contains a direct product of $\Omega^+(2n-2k, q)$ and $\Omega(2k+1, q)$, where $k = 1$ or $k = 2$ according to

the parity of n. We then recursively construct standard generators for each. Within the centraliser of an involution of + type, we find the 'glue' element.

- If $n > 2$ is odd, then an involution i is *suitable* if it has a -1-eigenspace E_- of dimension $2n-2$ which supports a form of + type.
- If $n > 2$ is even, then an involution i is *suitable* if it has a -1-eigenspace E_- of dimension $2n-4$ which supports a form of + type.

Our algorithm, `OneOmegaCircle3`, is similar to `OneOmegaPlus3` and applies when $n > 2$. We construct the subgroup $H := \mathrm{SO}(E_+) \times_{C_2} \mathrm{SO}^+(E_-)$ of the centraliser of i, and call `OneSpecialPlus` and `OneSpecialCircle` to construct the involution whose centraliser contains the 'glue' element.

Algorithms for the remaining cases – $\Omega(3,q)$ and $\Omega(5,q)$ – are presented in Section 8.

7 Algorithm `Two` for orthogonal groups

Consider first $G = \Omega^+(d,q)$. If $q \equiv 1 \bmod 4$, then Algorithm `Two` is essentially the same as that presented for non-orthogonal groups. If $q \equiv 3 \bmod 4$, then the -1 eigenspace of an involution in G has dimension a multiple of 4 if it supports a form of + type. Hence if d is a multiple of 8 we find an involution whose eigenspaces are of equal dimension, and which support forms of + type, and proceed as in the case of non-orthogonal groups. If $d \equiv e \bmod 8$, where $e \in \{2,4,6\}$, and $d > 8$, we find an involution with one eigenspace of dimension e and one of dimension $d-e$, construct generating sets for $\Omega^+(e,q)$ and $\Omega^+(d-e,q)$ in the familiar style, apply Algorithm `One` to the former, and Algorithm `Two` to the latter, and glue.

For $\epsilon \in \{-1,0\}$, we process $\Omega^\epsilon(d,q)$ as in Algorithm `One`, but apply Algorithm `Two`, rather than Algorithm `One`, in the call that processes a copy of $\Omega^+(d-e,q)$.

8 Base cases for orthogonal groups

8.1 Groups preserving forms of + type

Both $\Omega^+(2,q)$ and $\mathrm{SO}^+(2,q)$ are cyclic of order dividing $q-1$. Hence the cost of their constructive recognition is the cost of a call to a discrete log oracle for $\mathrm{GF}(q)$.

The remaining base cases occur for $n = 2$. As we observed in Lemma 3.3, $\Omega^+(4,q)$ is the central product of two copies of $\mathrm{SL}(2,q)$ arising from a tensor decomposition of the underlying space.

This tensor decomposition is readily made explicit: by random selection, we construct an element of $\Omega^+(4,q)$ which acts as a scalar on one of the factors and, using the algorithm of [24, §4], construct the tensor factors. Subject to a discrete logarithm oracle for $\mathrm{GF}(q)$, we now use the algorithm of [12] to recognise constructively the copies of $\mathrm{SL}(2,q)$.

Lemma 8.1 *Statement about the cost here.*

Similar comments apply to $\mathrm{SO}^+(4,q)$ which has structure $C_2.(\mathrm{PSL}(2,q)\times\mathrm{PSL}(2,q)).C_2$.

8.2 Groups preserving forms of $-$ type

As we observed in Lemma 3.4, $\Omega^-(4,q) \cong \mathrm{PSL}(2,q^2)$. Subject to a discrete logarithm oracle for $\mathrm{GF}(q^2)$, we use the algorithm of [12] to recognise constructively this group, Similar comments apply to $\mathrm{SO}^+(4,q) \cong C_2 \times \mathrm{PSL}(2,q^2)$.

We must also consider $G = \Omega^-(6,q)$ where $q \equiv 3 \bmod 4$. The centraliser of a non-central involution in G contains $\Omega^+(4,q) \times \Omega^-(2,q)$ and so `OneOmegaMinus3` does not apply. Instead, we outline a new algorithm to obtain standard generators for $\Omega^-(6,q)$, assuming that $q > 3$. Recall that V denotes the underlying 6-dimensional space.

1. Find, by random search, an element of G that powers up to an an involution, with an eigenspace E of dimension 4 supporting a form of $+$ type and an eigenspace F of dimension 2 supporting a form of $-$ type.

2. Construct a generating set for $\Omega(F)$.

3. Now find, by random search, $h \in G$ such that $T = E \cap E^h$ is of dimension 2, and supports a form of $+$ type.

4. The centraliser of T in G contains $\Omega(F)$ and $\Omega(F^h)$. With high probability, the union of these two cyclic groups generates the centraliser $H := \Omega^-(4,q)$ of T in G. Decide this using the 'naming' algorithm of [26]. If not, repeat steps 3 and 4 until it is true.

5. Construct a hyperbolic basis (e_2, f_2, x, y) for the orthogonal complement $T^\perp$ of T.

6. Now construct standard generators for H. One of the standard generators for H is δ, and $\delta^{(q^2-1)/4}$ is the involution whose $+1$ and -1 eigenspaces, restricted to $T^\perp$, are $\langle e_2, f_2\rangle$ and $\langle x, y\rangle$.

7. Allowing this involution to act on the whole of V, the -1-eigenspace is unchanged; and in the centraliser of this involution we find a copy of $K = \Omega^+(4,q)$.

8. Construct a hyperbolic basis (e_1, f_1) for T, so that $(e_1, f_1, e_2, f_2, x, y)$ is a hyperbolic basis for V. Rewrite the standard generators of H with respect to this basis. All but one of the standard generators of G now appear among the standard generators of H.

9. The remaining standard generator for G is $(e_1, e_2)^-(f_1, f_2)^-$ and lies in K. We now construct this generator as an SLP in the generators of $K = \Omega^+(4,q)$.

Observe that if $q = 3$ then $\Omega(F)$ is of order 2, and this method fails. Instead we use permutation group techniques to construct standard generators for $\Omega^-(6,3)$.

The description of this algorithm conceals a subtle trap. When we find standard generators for an orthogonal group $G = \Omega(V)$ the input consists of a generating set for G, and the form that is preserved is not specified. The form is determined up to a non-zero scalar multiple, and a choice of form is made implicitly by the choice of standard generators. It is of course easy, given standard generators with respect to a given form, to write down standard generators with respect to any non-zero scalar multiple of this form. In the above algorithm standard generators are constructed for $\Omega(E)$ and for $\Omega(\langle e_2, f_2, x, y\rangle)$, and these standard generators must be chosen with respect to the restriction to these spaces of the same form on V.

The analysis of this algorithm is elementary.

Lemma 8.2 *Some statement about cost of the O^-6 algorithm.*

PROOF: To compute the probability that $E \cap E^h$ is of dimension 2, and supports a form of + type, we count the number of pairs of subspaces of dimension 4 that support a form of + type, and count the number of pairs that in addition intersect in a space of + type. This gives a probability that converges rapidly to 1/2. To estimate the probability that the union of $\Omega(F)$ and $\Omega(F^h)$ generates H, we compute the probability that these subgroups lie in a maximal subgroup. For example, the probability that they both lie in a copy of $\mathrm{PSL}(2,q)$ is $O(1/q)$, and one sees easily that the probability of failure is $O(1/q)$. □

8.3 Groups preserving forms of 0 type

As we observed in Lemma 3.5, $\Omega(3,q) \cong \mathrm{PSL}(2,q)$. Subject to a discrete logarithm oracle for $\mathrm{GF}(q)$, we use the algorithm of [12] to recognise constructively this group. Similar comments apply to $\mathrm{SO}(3,q)$.

We must also consider $G = \Omega(5,q)$ where $q \equiv 3 \bmod 4$. The centraliser of a non-central involution in G contains $\Omega^-(2,q)$ and so `OneOmegaCircle3` does not apply. Instead, we outline a new algorithm to obtain standard generators for $\Omega(5,q)$, assuming that $q > 3$.

1. Find, by random search, an element of G that powers up to an involution whose -1-eigenspace E has dimension 4 and supports a form of + type.

2. Find, by random search, an element h of G such that $T = E \cap E^h$ has dimension 3 and supports a non-degenerate form, and $T^\perp$ supports a form of + type.

3. Construct standard generators for the centraliser $\Omega(E)$ of $E^\perp$, and hence for the centraliser $\Omega(E^h)$ of $(E^\perp)^h$.

4. Construct a hyperbolic basis (e_2, f_2, x) of T, and find the standard generators for the centraliser $\Omega(T)$ of $T^\perp$ with respect to this basis as SLPs in the given generators of G by using explicit membership testing in $\Omega(E)$.

5. Observe that the centraliser K in $\Omega(E)$ of x acts as $\Omega(3, q)$ on the orthogonal complement of $\langle x \rangle$ in E. Since we have found standard generators for $\Omega(E)$, we can now construct standard generators for K as SLPs in these standard generators.

6. In the same way we construct generators for the centraliser L of x in $\Omega(E^h)$.

7. Construct a hyperbolic basis (e_1, f_1) for the orthogonal complement of T in V.

8. The union of K and L generates the centraliser M of x in G, which acts as $\Omega^+(4, q)$ on the orthogonal complement of x.

9. Construct standard generators for $M = \Omega^+(4, q)$, and so obtain $v = (e_1, e_2)^-(f_1, f_2)^-$ as an SLP in the generators of M.

10. The standard generators of G with respect to the basis (e_1, f_1, e_2, f_2, x) are the standard generators for $\Omega(T)$, together with v.

Lemma 8.3 *Some statement about cost of the O^5 algorithm.*

We can easily find standard generators for $\Omega(5, 3)$, for example, by considering it as a permutation group acting on the set of isotropic vectors.

9 Finding strong involutions

In the first step of our main algorithms, as outlined in Sections 4–7, by random search, we obtain an element of even order that powers to a strong or suitable involution. We now estimate the proportion of such elements in $\mathrm{SX}(d, q)$.

9.1 The special linear case

We commence our analysis with $\mathrm{SL}(d, q)$. We first estimate the proportion of elements of $\mathrm{GL}(d, q)$ that power to an involution having an eigenspace of dimension within a certain range, and then derive similar results for $\mathrm{SL}(d, q)$.

Lemma 9.1 *The number of irreducible monic polynomials of degree $e > 1$ with coefficients in $\mathrm{GF}(q)$ is k where $(q^e - 1)/e > k \geq q^e(1 - q^{-1})/e$.*

Proof: We use the inclusion-exclusion principle to count the number of elements of $\mathrm{GF}(q^e)$ that do not lie in any maximal subfield containing $\mathrm{GF}(q)$, and divide this number by e, since every irreducible monic polynomial of degree e over $\mathrm{GF}(q)$ corresponds to exactly e such elements. Thus

$$k = \frac{q^e - \sum_i q^{e/p_i} + \sum_{i<j} q^{e/p_i p_j} - \cdots}{e}$$

where $p_1 < p_2 < \cdots$ are the distinct prime divisors of e. The inequality $(q^e-1)/e > k$ is obvious. If e is a prime, then $k = (q^e-q)/e \geq q^e(1-1/q)/e$, with equality if $e = 2$. Now suppose that e is composite, and set $\ell = p_1$. Then from the above formula

$$ek \geq q^e - q^{e/\ell} - q^{(e/\ell)-1} - \ldots - 1 > q^e - q^{e-1}.$$

The result follows. □

Lemma 9.2 *The number of irreducible monic polynomials of degree $e > 1$ with coefficients in* $\mathrm{GF}(q)$*, and specified non-zero constant term $a \in \mathrm{GF}(q)^\times$, is $k(a)$, where $(q^e-1)/e > (q-1)k(a) \geq q^e(1-q^{-1})/e$.*

Proof: Suppose first that $e = 2$. Then $2k(a)$ is the number of elements of $\mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ of norm a. The number of elements of $\mathrm{GF}(q^2)$ of norm a is $q+1$, and either 2 or 0 of these lie in $\mathrm{GF}(q)$, depending on whether or not a is a square in $\mathrm{GF}(q)$. It follows that $k(a) = (q \pm 1)/2$

Now suppose that $e > 2$. If e is prime the number of elements of $\mathrm{GF}(q^e)$ of norm a is $(q^e-1)/(q-1)$, and the number of elements of $\mathrm{GF}(q)$ of norm a lies between 0 and $q-1$. It follows easily that $k(a)$ lies between the given bounds. If e is composite then, with the notation of Lemma 9.1, we find $ek(a) > (q^e-1)/(q-1) - \sum_i q^{e/p_i} + \sum_{i<j} q^{e/p_ip_j} - \cdots$. Here we have taken the number of elements of $\mathrm{GF}(q^e)$ of norm a, and have subtracted the number of elements in the proper subfields of $\mathrm{GF}(q^e)$ containing $\mathrm{GF}(q)$, regardless of their norm. Since $(q^e-1)/(q-1) = q^{e-1}+q^{e-2}+\cdots+1$, it follows that $ek(a) \geq q^{e-1}$, which is the required lower bound. The upper bound is now obvious. □

Lemma 9.3 *Let $d \geq e > d/2$ for $d \geq 4$. The proportion of elements of* $\mathrm{GL}(d,q)$ *whose characteristic polynomial has an irreducible factor of degree e lies between $(1/e)(1-1/q)$ and $1/e$.*

Proof: Let the characteristic polynomial of $g \in \mathrm{GL}(d,q)$ have an irreducible factor $h(x)$ of degree e. Then $\{w \in V : w.h(g) = 0\}$ is a subspace of V of dimension e. It follows that the number of elements of $\mathrm{GL}(d,q)$ of the required type is $k_1k_2k_3k_4k_5$ where k_1 is the number of subspaces of V of dimension e, k_2 is the number of irreducible monic polynomials of degree e over $\mathrm{GF}(q)$, k_3 is the number of elements of $\mathrm{GL}(e,q)$ that have a given irreducible characteristic polynomial, k_4 is the order of $\mathrm{GL}(d-e,q)$, and k_5 is the number of complements in V to a subspace of dimension e. In more detail,

$$\begin{aligned}
k_1 &= \frac{(q^d-1)(q^d-q)\cdots(q^d-q^{e-1})}{(q^e-1)(q^e-q)\cdots(q^e-q^{e-1})} \\
k_3 &= (q^e-q)(q^e-q^2)\cdots(q^e-q^{e-1}) \\
k_4 &= (q^{d-e}-1)(q^{d-e}-q)\cdots(q^{d-e}-q^{d-e-1}) \\
k_5 &= q^{e(d-e)}.
\end{aligned}$$

The formula for k_3 arises by taking the index in $\mathrm{GL}(e,q)$ of the centraliser of an irreducible element, this centraliser being cyclic of order q^e-1. The formula for k_2 is given in Lemma 9.1. Hence $k_1k_2k_3k_4k_5 = |\mathrm{GL}(d,q)| \times k_2/(q^e-1)$. The result follows. □

Lemma 9.4 *Let $e \in (d/3, d/2]$ and $d \geq 4$. Then the proportion of elements of $\mathrm{GL}(d,q)$ that have a characteristic polynomial with exactly one irreducible factor of degree e lies in the interval $[(e^{-1}-e^{-2})(1-1/q), (e^{-1}-e^{-2})+e^{-2}/q]$.*

PROOF: This proportion may be estimated as in the proof of Lemma 9.3, but k_4 must be replaced by the number of elements of $\mathrm{GL}(d-e,q)$ whose characteristic polynomial does not have an irreducible factor of degree e. Thus the proportion required is $(1/e)(1-c_1/q) - (1/e^2)(1-c_1/q)(1-c_2/q)$, where c_1 and c_2 lie in the interval $[0,1]$. Clearly this formula takes its minimum value, for c_1 and c_2 in the given range, when $c_1 = 1$ and $c_2 = 0$, and takes its maximum value when $c_1 = 0$ and $c_2 = 1$. Thus the proportion lies within the range stated. □

We now show that the results of these lemmas hold if $\mathrm{GL}(d,q)$ is replaced by $\mathrm{SL}(d,q)$.

Lemma 9.5 *The results of Lemmas 9.3 and 9.4 hold if $\mathrm{GL}(d,q)$ is replaced by $\mathrm{SL}(d,q)$.*

PROOF: We first prove that the proportion quoted in Lemma 9.3 is also true for $\mathrm{SL}(d,q)$. If $e < d$ the number of elements of $\mathrm{GL}(d,q)$ of the required type may be obtained by replacing k_4 with the number of elements of $\mathrm{GL}(d-e,q)$ of a specified determinant. But the number of such elements is exactly the number of elements of $\mathrm{GL}(d-e,q)$ divided by $q-1$; so the result follows. If $d = e$ this argument fails, and the proportions in the cases $\mathrm{GL}(d,q)$ and $\mathrm{SL}(d,q)$ are not identical. In this case we replace k_2 by $k(1)$ as in Lemma 9.2. By that lemma, the proportions still lie within the given bounds. The case of Lemma 9.4 can be dealt with in the same way. □

We now obtain a lower bound for the proportion of $g \in \mathrm{SL}(d,q)$ such that g has even order $2n$, and g^n has an eigenspace with dimension in a given range. To perform this calculation, we consider the cyclic groups C_{q^e-1} of order q^e-1. If n is an integer, we write $v_2(n)$ for the largest power of 2 that divides n.

Lemma 9.6 *If $v_2(m) = v_2(n)$ then $v_2(q^m-1) = v_2(q^n-1)$.*

PROOF: It suffices to consider the case where $m = kn$, and k is odd. Then $(q^m-1)/(q^n-1)$ is the sum of k powers of q^n, and so is odd. □

Lemma 9.7 *If $u < v$ then $v_2(q^{2^u}-1) < v_2(q^{2^v}-1)$, and if $u > 0$ then $v_2(q^{2^u}-1) = v_2(q^{2^{u+1}}-1) - 1$.*

PROOF: Observe that $(q^{2^{u+1}}-1)/(q^{2^u}-1) = q^{2^u}+1$ which is even. Now $v_2(q^{2^u}-1) > 1$ if $u > 0$. It then follows that $v_2(q^{2^u}+1) = 1$. □

Theorem 9.8 *Let $d \geq 4$. Then the proportion of elements of $\mathrm{SL}(d,q)$ that power to an involution whose -1 eigenspace lies in the range $(d/3, 2d/3]$ is greater than*

$$\left(\frac{1}{2d}\right)\left(1-\frac{1}{q}\right).$$

PROOF: Let 2^k be the unique power of 2 in the range $(d/3, 2d/3]$. If the characteristic polynomial of $g \in \mathrm{SL}(d,q)$ has a unique irreducible factor of degree 2^k, and the order of the restriction of g to the corresponding block of dimension 2^k has order a multiple of $v_2(q^{2^k}-1)$, then by the previous two lemmas g will power to an involution whose -1-eigenspace has dimension 2^k.

We prove the theorem by estimating the proportion of elements of $\mathrm{SL}(d,q)$ of this type. By Lemma 9.5 the proportion of elements of $\mathrm{SL}(d,q)$ whose characteristic polynomials have exactly one irreducible factor of degree $e = 2^k$ is at least $e^{-1}(1-q^{-1})$ if $e > d/2$, and is at least $(e^{-1}-e^{-2})(1-q^{-1})$ if $d/2 \geq e > d/3$. Thus the proportion is at least $d^{-1}(1-q^{-1})$. Suppose now that the characteristic polynomial of g does have exactly one irreducible factor of degree 2^k. Set $x = v_2(q^{2^k}-1)$. We now prove that the probability that the order of g is a multiple of 2^x is greater than $1/2$.

The action of g on the g-invariant block W of dimension 2^k can be used to map g into $T = \mathrm{GF}(q^{2^k}) \setminus U$ where U is the union of all proper subfields of $\mathrm{GF}(q^{2^k})$ that contain $\mathrm{GF}(q)$ by mapping g to a zero of the characteristic polynomial of g restricted to W. This mapping is not unique. The Galois group of $\mathrm{GF}(q^{2^k})$ over $\mathrm{GF}(q)$ acts regularly on T, and the image of g is determined up to the action of this Galois group. Since we have no need to distinguish between elements of the same orbit of this Galois group on T, we may assume that the image of g is uniformly distributed in T. But exactly half the elements of $\mathrm{GF}(q^{2^k})^\times$ have order a multiple of 2^x, and none of the elements of U has order a multiple of 2^x. Thus over half of the elements of T have order a multiple of 2^x. The result follows. □

Lemma 9.9 *Given $g \in \mathrm{GL}(d,q)$ one can determine whether or not g is of even order, and in the positive case determine the dimension of the -1-eigenspace of the power g that is an involution, with $O(d^3 \log q)$ field operations.*

PROOF: In Las Vegas $O(d^3)$ field operations the characteristic polynomial $f(t)$ of g can be computed (see [18, Section X]) and in Las Vegas $O(d^2 \log q)$ field operations it can be factorised as $f(t) = \prod_{i=1}^m f_i(t)^{n_i}$, where the $f_i(t)$ are distinct monic irreducible polynomials (see [36, Theorem 14.14]). If the 2-part of the order of $t + (f_i(t))$ in the group of units of the field $\mathrm{GF}(q)[t]/(f_i(t))$ is 2^{x_i}, if $x = \max_i(x_i)$, and if $I = \{i : x_i = x\}$, then, provided that $x > 0$, the required dimension is $\sum_{i \in I} n_i d_i$, where d_i is the degree

of $f_i(t)$. To compute x_i raise $t + (f_i(t))$ to the power a_i, where a_i is the odd part of $q^i - 1$, and then x_i is the number of times that the resulting field element needs to be squared to give rise to the identity. Since computing t^n in any ring, given t, requires at most $2\log_2(n)$ ring operations, all these steps may be carried out in $O(d^3 \log q)$ field operations. □

Corollary 9.10 *There is a Las Vegas algorithm that takes as input a generating set X for $\mathrm{SL}(d, q)$, where $d \geq 4$, and returns an element g of $\mathrm{SL}(d, q)$ as a straight line program on X, where g is of even order, and powers to an involution whose -1-eigenspace lies in the range $(d/3, 2d/3]$, with Las Vegas complexity $O(d(\xi + d^3 \log q))$ field operations.*

PROOF: This follows at once from the previous two results. □

9.2 The symplectic and orthogonal groups

If $h(x) \in \mathrm{GF}(q)[x]$ is a monic polynomial with non-zero constant term, let $\tilde{h}(x) \in \mathrm{GF}(q)[x]$ be the monic polynomial whose zeros in the algebraic closure of $\mathrm{GF}(q)$ are the inverses of the zeros of $h(x)$. Hence the multiplicity of a zero of $h(x)$ is the multiplicity of its inverse in $\tilde{h}(x)$, and $h(x)\tilde{h}(x)$ is a symmetric polynomial. We call $\tilde{h}$ the *reverse* of h.

Lemma 9.11 *Let $g \in \mathrm{SL}(2n, q)$ have characteristic polynomial $f(x) = h(x)\tilde{h}(x)$, where $h(x) \neq \tilde{h}(x)$ is monic and irreducible. Let c be the constant term of $h(x)$. Then g preserves a non-degenerate symmetric bilinear form on the underlying space, and every such form is of $+$ type. As an element of the corresponding orthogonal group, g has spinor norm $c \bmod \mathrm{GF}(q)^2$.*

PROOF: Clearly g preserves a non-degenerate symmetric bilinear form, since $\tilde{f} = f$. Choose one such form. The null spaces of $h(g)$ and $\tilde{h}(g)$ are orthogonal complements, and the form restricted to each of these is the null form, as $h(x) \neq \tilde{h}(x)$, so the form is of $+$ type.

Following the Zassenhaus definition [37, p. 444], we compute the spinor norm of g as as the product of two terms in $\mathrm{GF}(q)^\times/\mathrm{GF}(q)^2$. The first is the discriminant of the quadratic form restricted to the maximum subspace U of V on which $g + 1$ acts nilpotently. Since -1 is not an eigenvalue of g, this term vanishes. The second term is $\det((1+g)/2)$ restricted to the orthogonal complement of U, modulo $\mathrm{GF}(q)^2$; but here $U = 0$. Since the dimension is even, the factor of $1/2$ does not make any contribution. Let a be a zero of $h(x)$ in $\mathrm{GF}(q^n)$, so $1/a$ is a zero of $\tilde{h}(x)$. Let N denote the norm map from $\mathrm{GF}(q^n)$ to $\mathrm{GF}(q)$. Then the second term is

$$N(1+a)N(1+a^{-1})\mathrm{GF}(q)^2 = N(1+a)^2N(a^{-1})\mathrm{GF}(q)^2 = N(a)\mathrm{GF}(q)^2 = c\mathrm{GF}(q)^2.$$

The result follows. □

Corollary 9.12 *The proportion of elements of $\Omega^+(2n,q)$ whose characteristic polynomial is the product of two distinct irreducible polynomials, each the reverse of the other, is the same as the proportion of such elements in $\mathrm{SO}^+(2n,q)$, up to a factor of the form $1+O(1/q)$.*

PROOF: By the previous result, the two proportions in question are determined by the proportion of elements a of $\mathrm{GF}(q^n)$ that do not lie in $\mathrm{GF}(q^r)$ for any proper factor r of n, and for which $N(a)$ is or is not required to be a square. The proportion of elements of $\mathrm{GF}(q^n)^\times$ whose norms are squares in $\mathrm{GF}(q)$ is precisely $1/2$, and the proportion of elements that lie in a proper subfield containing $\mathrm{GF}(q)$ is $O(1/q)$. The result follows, since $\Omega^+(2n,q)$ has index 2 in $\mathrm{SO}^+(2n,q)$. □

The following is an analogue of Lemma 9.3.

Lemma 9.13 *Let G be one of the groups $\mathrm{Sp}(2n,q)$, $\mathrm{SO}^+(2n,q)$, $\mathrm{SO}^-(2n,q)$. Let $n \geq m > n/2$ where $n \geq 2$, and $n > m$ if $G = \mathrm{SO}^-(2n,q)$. The proportion of elements of G whose characteristic polynomial has an irreducible factor of degree m that is not equal to its reverse lies in the interval*

$$\left(\frac{1-q^{-1}}{2m} - \frac{1}{2q^{\lceil m/2 \rceil}}, \frac{1}{2m}\right),$$

and is strictly positive.

PROOF: Let $g \in G$ act on the natural module V, and let $h(x)$ be an irreducible factor of degree m of the characteristic polynomial $f(x)$ of g not equal to its reverse. Let V_0 be the kernel of $h(g)$. Since $h(x) \neq \tilde{h}(x)$, and g acts irreducibly on V_0, it follows that V_0 is totally isotropic. Also $\tilde{h}(x)$ is a factor of $f(x)$ since $f(x) = \tilde{f}(x)$, and if V_1 is the kernel of $\tilde{h}(x)$ then V_1 is totally isotropic. Since $h(x)$ and $\tilde{h}(x)$ divide $f(x)$ with multiplicity 1, V_0 and V_1 are uniquely determined, and the form restricted to $V_2 = V_0 \oplus V_1$ is non-degenerate.

Thus the number of possibilities for g is the product $\ell_1\ell_2\ell_3\ell_4\ell_5/2$, where ℓ_1 is the number of choices for V_2, and ℓ_2 is the number of choices for V_0 given V_2, and ℓ_3 is the number of irreducible monic polynomials $h(x)$ of degree m over $\mathrm{GF}(q)$ such that $h(x) \neq \tilde{h}(x)$, and ℓ_4 is the number of elements of $\mathrm{GL}(m,q)$ with a given irreducible characteristic polynomial, and ℓ_5 is the order of $\mathrm{GX}(V_2^\perp)$. The factor $1/2$ in the above expression arises from the fact that every such element g is counted twice, because of the symmetry between $h(x)$ and $\tilde{h}(x)$. In more detail

$$\begin{aligned}
\ell_1 &= |\mathrm{GX}(V)|/(|\mathrm{GX}(V_2) \times \mathrm{GX}(V_2^\perp)|) \\
\ell_2 &= |\mathrm{GX}(V_2)|/|\mathrm{GL}(V_0)| \\
\ell_3 &\sim q^m/m
\end{aligned}$$

$$\begin{aligned}\ell_4 &= |\mathrm{GL}(V_0)|/(q^m-1)\\ \ell_5 &= |\mathrm{SX}(V_2^\perp)|.\end{aligned}$$

A more precise estimate for ℓ_3 is given later.

These results are obtained as follows. Witt's Theorem (see Theorem 2.1) implies that $\mathrm{GX}(V)$ acts transitively on the set of subspaces of V that are isometric to V_2, and the normaliser of V_2 in $\mathrm{GX}(V)$ is $\mathrm{GX}(V_2)\times\mathrm{GX}(V_2^\perp)$. Similarly $\mathrm{GX}(V_2)$ acts transitively on the maximal totally isotropic subspaces of V_2, and the normaliser of V_0 in $\mathrm{GX}(V_2)$ is isomorphic to $\mathrm{GL}(V_0)$. Thus ℓ_1 and ℓ_2 are as stated. We observe that ℓ_3 is the number of orbits of the Galois group of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ acting on those $a\in\mathrm{GF}(q^m)$ that do not lie in a proper subfield containing $\mathrm{GF}(q)$, and have the property that the orbit of a does not contain a^{-1}. This last condition is equivalent to the statement that $h(x)\neq\tilde{h}(x)$. Note that $h(x)=\tilde{h}(x)$ if and only if m is even, and $a^{-1}=a^{q^{m/2}}$. The estimate for $k(a)$ in Lemma 9.1 becomes an estimate for ℓ_3 once we subtract (at least from the lower bound) the number of monic irreducible symmetric polynomials of degree m over $\mathrm{GF}(q)$. The number of monic symmetric polynomials of degree m over $\mathrm{GF}(q)$ is $q^{\lfloor m/2\rfloor}$ and at least one of these vanishes at 1, and hence is reducible. Thus $m^{-1}(q^m-1)>\ell_3\geq m^{-1}q^m(1-q^{-1})-q^{\lfloor m/2\rfloor}+1$. The small detail of adding 1 to the lower bound, proved by observing that at least one of these polynomials is reducible, has the effect of ensuring that the stated lower bound is strictly positive in all cases, being the precise value, namely 1, when $q=3$ and $m=2$, the polynomial in question being x^2+x+2. The product of the ℓ_i is $\ell_3|G|/(q^m-1)$ and the result follows. □

Lemma 9.14 *Let G be as in the previous lemma, and let $m\in(n/3,n/2]$. Let S denote the number of elements of G whose characteristic polynomial has exactly two irreducible factors of degree m, say $h(x)$ and $\tilde{h}(x)$, where these are distinct. Then $S=\frac{1}{2}|G|(m^{-1}-\frac{1}{2}m^{-2})(1+c/q)$ where c lies between two absolute constants. In all cases $S>0$.*

Proof: The proof is similar to that of Lemma 9.4. □

Lemma 9.15 *The previous two lemmas also apply when $G=\Omega^\pm(2n,q)$.*

Proof: Again the proof is similar, in the light of Corollary 9.12. □

We now obtain the analogue of Theorem 9.8.

Theorem 9.16 *Let G be one of the groups $\mathrm{Sp}(2n,q)$, $\mathrm{SO}^\pm(2n,q)$, $\mathrm{SO}(2n+1,q)$, $\Omega^\pm(2n,q)$, $\Omega(2n+1,q)$, where $n\geq 2$. Then, for some absolute constant $c>0$, the proportion of $g\in G$ of even order, such that a power of g is an involution z with its -1-eigenspace of dimension in the range $(2n/3,4n/3]$, is at least c/n. In the case of orthogonal groups the same is true if we require the -1-eigenspace of z to support a form of $+$ type, except in the case of $\Omega^{\pm1}(4,q)$ when $q\equiv 3 \bmod 4$.*

PROOF: Given Lemmas 9.13 and 9.14, the proof is essentially the same as that of Theorem 9.8. One significant difference is that the 2-adic value of the order of g will be one less than in the corresponding case of $\mathrm{SL}(d,q)$, since $h(x)$ here has half the degree of the corresponding irreducible polynomial in the case of $\mathrm{SL}(d,q)$. So one has to take into account irreducible factors $k(x)$ of the characteristic polynomial of g for which $k(x) = \tilde{k}(x)$. For example, in $\mathrm{Sp}(3.2^{t-1},q)$ we are looking for an element g of even order whose characteristic polynomial is of the form $h(x)\tilde{h}(x)k(x)$, where $h(x) \neq \tilde{h}(x)$ is irreducible of degree 2^{t-1}. When g is powered up to produce the involution z we want the -1 eigenspace of z to have dimension exactly 2^t. In fact we want this eigenspace to be the space W_1 annihilated by $k(g)$. Suppose then that $k(x)$ is irreducible of degree 2^{t-1}. Thus the zeros of $k(x)$ lie in $\mathrm{GF}(2^{t-1})$, as do the zeros of $h(x)$. We need to prove that the 2-adic value of the order of g restricted to W_1 is likely to be less than the 2-adic value of the order of g restricted to the space $W_2 = W_1^\perp$ annihilated by $h(g)\tilde{h}(g)$. In other words, we need to compare the 2-adic values of the probable multiplicative orders of a zero a of $h(x)$ and of a zero b of $k(x)$ in the algebraic closure of $\mathrm{GF}(q)$. The probability that the 2-adic value of the order of a is $v_2(q^{2^{t-1}}-1)$ is slightly greater than $1/2$. However, since $k(x) = \tilde{k}(x)$ it follows that the order of b divides $q^{2^{t-2}+1}$. Now $v_2(q^{2^{t-2}+1}) = 1$ if $q \equiv 1 \bmod 4$, and $v_2(q^{2^{t-2}+1}) = v_2(q+1) = v_2(q^2-1)-1$ if $q \equiv 3 \bmod 4$. Thus the probability that g powers to an involution whose -1 eigenspace is W_1 is high for large values of n.

A further complication occurs with $\Omega^{\pm 1}(2n,q)$. The -1 eigenspace of the involution z will support a form of $+$ type, the spaces annihilated by $h(g)$ and $\tilde{h}(g)$ being totally isotropic subspaces. Now the condition that g should lie in $\Omega^{\pm 1}(2n,q)$ imposes a restriction on the spinor norm of the restriction of g to W_1 and to $W_2 = W_1^\perp$, the product of these spinor norms being prescribed. By the Zassenhaus formula [37, p. 444] for the spinor norm of g restricted to W_1, we see that this is $\det(\frac{1}{2}(1+g|^{W_1})) \bmod \mathrm{GF}(q)^2$. Since W_1 is of even dimension the factor $1/2$ may be dropped. If $\{\alpha_i : i \in I\}$ are the zeros of $h(x)$ in the algebraic closure of $\mathrm{GF}(q)$, then $\{\alpha_i : i \in I\} \cup \{\alpha_i^{-1} : i \in I\}$ is the set of zeros of $h(x)\tilde{h}(x)$, so the spinor norm of $g|_{W_1}$ is

$$\prod_{i\in I}(1+\alpha_i)(1+\alpha_i^{-1}) = \prod_{i\in I}(1+\alpha_i)^2\alpha_i^{-1}.$$

But clearly $\prod_{i\in I}(1+\alpha_i) \in \mathrm{GF}(q)$, so the spinor norm of g is $\prod_{i\in I}\alpha_i \bmod \mathrm{GF}(q)^2 = \det(h(g) \bmod \mathrm{GF}(q)^2$. Thus the determinant of $h(g)$ is constrained to be a square, or (more probably) to be a non-square, given the action of g on W_2.

Clearly this does not cause problems for large values of n, but there are problems with $n = 2$. In this case we are trying to construct an involution z whose -1-eigenspace has dimension 2 and that supports a form of $+$ type. But if $q \equiv 3 \bmod 4$ then no such element exists in $\Omega^{\pm 1}(4,q)$. In this case we need to find an involution whose -1 eigenspace is of dimension 2, and hence supports a form of $-$ type. Such an involution may be obtained in $\Omega^+(4,q)$ by finding an element g whose characteristic polynomial is the product of two polynomials of degree 2, each equal to its reverse, and where the orders of the restrictions of g to the corresponding g-invariant subspaces have

different 2-adic values. These values must be strictly less than $v_2(q+1)$ for g to lie in $\Omega^+(4,q)$. For $\Omega^-(4,q)$ we may take g to be an element whose characteristic polynomial has a unique irreducible factor of degree 2. The order of the restriction of g to the 2-dimensional irreducible g-invariant module W will then have 2-adic value less than $v_2(q+1)$, and should be greater than the 2-adic value of the order of the restriction of g to $W^\perp$, which is at most one.

The result follows. □

`Theorem 9.17` *`We can construct suitable involutions for the orthogonal groups in time ...`*

9.3 The unitary groups

We finally turn to the unitary groups.

Theorem 9.18 *For some absolute constant $c > 0$, the proportion of $g \in \mathrm{SU}(d,q)$ that have even order, such that a power of g is an involution with its -1-eigenspace of dimension in the range $(d/3, 2d/3]$, is at least c/d.*

Proof: The analysis in this case is almost exactly the same as for the symplectic groups. The only difference comes from the analysis of the restriction of g to W_i where the condition $h(x) = \tilde{h}(x)$ is replaced by the condition that $h(x)$ to be the image of $\tilde{h}(x)$ under the Frobenius map $a \mapsto a^q$. This now requires W_i to have odd dimension $2t+1$, say, and then the order of g will divide $q^{2t+1}+1$. □

In summary, Theorems 9.8, 9.16 and 9.18 provide an estimate of the complexity of finding a strong involution of the type required as $O(d(\xi + d^3 \log q))$ field operations.

10 Involutions with eigenspaces of specified dimension

We now describe and analyse an algorithm to construct an involution in $G \in \mathcal{C}$ with eigenspaces of specified dimension; say with -1-eigenspace of dimension e. We use this algorithm in Algorithm `TwoEven` to construct an involution with eigenspaces of equal dimension.

We outline the algorithm for the case where $G = \mathrm{SL}(d,q)$; the other cases are similar. `However, in its application to orthogonal groups of + type, we also need to specify the type of the restriction of the form to an eigenspace.`

1. Find, by random search, $g \in G$ of even order that powers to a strong involution h_1.

2. Let r and s denote the ranks of the -1- and $+1$-eigenspaces of h_1.

3. If $r = e$ then h_1 is the desired involution.

4. Construct the centraliser in G of h_1. Obtain generators for the special linear group S_- on the -1-space, where S_- acts as the identity on the $+1$-eigenspace of h_1. Similarly obtain generators for the special linear group S_+ on the $+1$-space.

5. Consider the case where $s \leq e < r$. By recursion on d, find an involution in S_- whose -1-eigenspace has dimension e.

6. Consider the case where $e \leq \min(r, s)$. If $r < s$, find an involution in S_- whose -1-eigenspace has dimension e. Similarly, if $s < r$, find in S_+ an involution whose -1-eigenspace has dimension e.

7. Consider the cases where $s \geq e > r$ or $e \geq \max(r, s)$. Find an involution h_2 in S_+ whose -1-eigenspace has dimension $e - r$. Now $h_1 h_2$ is an involution of the required type.

The recursion is founded trivially with the case $d = 4$.

Theorem 10.1 *Using this algorithm, an involution in* $\mathrm{SX}(d, q)$ *or* $\Omega^\epsilon(d, q)$ *can be constructed with* $O(d(\xi + d^3 \log q))$ *field operations that has its* -1*-eigenspace of any even dimension in* $[0, d]$.

PROOF: Theorems 9.8, 9.16 and 9.18 imply that h_1 can be constructed with at most $O(d(\xi + d^3 \log q))$ field operations. We show in Sections 12 and 13 that generators for S_- and S_+ can be constructed in at most $O(d(\xi + d^3 \log q))$ field operations. Thus the above algorithm requires $O(d(\xi + d^3 \log q))$ field operations, plus the number of field operations required in the recursive call. Since the dimension of the matrices in a recursive call is at most $2d/3$, Lemma 2.4 implies that the total complexity is as stated. □

11 Exponentiation

A frequent step in our algorithms is computing the power g^n for some $g \in \mathrm{GL}(d, q)$ and integer n. The value of n may be as large as $O(q^d)$. We could construct g^n with $O(\log(n))$ multiplications using the familiar black-box squaring technique. Instead, we describe the following faster algorithm to perform this task.

1. Construct the Frobenius normal form of g and record the change-of-basis matrix.

2. From the Frobenius normal form, we read off the minimal polynomial $h(x)$ of g, and factorise $h(x)$ as a product of irreducible polynomials.

3. This determines a multiplicative upper bound to the order of g. If $\{f_i(x) : i \in I\}$ is the set of distinct irreducible factors of $h(x)$, and if d_i is the degree of $f_i(x)$, then the order of the semi-simple part of g divides $\prod_i q^{d_i} - 1$, and the order of the unipotent part of g can be read off directly. The product of these two factors gives the required upper bound m.

4. If $n > m$ we replace n by $n \bmod m$. By repeated squaring we calculate $x^n \bmod h(x)$ as a polynomial of degree $k-1$, where k is the degree of $h(x)$.

5. This polynomial is evaluated in g to give g^n.

6. Conjugate g^n by the inverse of the change-of-basis matrix to return to the original basis.

We now consider the complexity of this algorithm.

Lemma 11.1 *Let $g \in \mathrm{GL}(d,q)$ and let $0 \le n < q^d$. Then g^n can be computed using the above algorithm with Las Vegas $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations.*

PROOF: The Frobenius normal form of g, and the corresponding change of basis matrix, can be computed using the algorithm of [14]. It has complexity $O(\mu(d) \log d + dm(d))$, where $\mu(d)$ is the number of field operations required to multiply two $d \times d$ matrices, and $m(d)$ is the number of field operations required to multiply two polynomials of degree d. Since $\mu(d) \le d^3$ and $m(d)$ is $O(d \log d \log\log d)$ (see [36]), in at most Las Vegas $O(d^3 \log d)$ field operations we obtain the minimal polynomial of g.

The minimal polynomial can be factored in Las Vegas $O(d^2 \log q)$ field operations [36, Theorem 14.14]. Calculating $x^n \bmod h(x)$ requires $O(\log(n))$ multiplications in $\mathrm{GF}(q)[x]/(h(x))$, and hence at most $O(d^2 \log d \log\log d \log q)$ field operations [36]. Evaluating the resultant polynomial in g requires $O(d)$ matrix multiplications; but multiplying by g only costs $O(d^2)$ field operations, since g is sparse in Frobenius normal form. Finally, conjugating g by the inverse of the change-of-basis matrix costs a further $O(d^3)$ field operations. □

This algorithm is similar to that of [10] to determine the order of an element of $\mathrm{GL}(d,q)$.

12 Constructing direct factors

We consider the following problem. We are given a subset X of the centraliser of an involution in $\mathrm{GX}(d,q)$, so $X \subset \mathrm{GX}(E) \times \mathrm{GX}(F)$, where E and F are the eigenspaces of the involution. Given that $G := \langle X \rangle$ contains $\Omega\mathrm{X}(E) \times \Omega\mathrm{X}(F)$, find (as SLPs in X) generating sets for $\Omega\mathrm{X}(E)$ and $\Omega\mathrm{X}(F)$.

In summary, we prove the following result.

Theorem 12.1 *There is a Las Vegas algorithm, with complexity $O(d\xi + d^4)$ field operations, that takes as input a subset X of $\mathrm{GX}(E) \times \mathrm{GX}(F)$, where E and F are the eigenspaces of an involution in $\mathrm{GX}(d, q)$, that generates a group containing $\Omega\mathrm{X}(E) \times \Omega\mathrm{X}(F)$, and returns generating sets for $\Omega\mathrm{X}(E)$ and $\Omega\mathrm{X}(F)$ as* SLPs *in X.*

Our proof of this theorem relies heavily on the one-sided Monte Carlo recognition algorithm of Niemeyer & Praeger [26, 28]. We outline briefly this algorithm. The input is a subset Y of a classical group in $\mathrm{GL}(d, q)$, of known type X say. It endeavours to prove that $G := \langle Y \rangle$ contains $\mathrm{SX}(d, q)$, given that G is an irreducible subgroup of $\mathrm{GX}(d, q)$ that does not preserve any bilinear or quadratic form not preserved by $\mathrm{GX}(d, q)$.

In order to decide this, a set S of elements of G is sought with certain properties. For most values of the parameters (X, d, q), the following is the case. The set S consists of two elements. A set P of pairs of primes or squares of primes, each dividing $|\Omega\mathrm{X}(d, q)|$, is defined; and for some pair (ℓ_1, ℓ_2) of elements of P it is required that ℓ_1 should divide the order of one element of S, and ℓ_2 should divide the order of the other. Moreover ℓ_1 and ℓ_2 are prime to $q - 1$. We call parameters (X, d, q) for which this holds *standard*. (These include all generic cases [26] and some of the non-generic cases of [28].)

The set P is chosen so that the proportion of elements of G whose order is a multiple of either element of P is bounded below by a single positive absolute constant; and any irreducible subgroup of the classical group that does not preserve a form that is not preserved by the classical group, but which does contain a set S as above, must contain $\Omega\mathrm{X}(d, q)$. Thus S is a *witness* that G contains $\Omega\mathrm{X}(d, q)$. If the parameters are not standard, then the algorithm requires different types of witness.

Recall that a *primitive prime divisor* of $q^e - 1$ is a prime divisor of $q^e - 1$ that does not divide $q^i - 1$ for any positive integer $i < e$. If r is a primitive prime divisor of $q^e - 1$ then $r \equiv 1 \bmod e$, and so $r \geq e + 1$. The primes and prime powers in elements of P are primitive prime divisors of various types. We are not concerned here with the precise variations used. However, a necessary condition for an element g of $\mathrm{SX}(d, q)$ to have order a multiple of such a prime power is that the characteristic polynomial of g should have an irreducible factor of degree a multiple of k. Moreover $k > d/2$.

To find a witness, the expected number of random elements to be examined is at most $O(\log \log d)$; see [26, Proposition 7.5].

12.1 The standard parameter case

Let us now return to the problem: given $G := \langle X \rangle$ contains $\Omega\mathrm{X}(E) \times \Omega\mathrm{X}(F)$, find (as SLPs in X) generating sets for $\Omega\mathrm{X}(E)$ and $\Omega\mathrm{X}(F)$. We assume that (X, e, q) are standard; in particular, this implies that $e > 2$.

Our algorithm, `GenerateFactor`, is the following.

1. Repeatedly find random elements $gh \in G$, where $g \in \mathrm{GX}(E)$ and $h \in \mathrm{GX}(F)$, until we find two elements $g_1 h_1$ and $g_2 h_2$ such that (g_1, g_2) acts as a witness for

$\Omega\mathrm{X}(E)$, with corresponding prime powers (ℓ_1, ℓ_2), and where the pseudo-order n_i of h_i is prime to ℓ_i for $i = 1, 2$. Let $m_i = n_i(q-1)$.

2. Then $(g_i, h_i)^{m_i} = (g_i^{m_i}, 1)$, and $\langle g_1^{m_1}, g_2^{m_2} \rangle$ generates $\Omega\mathrm{X}(e, q)$, as required.

Lemma 12.2 *The Las Vegas algorithm,* `GenerateFactor`*, constructs a generating pair for* $\Omega\mathrm{X}(E)$ *in* $O(d\xi + d^4)$ *field operations, provided that the parameters* (X, e, q) *are standard.*

Proof: Since the proportion of elements in $\mathrm{GX}(E)$ that are candidates for g_i is bounded away from 0 [26, Proposition 7.5], we need only estimate the proportion of elements h_i of $\mathrm{GX}(F)$ with *pseudo-order* prime to ℓ_i. (For a definition of this concept, see Section 13.)

This will be the case if the characteristic polynomial of h_i does not have an irreducible factor of degree a multiple of $k_i > 1$.

By considering a very restricted choice, we obtain conversative estimates for the proportion of such h_i. Let $p_i(x)$ be the characteristic polynomial of h_i.

- If $\mathrm{X} = \mathrm{SL}$ or $\mathrm{X} = \mathrm{U}$, then we require $p_i(x)$ to be irreducible if f is not a multiple of k_i, and to have an irreducible factor of degree $k_i - 1$ otherwise.

- If $\mathrm{X} = \mathrm{Sp}$ or F supports a non-degenerate orthogonal form of $+$ type and $k_i > 2$ and $f > 2$, then we require $p_i(x)$ to be irreducible if f is not a multiple of k_i, and to have an irreducible factor of degree $k_i - 2$ otherwise.

- If F supports a non-degenerate orthogonal form of $-$ type and $k_i > 2$ and $f > 2$, then we require $p_i(x)$ to have an irreducible factor of degree $f-2$ or $f-4$. Note that if $f = 4$ then $f - 2$ is not a multiple of k_i.

- If F supports a non-degenerate orthogonal form and is of odd dimension and $k_i > 2$, then we take $p_i(x)$ to have an irreducible factor of degree $f-1$ or $f-3$.

In all these cases the proportion of such elements is $1 : O(f)$.

Hence we require at most $O(d)$ random elements of G to find two suitable elements of G. The cost of computing and factorising the characteristic polynomial of $g \in G$ to determine its suitability is $O(d^3)$ field operations (see [18, Section X]). The powering operation, which need only take place in E, is performed twice. □

12.2 The dimension 2 case

We now consider the case where $e = 2$ and $\mathrm{X}(e, q) = \mathrm{SL}(2, q)$, where $q > 3$.

We first show that, with high probability, $\mathrm{SL}(2, q)$ can be generated by an irreducible element and a random conjugate.

Lemma 12.3 *Let $g \in \mathrm{SL}(2,q)$ act irreducibly on the underlying space, and let H be a maximal subgroup of $\mathrm{SL}(2,q)$ containing g. Then H is either a conjugate of $\mathrm{SL}(2,r)$, where q is a proper power of r, or is isomorphic to the dihedral group of order $2(q+1)$, or is isomorphic to one of A_4, S_4 or A_5.*

PROOF: This result can be read off from [23, Hauptsatz 8.27]. □

Corollary 12.4 *The probability that an irreducible element and one random conjugate of this elements will fail to generate $\mathrm{SL}(2,q)$ is at most XXX.*

PROOF: Observe that g lies in a unique dihedral group of order $q+1$, since distinct cyclic subgroups of $\mathrm{SL}(2,q)$ of order $q+1$ intersect trivially. Thus the probability that g and a random conjugate h of g will lie in the same dihedral group is $1:k$, where $k = |\mathrm{SL}(2,q)|/2(q+1) = (q^2-q)/2$. The probability that g will lie in a given copy of $\mathrm{SL}(2,r)$ is then $r^2-r : q^2-q$, and the probability that both g and h will lie in this copy is the square of this. The number of copies of $\mathrm{SL}(2,r)$ in $\mathrm{SL}(2,q)$ is $q(q^2-1)/r(r^2-1)$, so the probability that g and h lie in the same copy of $\mathrm{SL}(2,r)$ is at most $1 : O(q/r)$. If $q = p^e$ and $\{\ell_i : i \in I\}$ is the set of primes dividing e, then $r = p^{e/l_i}$ for some $i \in I$, since $\mathrm{SL}(2,r)$ is a maximal subgroup of $\mathrm{SL}(2,q)$. Thus the probability that g and h both lie in the same copy of $\mathrm{SL}(2,r)$ for some $r < q$ is at most $1 : \sum_{i\in I} q^{-1/\ell_i}$. Since $|I| < \log e$, this probability is at most $1 : q^{-1/2} + O(q^{-1/3}\log\log q)$. Obviously the probability that g and h both lie in the same copy of A_4 or S_4 or A_5 is $1 : O(q^3)$, since $\mathrm{SL}(2,q)$ contains at most two conjugacy classes of any one of these groups. □

This suggests the following algorithm to construct an irreducible element of $\mathrm{SL}(2,q)$.

1. First consider the case where $q \neq 2^s - 1$ for $s \in \mathbb{N}$. Search for $(g,h) \in G$ where:
   - g has no irreducible factor of odd degree;
   - h has irreducible characteristic polynomial, and had order divisible by odd prime $\ell \neq p$ where ℓ divides q^2-1 and does not divide $q-1$.
2. Next consider the case where $q = 2^s - 1$ for $s \in \mathbb{N}$. Search for $(g,h) \in G$ where:
   - g has odd order;
   - h has order divisible by 2^s.

Let k be the pseudo-order of g. We evaluate $(g,h)^k$ to obtain $(1,h^k)$. Observe that $x := h^k$ is an irreducible element of $\mathrm{SL}(2,q)$. Lemma 12.3 implies that, with high probability, x and a random conjugate will generate $\mathrm{SL}(2,q)$.

Lemma 12.5 *There is a Las Vegas algorithm constructs a generating pair for $\Omega\mathrm{X}(E) \equiv \mathrm{SL}(2,q)$ in $O(d\xi + d^4)$ field operations.*

PROOF: As in Lemma 12.2, $g \in \Omega X(E)$ can be constructed, in $O(d\xi + d^4)$ field operations, Now the result now follows from Corollary 12.4: namely, g, together with one random conjugate of g, will generate $\mathrm{SL}(2, q)$. □

12.3 Dimension 4 cases

Two further non-standard sets of parameters are $(\Omega^\epsilon, 4, q)$, for $\epsilon = \pm 1$.

Recall that $\Omega^-(4, q)$ is isomorphic to $\mathrm{SL}(2, q^2)$, and hence is essentially covered by the previous lemma. We need an element $(g, h) \in \mathrm{SO}^-(4, q) \times \mathrm{SO}^\epsilon(d-4, q)$ that powers to an element of $\mathrm{SO}^-(4, q)$ of order not dividing $q^2 - 1$. We are thus looking for an element (g, h) where the order of g is a multiple of an odd prime dividing $q^2 + 1$, and the order of h is not. It is sufficient for the characteristic polynomial of h to have no irreducible factor of degree a multiple of 4.

Recall that $\Omega^+(4, q)$ is the central product of two copies of $\mathrm{SL}(2, q)$. Exactly as in the case of the previous lemma, we can find elements (g, h) where $h \in \Omega^+(4, q)$ and its projection to a given copy of $\mathrm{SL}(2, q)$ acts irreducibly (in dimension 2), and hence proceed as in that lemma. So if $\Omega(E)$ is isomorphic to $\Omega^\epsilon(4, q)$, we construct one or (if $\epsilon = +1$) two suitable elements of $\Omega(E)$ by powering a suitable element of G, found by random selection, and then construct a generating set for $\Omega(E)$ from conjugates of this element, or pair of elements.

Thus we arrive at the following lemma.

Lemma 12.6 *The above Las Vegas algorithm constructs a generating pair for* $\Omega(E) \equiv \Omega^\epsilon(4, q)$ *(where* $q > 3$ *if* $\epsilon = +$*) in* $O(d\xi + d^4)$ *field operations.*

12.4 The other non-standard cases

`EOB -- FOLLOWING NEEDS TO BE MADE MORE PRECISE. SHOULD WE SPECIFY THE EXAMPLES EXPLICITLY?` We are now left with a finite number of possibilities for $\Omega X(E)$, of which $\mathrm{SL}(2, 3)$ and $\Omega^+(4, 3)$ are soluble. Since $\mathrm{SL}(2, 3)$ is generated by the conjugates of any The remaining exceptional cases are listed in [26] and are perfect, being simple modulo scalars. Since the groups do not consist entirely of diagonal elements, we can find a non-diagonalisable element of the group, and generate $\Omega X(E)$ with a given degree of confidence by a uniformly bounded number of random conjugates of this element.

12.5 The strong involution case

Finally we consider the case in which $e \in [d/3, 2d/3]$ and obtain a stronger result when E is an eigenspace of a strong involution. We assume that d is sufficiently large to avoid non-standard parameters. Using `GenerateFactor`, we search for $(g_i, h_i) \in \mathrm{GX}(E) \times \mathrm{GX}(F)$, where $\{g_1, g_2\}$ is be a witness, and the characteristic polynomial of h_i does not have an irreducible factor of degree a multiple of k_i for some k_i. Now $k_i > e/2 \geq d/6$, and as d tends to infinity the probability that the characteristic

polynomial of h_i will have such a factor clearly tends to 0. Thus the number of random elements of G that we need, with a given probability of success, to consider is bounded.

Theorem 12.7 *There is a Las Vegas algorithm, with complexity $O(\xi + d^3)$ field operations, that takes as input a subset X of $\mathrm{GX}(E) \times \mathrm{GX}(F)$, where E and F are the eigenspaces of an involution in $\mathrm{GX}(d, q)$, that generates a group containing $\Omega\mathrm{X}(E) \times \Omega\mathrm{X}(F)$, where the dimension of E is at least $d/3$, and returns a generating set for $\Omega\mathrm{X}(E)$ as* SLPs *in X.*

13 Constructing an involution centraliser

In applying our algorithms to groups in $\mathcal{C}$, we construct involution centralisers. In particular, we must solve the following problems. Let u be an involution in $\mathrm{SX}(d, q)$ and let E_+ and E_- denote the eigenspaces of u.

1. Construct a generating set for a subgroup of the centraliser of u that contains $\mathrm{SX}(E_+) \times \mathrm{SX}(E_-)$.

2. Suppose that the eigenspaces, E_+ and E_- are isometric. Construct the projective centraliser of u. As we observed in Section 2, its preimage in $\mathrm{SX}(d, q)$ contains an element which interchanges the eigenspaces.

If E_+ and E_- have the same dimension they are isometric, except in the case of orthogonal groups of $-$ type.

In our discussion, we focus on $\mathrm{SX}(d, q)$; similar results hold for $\Omega^\epsilon(d, q)$.

Elements of the centraliser of an involution in a black-box group having an order oracle can be constructed using an algorithm of Bray [5]. They are constructed using the following result.

Theorem 13.1 *If u is an involution in a group G, and g is an arbitrary element of G, then $[u, g]$ either has odd order $2k + 1$, in which case $g[u, g]^k$ commutes with u, or has even order $2k$, in which case both $[u, g]^k$ and $[u, g^{-1}]^k$ commute with u.*

That these elements centralise u follows from elementary properties of dihedral groups.

Bray [5] also proves that if g is uniformly distributed among the elements of G for which $[u, g]$ has odd order, then $g[u, g]^k$ is uniformly distributed among the elements of the centraliser of u. If $[u, g]$ has even order, then the elements returned are involutions; but if just one of these is selected, then it is independently and uniformly distributed within that class of involutions.

Parker & Wilson [32] prove the following:

Theorem 13.2 *There is an absolute constant c such that if G is a finite quasisimple classical group, with natural module of dimension d over a field of odd characteristic, and u is an involution in G, then $[u, g]$ has odd order for at least a proportion c/d of the elements g of G.*

Hence, by a random search of length at most $O(d)$, we construct random elements of the centraliser of the involution. Liebeck & Shalev [21] prove that if $H_0 \leq H \leq \mathrm{Aut}(H_0)$, where H_0 is a finite simple group, then the probability that two random elements of G generate a group containing H_0 tends to 1 as $|H_0|$ tends to infinity. A similar result clearly holds for a direct product of two simple groups.

In its black-box application, this algorithm assumes the existence of an order oracle. We do not require such an oracle for a linear group. If a multiplicative upper-bound B for the order of $g \in G$ is available, then we can learn in polynomial time the *exact* power of 2 (or of any specified prime) that divides $|g|$. By repeated division by 2, we write $B = 2^m b$ where b is odd. Now we compute $h = g^b$; since the order of h divides 2^m, we can determine the precise value by repeated squaring. If $g \in \mathrm{GL}(d, q)$, then a multiplicative upper bound of magnitude $O(q^d)$ can be obtained for $|g|$ using the algorithms of [10] and [34] in at most $O(d^3 \log q)$ field operations. We call this upper bound the *pseudo-order* of g. Further, as discussed in [19], the construction of the centraliser of an involution requires only knowledge of the pseudo-order.

In summary, [19, Theorem 7] implies the following.

Theorem 13.3 *The Bray algorithm to construct the centraliser of an involution in* $\mathrm{SX}(d, q)$ *has complexity* $O(d(\xi + d^3 \log q))$ *field operations.*

This algorithm can be readily adapted (using projective rather than linear pseudo-orders) to compute the preimage in $\mathrm{SX}(d, q)$ of the centraliser of an involution in the simple projective image of $\mathrm{SX}(d, q)$.

Once we construct a subgroup of the centraliser containing its derived group, we can apply the algorithms of Section 12 to obtain generators for the derived subgroups of the projections of the centralisers of the two eigenspaces.

We summarise the preceding discussion.

Theorem 13.4 *Let h be an involution in $\langle X \rangle = G$, where $\mathrm{SX}(d, q) \leq G \leq \mathrm{GX}(d, q)$. Assume that the -1-eigenspace of h has dimension e in the range $(d/3, 2d/3]$. Generating sets for the images in $\mathrm{SX}(e, q)$ and $\mathrm{SX}(d - e, q)$ that centralise the eigenspaces can be found in $O(d(\xi + d^3 \log q))$ field operations. If the eigenspaces are isometric, so $e = d/2$ and $d \equiv 0 \bmod 4$, then we can similarly find an element in $\mathrm{SX}(d, q) \wr C_2$ which interchanges the two copies of $\mathrm{SX}(d, q)$.*

14 The base cases for the non-orthogonal groups

We now consider the base cases for Algorithms `One` and `Two` when $G = \mathrm{SX}(d, q)$ is a non-orthogonal group. Recall that, for $d = 2n$, $Y_0 = \{s, t, \delta, u, v\}$ generates $\mathrm{SX}(2, q) \wr C_n$ or $\mathrm{SX}(2, q) \wr S_n$ depending on the type. As the first and major part of each algorithm, we construct Y_0. As a final step, we construct the additional elements x, y. Clearly the elements of Y_0 could be constructed by constructively recognising $\mathrm{SX}(4, q)$; however, both u and v can be obtained by constructively recognising $\mathrm{SX}(2, q) \wr C_2$, a computation practically more efficient than that for $\mathrm{SX}(4, q)$.

Hence we designate the following as base cases: $\mathrm{SX}(2,q)$, $\mathrm{SX}(2,q) \wr C_2$, $\mathrm{SX}(3,q)$ and $\mathrm{SX}(4,q)$. The last two arise *at most once* during an application of Algorithm `One` or `Two`.

In the remainder of this section, we outline the specialised algorithms for the base cases. We first summarise their cost.

Theorem 14.1 *Subject to the availability of a discrete log oracle for* $\mathrm{GF}(q)$*,* SLPs *for standard generators and other elements of* $\mathrm{SX}(d,q)$ *for* $d \leq 4$ *can be constructed in* $O(\xi \log\log q + \log q)$ *field operations.*

14.1 $\mathrm{SX}(2,q)$

The base case encountered most frequently is $\mathrm{SL}(2,q)$ in its natural representation. An algorithm to construct an element of $\mathrm{SL}(2,q)$ as an SLP in an arbitrary generating set is described in [12]. This algorithm requires $O(\log q)$ field operations, and the availability of discrete logarithms in $\mathrm{GF}(q)$.

Observe that $G = \mathrm{SU}(2,q)$ is isomorphic to $\mathrm{SL}(2,q)$. We can write G over $\mathrm{GF}(q)$ by conjugating G by a diagonal matrix $\mathrm{diag}(\alpha, 1)$ where α is an element of trace 0 in $\mathrm{GF}(q^2)$; alternatively we could use the algorithm of [15]; either requires $O(\log q)$ operations.

14.2 $\mathrm{SL}(2,q) \wr C_2$

In executing Algorithms `OneEven` or `OneOdd`, or `TwoTimesFour` or `TwoTwiceOdd`, each pair of recursive calls generates an instance of the following problem.

Problem 14.2 *Let* V *be the natural module of* $G = \mathrm{SX}(4,q)$*, and let* (e_1, f_1, e_2, f_2) *be a hyperbolic basis for* V*. Given a generating set for* X*, and the involution* u*, where* u *maps* e_1 *to* $-e_1$ *and* f_1 *to* $-f_1$*, and centralises the other basis elements, construct the involution* b *of* G *that permutes the basis elements, interchanging* e_1 *with* e_2*, and* f_1 *with* f_2*.*

Consider the procedure `OneEven`. Observe that in line 15 we construct $\mathrm{SX}(4,q)$. Now b is the permutation matrix used in line 16 to "glue" v_1 and v_2 together to form v, the long cycle. We could use the algorithm of Section 14.3 to find b directly in $\mathrm{SX}(4,q)$. Instead, for reasons of practical efficiency, we use the following algorithm to find b inside the projective centraliser of $u \in \mathrm{SX}(4,q)$.

1. Using the Bray algorithm, construct the projective centraliser H of u in $\mathrm{SX}(4,q)$, that contains $\mathrm{SL}(2,q) \wr C_2$.

2. Find $h \in H$ that interchanges the spaces $\langle e_1, f_1 \rangle$ and $\langle e_2, f_2 \rangle$. Observe that bh lies in $\mathrm{SL}(2,q) \times \mathrm{SL}(2,q)$.

3. Using the algorithms described in Section 12, construct the two direct factors and so construct bh and thus b as an SLP.

Observe that we can conjugate, using h, the solution from one copy of $\mathrm{SL}(2,q)$ to the other, thus requiring just one constructive recognition of $\mathrm{SL}(2,q)$. This algorithm is that same as that for $\mathrm{SL}(2,q)$.

14.3 $\mathrm{SX}(3,q)$ and $\mathrm{SX}(4,q)$

We use the involution-centraliser algorithm of [19] to construct standard generators for $\mathrm{SX}(3,q)$, and the additional elements $x, y \in \mathrm{SX}(4,q)$.

We briefly summarise this algorithm. Assume $G = \langle X \rangle$ is a black-box group with order oracle. We are given $g \in G$ to be expressed as an SLP in X. In our description, if we "find" an element g of G, then we mean that we obtain its SLP in X. First find by random search $h \in G$ such that gh has even order 2ℓ, and $z := (gh)^\ell$ is a non-central involution. Now find, by random search and powering, an involution $x \in G$ such that xz has even order $2m$, and $y := (xz)^m$ is a non-central involution. Note that an SLP is known for x, but, at this stage, not for either of y nor z. Observe that x, y and z are non-central involutions. We construct their centralisers using the Bray algorithm. We *assume* that we can solve the explicit membership problem in these centralisers; see below for further discussion of this point. In particular, we find y as an element of the centraliser in G of x, and z as an element of the centraliser in G of y, and gh as an element of the centraliser in G of z. Now that we know an SLP for gh and h, we can write down an SLP for g.

In summary, this algorithm reduces the constructive membership test for G to three constructive membership tests in involution centralisers in G. But this is an imperfect recursion, since the algorithm may not be applicable to these centralisers. We do not rely on the recursion; instead we construct explicitly the desired elements of the centralisers, since their derived groups are (direct products of) $\mathrm{SL}(2,q)$ and we can use the algorithm of [12]. In this context, the complexity of the involution-centraliser algorithm is that stated in Theorem 14.1.

As presented, this is a black-box algorithm requiring an order oracle. If G is a linear group, the algorithm does not require an order oracle, exploiting instead the multiplicative bound for the order of an element which can be obtained in polynomial time as described in Section 13.

Since the practical performance of this algorithm is rather slow for large fields, we organised Algorithms `One` and `Two` to ensure that they each need *at most one application*. If the dimension d of the input group is odd, then we invoke this algorithm once to construct standard generators for $\mathrm{SX}(3,q)$. If d is even, then as a final step, we construct the additional generators x and y using this algorithm. Let $h \in G = \mathrm{SX}(d,q)$ be the involution whose -1-eigenspace is $\langle e_1, f_1, e_2, f_2 \rangle$. Observe that h can be readily constructed as a word in the elements of Y_0, and that both x and y are elements of $C_G(h)$.

15 Complexity of the algorithms

We now analyse the principal algorithms, and in the next section estimate the length of the SLPs that express the canonical generators as words in the given generators. The time analysis is based on counting the number of field operations, the number of random elements, and the number of calls to the discrete logarithm oracle. Use of discrete logarithms in a given field requires first the setting up of certain tables, and these tables are consulted for each application. The time spent in the discrete logarithm algorithm, and the space that it requires, are not proportional to the number of applications in a given field.

Babai [1] presented a Monte Carlo algorithm to construct in polynomial time independent nearly uniformly distributed random elements of a finite group. An alternative is the *product replacement algorithm* of Celler *et al.* [9]. That this is also polynomial time was established by Pak [30]. For a discussion of both algorithms, we refer the reader to [33, pp. 26-30].

We now complete our analysis of the main algorithms.

Theorem 15.1 *The number of field operations carried out in Algorithm* `OneEven` *is* $O(d(\xi + d^3 \log q))$.

PROOF: The proportion of elements of G with the required property in line 6 is at least k/d for some absolute constant k, as proved in Section 9.

The number of field operations required in lines 8 and 14 is $O(d(\xi + d^3 \log q))$, as proved in Section 13.

The recursive calls in lines 10 and 11 are to cases of dimension at most $2d/3$, and hence they increase by only a constant factor the number of field operations.

The number of field operations required in lines 9 and 13 is at most $O(d^3 \log q)$, as proved in Section 12.

The result follows. □

We estimate the number of calls to the $\mathrm{SL}(2, q)$ constructive recognition algorithm and the associated discrete logarithm oracle.

Theorem 15.2 *If* $d > 2$*, then Algorithms* `OneEven` *and* `TwoEven` *generate at most* $2d - 3$ *and* $6 \log d$ *calls to the discrete logarithm oracle for* $\mathrm{GF}(q)$ *respectively.*

PROOF: Each call to the constructive recognition oracle for $\mathrm{SL}(2, q)$ generates three calls to the discrete logarithm oracle for $\mathrm{GF}(q)$ [12]. Each solution to Problem 14.2 requires 3 calls to the discrete logarithm oracle.

Let $f(d)$ be the number of calls to the discrete logarithm oracle generated by applying `OneEven` to $\mathrm{SX}(d, q)$. Then $f(2) = f(4) = 3$ and $f(d) = f(e) + f(d - e) + 3$ for $d > 4$ and some $e \in (d/3, 2d/3]$. It follows that $f(d) \leq 2d - 3$ for $d > 2$.

Let $g(d)$ be the number of calls generated by applying `TwoEven` to $\mathrm{SX}(d, q)$, where d is even. Again $g(2) = g(4) = 3$ and $g(2n) \leq g(n) + 6$ for $n > 2$. Hence $g(d) \leq 6 \log d$. □

Similar results hold for the other algorithms. If we use the involution-centraliser algorithm [19] to construct either standard generators for $\mathrm{SX}(3,q)$, or the additional generators $x, y \in \mathrm{SX}(4,q)$, then the number of calls to the oracle in each case is 9.

16 Straight-line programs

We now consider the length of the SLPs for the standard generators for $\mathrm{SX}(d,q)$ constructed by our algorithms.

In its simplest form, an SLP on a subset X of a group G is a string, each of whose entries is either a pointer to an element of X, or a pointer to a previous entry of the string, or an ordered pair of pointers to not necessarily distinct previous entries. Every entry of the string defines an element of G. An entry that points to an element of X defines that element. An entry that points to a previous entry defines the inverse of the element defined by that entry. An entry that points to two previous entries defines the product, in that order, of the elements defined by those entries.

Such a simple SLP defines an element of G, namely the element defined by the last entry, and it can be obtained by computing in turn the elements for successive entries. The SLP is primarily used by replacing the elements X of G by the elements Y of some group H, where X and Y are in one-to-one correspondence, and then evaluating the element of H that the SLP then defines.

We now identify other desirable features of SLPs.

1. We need to replace the second type of node, that defines the inverse of a previously defined element, by a type of node with two fields, one pointing to a previous entry, and one containing a possibly negative integer. The element defined is then the element defined by the entry to which the former field points, raised to the power defined by the latter field. This reflects the fact that we raise group elements to very large powers, and have an efficient algorithm described in Section 11 for performing this.

2. An SLP may define a number of elements of G, and not just one element, so a sequence of nodes may be specified as giving rise to elements of G. Thus we wish to return a single SLP that defines all of the standard generators of $\mathrm{SX}(d,q)$, rather than an SLP for each generator. This avoids duplication when two or more of the standard generators rely on common calculations.

3. A critical concern is how the number of trials in a random search for a group element affects the length of an SLP that defines that element. Any discussion of this requires consideration of the algorithm used to generate random elements. We make two reasonable assumptions:

   (a) the associated random process is a stochastic process taking place in a graph whose vertices are defined by a *seed*;

(b) a random number generator now determines which edge adjoining the current vertex in the graph will be followed in the stochastic process.

By default, the length of the SLP will then increase by a constant amount for *every trial, successful or unsuccessful*. Should its length reflect only those trials that are successful? One additional assumption which allows us to explore this question is the following: *When embarking on a search that is expected to require d trials, we record the value of the seed, and repeatedly carry out a random search, using our random process, but returning, after every $\ell(d)$ steps, for some function ℓ of d, to the stored value of the seed, until we succeed.* We hypothesise that values for $\ell(d)$ range from $\log d$ to d and now analyse the lengths of the SLPs for the boundary values.

Theorem 16.1 *If the* SLPs *constructed satisfy properties* 1−3 *above, then their lengths are the following.*

$\ell(d)$	`OneMain`	`TwoMain`
$\log d$	$O(d \log d)$	$O(\log^3 d)$
d	$O(d \log d)$	$O(d \log d)$

PROOF: For each hypothesised value of $\ell(d)$, we wish to find functions $f(d)$ and $g(d)$ such that the lengths of the SLPs returned by Algorithms `One` and `Two` are bounded above by these functions respectively.

Let $e \in (d/3, 2d/3]$. Our analysis of Algorithm `One` implies that $f(d) \leq f(e) + f(d-e) + c \cdot \ell(d)$ for some constant $c > 0$.

Consider, for example, the case where $\ell(d) = d$. We wish to prove that $f(d) \leq k \cdot d \log d$ for some positive constant k. Let $k > 3c/(3\log(3) - 2)$, taking all logarithms to base 2. Assume by induction that $f(n) < kn \log(n)$ for all $n < d$ for some $d > 4$. Then

$$f(d) \leq f(e) + f(d-e) + cd < ke \log(e) + k(d-e)\log(d-e) + cd < kd \log(d),$$

as required, since $e \log(e) + (d-e)\log(d-e)$ takes its maximum value, for e in the given range, when $e = 2d/3$. The results are similar if $\ell(d) = \log d$.

Algorithm `Two` recurses either from the case $d = 4n$ to the case $d = 2n$ in one step, or from the case $d = 4n+2$ to the case $d = 4n$ and then to the case $d = 2n$. It is easy to see that the effect on the length of the SLP in the latter situation is dominated by the second step. If d is initially odd, then the contribution of the reduction to the even case, which is carried out once, may also be ignored here. The main contribution to the length of the SLP in passing from $d = 4n$ to $d = 2n$ arises from constructing an involution whose eigenspaces have dimension $2n$. This involution is constructed recursively, where the length of the recursion is $O(\log d)$. Thus the contribution to the length of the SLP in constructing this involution is $O(\log(d)\ell(d))$. Hence, $g(4n) \leq g(2n) + c\log(n)\ell(n)$ and $g(4n+2) \leq g(2n) + c\log(n)\ell(n)$ for some $c > 0$.

If $\ell(d) = O(\log d)$, then the inequality $g(n) \leq g(\lceil n/2 \rceil) + c\log^2(n)$ is satisfied by $g(n) = k\log^3(n)$ for sufficiently large k. Similar calculations can be carried for the other case, yielding the stated results. □

17 An implementation

Our implementation of these algorithms is publicly available in Magma. It uses:

- the product replacement algorithm [9] to generate random elements `also mention Prospector`;
- our implementations of Bray's algorithm [5] and the involution-centraliser algorithm [19].
- our implementations of the algorithm of [12] and [22].

The computations reported in Table 3 were carried out using Magma V2.13 on a Pentium IV 2.8 GHz processor. The input to the algorithm is $\mathrm{SX}(d, q)$. In the column entitled "Time", we list the CPU time in seconds taken to construct the standard generators.

Table 3: Performance of implementation for a sample of groups

Input	Time
$\mathrm{SL}(6, 5^8)$	2.2
$\mathrm{SL}(40, 5^8)$	22.5
$\mathrm{SL}(80, 5^8)$	130.8
$\mathrm{Sp}(10, 5^{10})$	19.5
$\mathrm{Sp}(40, 5^{10})$	280.4
$\mathrm{SU}(8, 3^{16})$	22.6
$\mathrm{SU}(20, 5^{12})$	47.6
$\mathrm{SU}(70, 5^2)$	191.3

References

[1] László Babai, Local expansion of vertex-transitive graphs and random generation in finite groups, *Theory of Computing*, (Los Angeles, 1991), pp. 164–174. Association for Computing Machinery, New York, 1991.

[2] László Babai and Endre Szemerédi. On the complexity of matrix group problems, I. In *Proc. 25th IEEE Sympos. Foundations Comp. Sci.*, pages 229–240, 1984.

[3] László Babai and Robert Beals, A polynomial-time theory of black-box groups. I. In *Groups St. Andrews 1997 in Bath, I*, volume 260 of *London Math. Soc. Lecture Note Ser.*, pages 30–64, Cambridge, 1999. Cambridge Univ. Press.

[4] L. Babai, P. Pálfy and J. Saxl, On the number of p-regular elements in simple groups, preprint.

[5] J.N. Bray, An improved method of finding the centralizer of an involution, *Arch. Math. (Basel)* **74** (2000), 241–245.

[6] Wieb Bosma, John Cannon, and Catherine Playoust, The MAGMA algebra system I: The user language, *J. Symbolic Comput.*, **24**, 235–265, 1997.

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

[8] Roger Carter. Simple groups of Lie Type. Wiley-Interscience, 1989.

[9] Frank Celler, Charles R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer and E.A. O'Brien, Generating random elements of a finite group, *Comm. Algebra*, **23** (1995), 4931–4948.

[10] Frank Celler and C.R. Leedham-Green, Calculating the order of an invertible matrix, In *Groups and Computation II*, volume 28 of *Amer. Math. Soc. DIMACS Series*, pages 55–60. (DIMACS, 1995), 1997.

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

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

[13] Jason Fulman, Peter M. Neumann, and Cheryl E. Praeger. A Generating Function Approach to the Enumeration of Matrices in Classical Groups over Finite Fields. Mem. Amer. Math. Soc. **176**, no. 830, 2005.

[14] Mark Giesbrecht. Nearly optimal algorithms for canonical matrix forms. SIAM J. Comput. 24 (1995), no. 5, 948–969.

[15] S.P. Glasby, C.R. Leedham-Green, and E.A. O'Brien. Writing projective representations over subfields. *J. Algebra*, 295, 51-61, 2006.

[16] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. The classification of the finite simple groups. Number 3. Part I, American Mathematical Society, Providence, RI, 1998.

[17] D.F. Holt and S. Rees. Testing modules for irreducibility. *J. Austral. Math. Soc. Ser. A* **57** (1994), 1–16.

[18] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory*. Chapman and Hall/CRC, London, 2005.

[19] P.E. Holmes, S.A. Linton, E.A. O'Brien, A.J.E. Ryba and R.A. Wilson, Constructive membership in black-box groups, preprint.

[20] William M. Kantor and Ákos Seress. Black box classical groups. *Mem. Amer. Math. Soc.*, **149**, 2001.

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

[22] F. Lübeck, K. Magaard, and E.A. O'Brien. Constructive recognition of $\mathrm{SL}_3(q)$. Preprint 2005.

[23] B. Huppert. *Endliche Gruppen I*, volume 134 of *Grundlehren Math. Wiss.* Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[24] C.R. Leedham-Green and E.A. O'Brien (1996), "Tensor Products are Projective Geometries", *J. Algebra*, **189**, 514–528, 1997.

[25] Peter M. Neumann and Cheryl E. Praeger. A recognition algorithm for special linear groups. *Proc. London Math. Soc.* (3), 65:555–603, 1992.

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

[27] Alice C. Niemeyer and Cheryl E. Praeger. Implementing a recognition algorithm for classical groups. In *Groups and Computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 273–296, Providence, RI, 1997. Amer. Math. Soc.

[28] Alice C.Niemeyer and Cheryl E.Praeger. A recognition algorithm for non-generic classical groups over finite fields. J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 223–253.

[29] E.A. O'Brien. Towards effective algorithms for linear groups. *Finite Geometries, Groups and Computation*, (Colorado), pp. 163-190. De Gruyter, Berlin, 2006.

[30] Igor Pak. The product replacement algorithm is polynomial. In *41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000)*, 476–485, IEEE Comput. Soc. Press, Los Alamitos, CA, 2000.

[31] Cheryl E. Praeger. Primitive prime divisor elements in finite classical groups. In *Groups St. Andrews 1997 in Bath, II*, 605–623, Cambridge Univ. Press, Cambridge, 1999.

[32] C.W. Parker and R.A. Wilson. Recognising simplicity in black-box groups. Preprint 2005.

[33] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[34] Arne Storjohann. An $O(n^3)$ algorithm for the Frobenius normal form. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation* (Rostock), 101–104, ACM, New York, 1998.

[35] Donald E. Taylor, The geometry of the classical groups. Sigma Series in Pure Mathematics, **9**. Heldermann Verlag, Berlin, 1992.

[36] Joachim von zur Gathen and Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2002.

[37] Hans Zassenhaus. On the spinor norm. Arch. Math. 13 1962 434–451.

School of Mathematical Sciences
Queen Mary, University of London
London E1 4NS,
United Kingdom
C.R.Leedham-Green@qmul.ac.uk

Department of Mathematics
Private Bag 92019, Auckland
University of Auckland
New Zealand
obrien@math.auckland.ac.nz

Last revised July 28, 2007