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 in its natural representation defined over a finite field F of odd characteristic. We present Las Vegas 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 polynomial-time, subject to the existence of a discrete logarithm oracle for F.

1 Introduction

The goal of the 'matrix group recognition project' is the development of efficient algorithms for the investigation of subgroups of $\mathrm{GL}(d, F)$ where F is a finite field. A particular aim is to construct 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: examples include constructing the Sylow p-subgroups of G for given prime p. We refer to the recent survey [35] for background related to this work.

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. Informally, a *constructive recognition algorithm* constructs an explicit isomorphism between 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 [38, p. 192].

In our context, $\langle X \rangle = G \leq \mathrm{GL}(d, F)$ is a classical group of odd characteristic in its *natural representation*, so one might regard the construction of the identity map as an easy exercise! However, a solution to the constructive recognition problem requires us to write an arbitrary element of G as an SLP in the given generating set X. In this paper, we define *standard generators* for G from which SLPs to arbitrary elements of

This work was supported in part by the Marsden Fund of New Zealand via grant UOA 721. We thank Peter Brooksbank and Cheryl Praeger for detailed commentary and discussion on various drafts of this paper. We thank John Bray, Bill Kantor, Frank Lübeck, Alice Niemeyer, and Robert Wilson for helpful discussions. 2000 *Mathematics Subject Classification.* Primary 20C20, 20C40.

G may readily be constructed, and then devise algorithms to construct these standard generators as SLPs in X.

We comment briefly on the significance of our work. As a doubly parameterised family, the classical groups in their natural representation are the most ubiquitous and challenging of all linear groups. The constructive recognition problem is fundamental: its solution is key to a number of other hard problems, including conjugacy testing of subgroups and elements, and construction of maximal subgroups. The algorithms we present here to solve the problem are both provably theoretically efficient and also eminently practical: their structure was influenced by this latter concern. Subject to the existence of a discrete logarithm oracle, their complexity is $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ measured in field operations, where q is the field size and ξ is the cost of constructing a random element.

Another striking aspect of our work is the short length of the SLPs in X we construct to encode the canonical generators of G. Subject to certain assumptions about the behaviour of the algorithm used to generate random elements, one family of algorithms constructs SLPs of length $O(\log^3 d)$, which is polynomial in $\log\log|G|$; by contrast, Babai & Szemerédi [3] prove that an arbitrary element of G has an SLP in X of length $O(\log^2 |G|)$.

Central to our work are centralisers of involutions, long of theoretical importance. As part of our analysis, we compute lower bounds to the proportions of elements that power to involutions of various types. Of particular interest is the proportion of elements of a classical group that power to a strong involution (see Definition 4.1). Our lower bound for this proportion follows easily from our estimates of the number of elements of the group whose characteristic polynomial factorises in a given way. A better bound – inversely proportional to the logarithm of the Lie rank rather than inversely proportional to the Lie rank – was recently obtained by Lübeck, Niemeyer, and Praeger [30]. Their paper, motivated by our work, uses very interesting and powerful techniques. We retain our analysis for two reasons: our results apply more generally to other classes of involutions needed by our algorithms, and are also used to construct the factors of the direct product of two classical groups.

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 $d > 1$, q is odd, and V denotes the underlying vector space.

- $\mathrm{GL}(d, q)$, the group of all invertible $d \times d$ matrices over $\mathrm{GF}(q)$.
- $\mathrm{Sp}(d, q)$, 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 type are conjugate in the corresponding general linear group. 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 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 $\mathrm{SO}^0(d,q) = \mathrm{SO}(d,q)$. 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.

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

Let $\mathcal{C}$ denote the union of the second and third classes of subgroups of $\mathrm{GL}(d,q)$, so it consists of classical groups in their natural representations. We say that $\mathrm{SX}(d,q)$ and $\Omega^\epsilon(d,q)$ have *type* **SL**, **Sp**, **SU**, $\mathbf{SO}^\epsilon$, or $\mathbf{\Omega}^\epsilon$, where $\epsilon \in \{-,0,+\}$, and *parameters* (type, d,q).

We may regard each of these 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. If V has an associated non-degenerate form, then we may write $\mathrm{O}(V)$ rather than, for example, $\mathrm{O}^-(V)$, allowing the type of the form to determine the type of the group.

1.2 The primary result

Let G be a classical group in its natural representation contained in $\mathcal{C}$. We present and analyse two Las Vegas algorithms that take as input a generating subset X of G and the form preserved by G, and return as output *standard generators* of G as SLPs in X. (These standard generators are defined in Section 3.) 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.

Let ξ denote an upper bound to the number of field operations needed to construct an independent (nearly) uniformly distributed random element of a group, and let $\chi(q)$ denote an upper bound to the number of field operations equivalent to a call to a discrete logarithm 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 G in $\mathcal{C}$, and returns standard generators for G as* SLPs *of length $O(\log^3 d)$ in X. The algorithm has complexity $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q + \chi(q)))$ measured in field operations if G is neither of type $\mathbf{SO}^-$ or $\mathbf{\Omega}^-$. Otherwise the complexity is $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q + \chi(q)) + \chi(q^2))$ measured in field operations.*

We prove this theorem by exhibiting an algorithm with the given specifications; 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 fewer recursive calls. The bound of $O(\log^3 d)$ for the length of the SLPs is achieved only by the second algorithm; both have the stated time complexity. 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.

If we *assume* that a random element of the group can be constructed in $O(d^3)$ field operations, then, for fixed q, and subject to the existence of a discrete logarithm oracle, both algorithms require $O(d^4 \log d)$ field operations to construct the standard generators.

Our estimate of the complexity contains the term $d\xi$. This encodes the fact that $O(d)$ random elements of the group are constructed outside the recursive calls. Random elements are also constructed in the recursive calls: the total number of random elements constructed is $O(d \log d)$. If ξ is at least d^3, then Lemma 2.4 implies that the cost of constructing random elements in the recursive calls does not affect the complexity estimate.

Once we have constructed these standard generators for G, a standard 'generalised echelonisation' algorithm can be used to write a given element of G as an SLP in these generators. We do not consider this task here, but refer the interested reader to the algorithm of [9, Section 5], which performs this task in $O(d^3 \log q + \log^2 q)$ field operations.

1.3 Related work

Already constructive recognition algorithms exist for various families of groups.

Brooksbank's algorithms [9] to construct (different and larger) canonical generating sets for the natural representation of each of $\mathrm{Sp}(d,q)$, $\mathrm{SU}(d,q)$, and $\Omega^\epsilon(d,q)$ have complexity

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

and again assumes the existence of a discrete logarithm oracle. The algorithm of Celler & Leedham-Green [16] for $\mathrm{SL}(d, q)$ has complexity $O(d^4 q)$.

Kantor & Seress [27] have developed *black-box* constructive recognition algorithms (see [38, p. 17]) for the classical groups. These algorithms do not run in time polynomial in the size of the input: their complexity involves q. However, Brooksbank & Kantor [11] demonstrate that the complexity of these algorithms can be made polynomial in $\log q$ given an oracle for explicit membership testing in $\mathrm{SL}(2, q)$ and (in some cases) in $\mathrm{SL}(2, q^2)$. Subject to a fixed number of calls to a discrete logarithm oracle for $\mathrm{GF}(q)$, Conder & Leedham-Green [17] and Conder, Leedham-Green & O'Brien [18] present a Las Vegas algorithm which constructively recognises $\mathrm{SL}(2, q)$ as a linear group in defining characteristic in time polynomial in the size of the input. Brooksbank [10] and Brooksbank & Kantor [11, 12] have exploited this work to produce better constructive recognition algorithms for black-box classical groups.

Other constructive recognition algorithms include those of Bäärnhielm [4] for the Suzuki groups and of Beals *et al.* [6] for black-box representations of alternating groups.

1.4 Other directions

We plan to develop similar constructive recognition algorithms for classical groups of characteristic 2 in their natural representation. We will also generalise these algorithms to deal with an arbitrary representation of a classical group in the defining characteristic. An efficient algorithm to write elements of classical groups given in any representation in the defining characteristic (even or odd) as SLPs in the standard generators has been developed by Costi [19].

1.5 The content of the paper

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 4–7 the algorithms are described: the non-orthogonal groups are first presented uniformly. The algorithms use involutions whose -1-eigenspaces have dimensions in a prescribed range. The cost of finding and constructing such involutions is analysed in Sections 8 and 9. We frequently compute high powers of elements of linear groups; an algorithm to do this efficiently is described in Section 10. In Section 11 we discuss how to construct the perfect quotients of the factors of a direct product of two classical groups. The centraliser of an involution is constructed using an algorithm of Bray [8]; this is considered in Section 12. The base cases of the algorithms (when $d \leq 6$) are discussed in Sections 13 and 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 [7].

2 Notation and background

Throughout the paper q denotes an odd prime power.

We assume familiarity with most basic results in the theory of classical groups; all can be found in [39]. Recall that the spinor norm (see [39, p. 163]) is a homomorphism from $\mathrm{SO}^\epsilon(d,q)$ to $\{\pm 1\}$ with kernel $\Omega^\epsilon(d,q)$. 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 or hermitian 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 [39, Theorem 7.4]; we have specialised the quoted theorem to the case where the form is non-degenerate. If the bilinear form restricted to U is non-degenerate, then f can be chosen to have determinant 1. If, in addition, the form is symmetric, and U has codimension at least 2 in V, we can choose f to have determinant 1 and 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 f, and then fh^{-1} will be the required isometry of V.

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

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.

Involution centralisers are fundamental to our algorithms. We briefly review the structure of involution centralisers in (projective) classical groups defined over fields of odd characteristic. A detailed account can be found in [23, 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, since the involution must have determinant 1.

If G preserves a non-degenerate form, then 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 $\mathrm{GL}(V)$, then 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 $\mathrm{SO}^\epsilon(m,q) \times \mathrm{SO}^\epsilon(n,q)$ consisting of those pairs of elements whose spinor norms are equal by $\mathrm{SO}^\epsilon(m,q) \times_{C_2} \mathrm{SO}^\epsilon(n,q)$.

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 $\epsilon = +$, and are of opposite types if $\epsilon = -$.

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 well-known result.

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 Las Vegas algorithms 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, then we write $f(n) = O(g(n))$ to mean $|f(n)| < C|g(n)|$ for some positive constant C and all sufficiently large n. The modulus here will be relevant only when $g(n)$ tends to 0 with n.

A *Las Vegas* algorithm is a randomised algorithm which never returns an incorrect answer, but may report failure with probability less than some specified value.

Our algorithms usually search for elements of G having a specified type. As part of the analysis of these algorithms, we determine a lower bound, say $1/k$, for the proportion of such elements in G. It is now an easy exercise to prescribe the probability of failure of the corresponding algorithm. Namely, to find such an element by random search with a probability of failure less than a given $\epsilon \in (0,1)$ it suffices to choose (with replacement) a sample of uniformly distributed random elements in G of size at least $\lceil -\log_e(\epsilon) \rceil k$. Hence we do not include such estimates as part of each theorem.

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, that $f(d) \leq md^k$ for all $d > 1$. This is obvious for $d = 2, 3$. 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

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

The result follows. □

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 $1-(1/3)^k-(2/3)^k > 0$.

2.2 The pseudo-order of a matrix

While the precise order of an arbitrary $g \in \mathrm{GL}(d, q)$ cannot be determined in polynomial time, because of problems with integer factorisation, we can readily compute a "good" multiplicative upper bound for $|g|$, which we shall call its *pseudo-order*.

Let the factorisation over $\mathrm{GF}(q)$ of the minimal polynomial $f(x)$ of g into powers of distinct irreducible monic polynomials be given by $f(x) = \prod_{i=1}^{t} f_i(x)^{n_i}$, where $\deg(f_i) = e_i$. Then $|g|$ divides $B = \mathrm{lcm}(q^{e_1}-1, \ldots, q^{e_t}-1) \times p^{\beta}$, where $\beta = \lceil \log_p \max n_i \rceil$ and $\mathrm{GF}(q)$ has characteristic p.

From B, we can readily learn in polynomial time the *exact* power of any specified prime that divides $|g|$. In particular, we can determine if g has even order.

Recall from [33] 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 $i < e$.

Definition 2.5 *Using the above notation, let $u_1 < u_2 < \ldots < u_s$ be the factors of the distinct degrees of the irreducible factors of $f(x)$. The pseudo-order of g is defined to be $n := p^{\beta} \cdot \prod_{k=1}^{s} r_k \cdot \prod_{j \in J} p_j$ where:*

(i) *$\{p_j : j \in J\}$ is the multiset of primes that divide $|g|$ and are at most $d+1$;*

(ii) *$r_k \neq 1$ if and only if $|g|$ is a multiple of a primitive prime divisor of $q^{u_k} - 1$ greater than $d+1$. In this case r_k is the product of all the primitive prime divisors of $q^{u_k} - 1$, with multiplicities, that are greater than $d+1$. (Here, the multiplicity of a prime is the multiplicity with which it divides $q^{u_k} - 1$.)*

Clearly $|g|$ divides the pseudo-order of g. If $r_k \neq 1$ then r_k is a *pseudo-prime divisor* of $|g|$.

Lemma 2.6 *The following algorithm returns the product m of the primitive prime divisors of $q^e - 1$, multiplied by powers of certain primes at most e.*

Algorithm 1: `Factorise`

```
begin
    $m := q^e - 1$;
    For $i = 1$ to $e - 1$ do if $i$ divides $e$ then $m := m/\gcd(m, q^i - 1)$;
    return $m$;
end
```

Proof: Let ℓ be a prime dividing the returned value of m. Since ℓ divides m, it follows that ℓ is a primitive prime divisor of $q^i - 1$ for some i dividing e. If the multiplicity of ℓ, as a prime divisor of $q^e - 1$, is greater than its multiplicity as a prime divisor of $q^i - 1$, then ℓ divides $(q^e - 1)/(q^i - 1) = 1 + q^i + \cdots + q^{e-i}$, and hence divides e. The result follows. □

The greatest common divisors used in the algorithm can be calculated readily using the following observations: $\gcd(q^i - 1, q^j - 1) = q^k - 1$, where $k = \gcd(i, j)$, and $\gcd(n/a, b) = \gcd(n, b)/\gcd(a, b)$.

Thus we can factorise B as $\prod_{k=1}^{s} r_k \prod_{j \in J} p_j$, where, for all j, p_j is a prime at most $d+1$, and r_k is the product of those primitive prime divisors (with multiplicities) of $q^{u_k} - 1$ that are greater than $d+1$.

For easy reference, we summarise the costs of certain basic operations.

Lemma 2.7

(i) *Multiplication and division operations for polynomials of degree d defined over $\mathrm{GF}(q)$ can be performed deterministically in $O(d \log d \log\log d)$ field operations. Using a Las Vegas algorithm, such a polynomial can be factored into its irreducible factors in $O(d^2 \log d \log\log d \log q)$ field operations.*

(ii) *Using Las Vegas algorithms, both the characteristic and minimal polynomial of $g \in \mathrm{GL}(d, q)$ can be computed in $O(d^3 \log d)$ field operations.*

(iii) *Using a Las Vegas algorithm, the multiplicative upper bound B to the order of $g \in \mathrm{GL}(d, q)$ can be computed in $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations.*

(iv) *Using a Las Vegas algorithm, the pseudo-order of $g \in \mathrm{GL}(d,q)$ can be computed in $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations.*

Proof: For the cost of polynomial operations, see [40, §8.3, §9.1, Theorem 14.14].

The characteristic and minimal polynomials of g can be computed in the claimed time using the Las Vegas algorithms of [1, 28] and [21] respectively.

Hence B can be obtained in the claimed time.

Using Lemma 2.6, we can express B as the product of at most $2d+1$ factors, each of which is either a pseudo-prime factor of B, or a prime-power factor of B. To compute the pseudo-order of g from this information requires $O(\log|g| \log d)$ operations in the ring $\mathrm{GF}(q)[t]/(f(t))$, as in [15]. □

We choose the bound of $d+1$ on the primes being extracted in our definition of pseudo-order for two reasons: Lemma 2.6 shows that bound must be at least d; the algorithm of [33] requires knowledge of the precise prime divisor in question if this is $d+1$ (in the definition of a large primitive prime divisor). Of course, the upper bound could be enormously increased without problems of integer factorisation arising.

Observe that the concept of primitive prime divisor is only well-defined if one regards q as part of the data. If $q = p^f$, then a primitive prime divisor of $q^e - 1$ need not be a primitive prime divisor of $p^{ef} - 1$, since the prime in question might divide $p^n - 1$ for some $n < ef$, but not $q^m - 1$ for any $m < e$. If the prime does not divide $p^n - 1$ for any $n < ef$, then it is a *strong* primitive prime divisor of $q^e - 1$, and in some cases this is a requirement for the algorithm of [33]. To accommodate this condition, we need to factorise B accordingly, this being achieved by the same algorithm that was used above, but with the parameters q and e replaced by p and fe respectively. These variations do not affect the complexity analysis.

3 Standard generators for classical groups

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

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 in turn is 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 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 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 $i, j < n$; in addition $w_1.e_i = w_1.f_i = w_2.e_i = w_2.f_i = w_1.w_2 = 0, w_1.w_1 = -2$, and $w_2.w_2 = 2\omega$ where ω is a primitive element of $\mathrm{GF}(q)$. Since ω is not a square in $\mathrm{GF}(q)$, this defines a form of $-$ type (see Lemma 2.3).

7. If V has dimension $2n+1$, then there are two equivalence classes of non-degenerate symmetric bilinear forms on V, distinguished by their discriminants. To convert a form in one class to a form in the other class, we multiply it by a non-square scalar, thus obtaining an inequivalent form preserved by the same group. A hyperbolic basis 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 $w.w = -1/2$. If necessary, we multiply the form for the input group by a non-square scalar.

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 $(e_1, f_1, \ldots, e_n, f_n, w)$.

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. We assume $n > 1$ for the groups $\mathrm{SO}^\epsilon(2n, q)$. In Table 2 the generators of $\mathrm{SO}^+(2n, q)$ 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 $B = (e_1, f_1, w_1, w_2)$. For $\mathrm{SO}(2n + 1, q)$ we write the action of matrices with respect to basis $B = (e_1, f_1, w)$.

6. In the definition for $\mathrm{SO}^-(2n, q)$, 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 $\mathrm{SO}^\epsilon(d, q)$, the generator σ has spinor norm -1; the others are the standard generators for the corresponding $\Omega^\epsilon(d, q)$. For $\epsilon = 0, +$, the value of b is determined by $q - 1 = 2^a \cdot b$ where b is odd; $\lambda = (-1)^{(q-1)/2}$.

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 $\mathrm{SL}(d, q)$ 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 $1 \leq i \leq n$, 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 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 that of $\Omega(2n + 1, q)$ is $C_2 \wr S_n$.

If G is $\mathrm{SL}(d, q)$ or $\mathrm{Sp}(d, q)$, then its standard generators have the property that it is easy to construct from them any of its root groups, and consequently we deduce that they generate G. 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 [13]. The situation is similar for $\mathrm{SU}(d, q)$ and the orthogonal groups, as we now show.

Lemma 3.1 *Let $G = \mathrm{SU}(d, q)$ for $d \geq 2$. Then $G = \langle s, t, \delta, u, v, x, y \rangle$.*

PROOF: If $d = 2$, then u, v, x and y are by convention trivial, and $\langle s, t, \delta \rangle$ is isomorphic to $\mathrm{SL}(2, q) \cong \mathrm{SU}(2, q)$. 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 $S = \langle x^{y^k} : 1 \leq k \leq q^2 - 1 \rangle$ is non-abelian of order q^3, having derived group and centre of order q. A similar calculation for $d = 2n$ where $n > 1$ shows that $\langle x^{y^k} : 0 \leq k < q^2 - 1 \rangle$ has order q^2. These groups correspond to the subgroups X_S^1 of [13] and the result follows from [13, Proposition 13.6.5]. □

Lemma 3.2 *Let $G = \Omega^+(2n, q)$ for $n \geq 2$. 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 [39, 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 for V 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 $\mathrm{SL}(2, q)$. 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. Observe that $v = s'$ in dimension 4.

Observe that the spinor norm of v is $+1$ if $n > 2$. If n is odd, this follows since v is of odd order. If $n > 2$ is even, then

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

and the observation follows from that for $n = 2$ and odd $n > 2$.

Since the Weyl group of $\Omega^+(2n, q)$ is generated modulo diagonal elements by $\{s, s', v\}$, the lemma is now proved. □

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
$\mathrm{SO}^-(2n,q)$	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^{-1} & 0 & 0 \\ 0 & 0 & A & B \\ 0 & 0 & C & A \end{pmatrix}$	$(e_1,e_2)^-(f_1,f_2)^-$	$(e_1,\ldots,e_{n-1})^{\epsilon n-1}(f_1,\ldots,f_{n-1})^{\epsilon n-1}$	$\begin{pmatrix} \lambda I_2 & 0 \\ 0 & -\lambda I_2 \end{pmatrix}$
Group	s	t	δ	u	v	σ
$\mathrm{SO}(2n+1,q)$	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} \omega^2 & 0 & 0 \\ 0 & \omega^{-2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$(e_1,e_2)^-(f_1,f_2)^-$	$(e_1,\ldots,e_n)^{\epsilon n}(f_1,\ldots,f_n)^{\epsilon n}$	$\begin{pmatrix} \omega^b & 0 & 0 \\ 0 & \omega^{-b} & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Table 2: Standard generators for orthogonal groups

Lemma 3.3 *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 [39, 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 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 $\Omega^-(4, q)$.

A similar argument to that in Lemma 3.2 shows that v has spinor norm $+1$. Since the Weyl group of $\Omega^-(2n, q)$ is generated modulo diagonal elements by $\{s, u, v\}$, the lemma is now proved. □

Lemma 3.4 *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 [39, 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 correspond, respectively, to the matrices

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

A similar argument to that in Lemma 3.2 shows that v has spinor norm $+1$. Since the Weyl group of $\Omega(2n+1, q)$ is generated modulo diagonal elements by $\{s, u, v\}$, the lemma is now proved. □

Lemma 3.5 *The standard generator σ lies in $\mathrm{SO}^\epsilon(d, q) \setminus \Omega^\epsilon(d, q)$.*

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

If $\epsilon \in \{+, 0\}$, then the spinor norm of σ is ω^b modulo the subgroup of squares of $\mathrm{GF}(q)^\times$ (see [41] and the proof of Lemma 8.14). Since b is odd and ω is a primitive element of $\mathrm{GF}(q)$, the result follows.

Now assume $\epsilon = -$. Observe that σ acts as -1 on a 2-dimensional subspace that supports a form of $+$ type if $q \equiv 3 \bmod 4$, and of $-$ type if $q \equiv 1 \bmod 4$, and σ acts as $+1$ on the orthogonal complement of this 2-dimensional subspace. The conclusion now follows since $\Omega^+(2, q)$ has odd order $(q-1)/2$ if $q \equiv 3 \bmod 4$, and $\Omega^-(2, q)$ has odd order $(q+1)/2$ if $q \equiv 1 \bmod 4$. □

Note that we could have taken $\sigma \in \mathrm{SO}^\epsilon(2n, q)$ to be $-I_{2n}$ if $\epsilon = -$ and either $q \equiv 1 \bmod 4$ or n is even; or if $\epsilon = +$ and n is odd and $q \equiv 3 \bmod 4$. In these cases $\mathrm{SO}^\epsilon(2n, q) \cong \Omega^\epsilon(2n, q) \times \langle -I_{2n} \rangle$.

We conclude with the following observation which influences the algorithms we develop in Section 4.

Lemma 3.6 *Let $G = \langle s, t, \delta, u, v, x, y \rangle \le \mathrm{GL}(2n, q)$ and let $H = \langle s, t, \delta, u, v \rangle$. If G is $\mathrm{SL}(2n, q)$ or $\mathrm{Sp}(2n, q)$ or $\mathrm{SU}(2n, q)$, then $H = \mathrm{SL}(2, q) \wr C_n$, or $H = \mathrm{SL}(2, q) \wr S_n$ or $H = \mathrm{SU}(2, q) \wr S_n$ respectively.*

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 the classical form preserved by G, and returns standard generators for G as SLPs in X. The standard generators are written 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.

In all cases, non-orthogonal and orthogonal, we use a 'divide and conquer' strategy.

Definition 4.1 *A strong involution in* $\mathrm{SX}(d, q)$ *for* $d > 2$ *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 d: algorithms `OneEven` and `OneOdd` address the case of even and odd d, respectively. If $d = 2n$, then Lemma 3.6 shows that $Y_0 := \{s, t, \delta, u, v\}$ generates $\mathrm{SX}(2, q) \wr C_n$ or $\mathrm{SX}(2, q) \wr S_n$ according to the type of the input group. If d is even, then, as the first and major task of the main algorithm, `OneEven` constructs Y_0; as a final step, `OneMain` constructs the additional elements x, y. The reason that we construct standard generators for $\mathrm{SX}(2, q) \wr C_n$ and $\mathrm{SX}(2, q) \wr S_n$ recursively, rather than for $\mathrm{SX}(d, q)$, is that this allows us to carry out the expensive construction of the additional elements *once*, outside the recursion.

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

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

```
   /* $X$ is a generating set for the classical group $G \in \mathcal{C}$ 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 $\mathrm{SX}(2,q) \wr S_{d/2}$, 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 $(X, \mathit{type}, \mathcal{F})$;
 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     In $C$ find generating sets $X_1$ and $X_2$ for $\mathrm{SX}(E_+)$ and $\mathrm{SX}(E_-)$;
 8     $((s_1, t_1, \delta_1, u_1, v_1), B_1) :=$ OneEven $(X_1, \mathit{type}, \mathcal{F}|_{E_+})$;
 9     $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ OneEven $(X_2, \mathit{type}, \mathcal{F}|_{E_-})$;
10     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 $B_2$;
11     $a := (s_1^2)^{v_1^{-1}}(s_2^2)$;
12     Find generators for the centraliser $D$ of $a$ in $G$;
13     In $D$ find a generating set $X_3$ for $\mathrm{SX}(\langle e_k, f_k, e_{k+1}, f_{k+1} \rangle)$;
14     In $\langle X_3 \rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
15     $v := v_2 b v_1$;
16     return $(s_1, t_1, \delta_1, u_1, v)$ and the change-of-basis matrix for $B$;
17 end
```

We make the following observations on Algorithm `OneEven`.

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

2. Generators for the involution centralisers in lines 6 and 13 are constructed using the algorithm of Bray [8], see Section 12. We need only a subgroup of the centraliser that contains the derived group.

3. The generators for the direct factors in line 7 are constructed using the algorithm described in Section 11.

4. The algorithms for the `BaseCase` call in line 3 are discussed in Section 13. In summary, `BaseCase` $(X, \mathit{type}, \mathcal{F})$ returns the standard generators, the associated SLPs, and the corresponding change-of-basis matrix 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 8.

6. The recursive calls in lines 8 and 9 are in smaller dimension. As shown in Lemma 2.4, these only affect the time and space complexity of the algorithm up to a constant multiple; however they contribute to the length of the SLPs produced. We consider these issues in Sections 15 and 16.

7. In line 11, a is an involution with -1-eigenspace $\langle e_k, f_k, e_{k+1}, f_{k+1}\rangle$.

8. The element b is the *glue*, used in the assignment $v := v_2 b v_1$ to 'glue' the elements v_1 and v_2. We discuss how to find b as an element of $\langle X_3\rangle$ in Section 13.2.

Algorithm `OneOdd`, for the odd degree case, is similar to Algorithm `OneEven` and much of this commentary also applies.

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

```
/* $X$ is a generating set for the classical group $G \in \mathcal{C}$ 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 $(X, \mathit{type}, \mathcal{F})$;
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      In $C$ find generating sets $X_1$ and $X_2$ for $\mathrm{SX}(E_+)$ and $\mathrm{SX}(E_-)$;
8      $((s_1, t_1, \delta_1, u_1, v_1, x, y), B_1) :=$ OneOdd $(X_1, \mathit{type}, \mathcal{F}|_{E_+})$;
9      $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ OneEven $(X_2, \mathit{type}, \mathcal{F}|_{E_-})$;
10     If $B_1 = (e_1, f_1, \ldots, e_k, f_k, w)$ and $B_2 = (e_{k+1}, f_{k+1}, \ldots, e_{(d-1)/2}, f_{(d-1)/2})$, then
       let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, \ldots, e_{(d-1)/2}, f_{(d-1)/2}, w)$;
11     $a := (s_1^2)^{v_1^{-1}}(s_2^2)$;
12     Find generators for the centraliser $D$ of $a$ in $G$;
13     In $D$ find a generating set $X_3$ for $\mathrm{SX}(\langle e_k, f_k, e_{k+1}, f_{k+1}\rangle)$;
14     In $\langle X_3\rangle$ find the permutation matrix $b = (e_k, e_{k+1})(f_k, f_{k+1})$;
15     $v := v_2 b v_1$;
16     return $(s_1, t_1, \delta_1, u_1, v, x, y)$ and the change-of-basis matrix for $B$;
17 end
```

We summarise the main algorithm for non-orthogonal groups as Algorithm `OneMain`.

```
Algorithm 4: OneMain ($X$, $type$, $\mathcal{F}$)   for non-orthogonal groups
  /* $X$ is a generating set for the classical group $G \in \mathcal{C}$ in odd characteristic, of
     type SL or Sp 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.                                                  */
begin
    $d :=$ the rank of the matrices in $X$;
    if $d$ is odd then
        $((s, t, \delta, u, v, x, y), B) :=$ OneOdd ($X$, $type$, $\mathcal{F}$);
    else
        $((s, t, \delta, u, v), B) :=$ OneEven ($X$, $type$, $\mathcal{F}$);
        Construct additional elements $x$ and $y$;
    end
    return $(s, t, \delta, u, v, x, y)$ and the change-of-basis matrix for $B$;
end
```

The correctness and complexity of this algorithm, and the lengths of the resulting SLPs for the standard generators, are discussed in Sections 8 and 15–16. The construction of x and y is discussed in Section 13.

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 4 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 eigenspaces E_+ and E_- of h. We construct the projective centraliser of h in $\mathrm{SX}(d,q)$ by applying the algorithm of [8] to construct the centraliser of $\bar{h}$ in $\mathrm{PX}(d,q)$, and taking its preimage C. We identify $c \in C$ that interchanges the two eigenspaces.

If we now find recursively the subset Y_0 of standard generators for $\mathrm{SX}(E_+)$ with respect to the basis $\mathcal{B}$, then Y_0^c 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, then 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 9. Algorithm TwoEven, which summarises the even degree case, returns the generating set Y_0 defined in Section 4. We complete the construction of Y exactly as in Section 4.

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

```
/* $X$ is a generating set for the classical group $G \in \mathcal{C}$ 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 $Y_0$ for $\mathrm{SL}(2,q) \wr C_{d/2}$
   if *type* is **SL**, otherwise for $\mathrm{SX}(2,q) \wr S_{d/2}$, 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 $d = 4$ return OneEven ($X, type, \mathcal{F}$);
4      $k := d/4$;
5      Find by random search $g \in G := \langle X \rangle$ of even order such that $g$ powers to an
       involution $h$ with eigenspaces of dimension $2k$;
6      Let $E_+$ and $E_-$ be the eigenspaces of $h$;
7      Find generators for the projective centraliser $C$ of $h$ in $G$ and identify an
       element $c$ of $C$ that interchanges the two eigenspaces;
8      In $C$ find a generating set $X_1$ for $\mathrm{SX}(E_+)$;
9      $((s_1, t_1, \delta_1, u_1, v_1), B_1) :=$ TwoEven($X_1, type, \mathcal{F}|_{E_+}$);
10     $s_2 := s_1^c$;
11     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 $B_1^c$;
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
```

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

```
/* $X$ is a generating set for the classical group $G \in \mathcal{C}$ 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 $Y_0$ for
   $\mathrm{SL}(2,q) \wr C_{d/2}$ if type is **SL**, otherwise for $\mathrm{SX}(2,q) \wr S_{d/2}$, as subgroup of $G$, the
   SLPs for the elements of $Y_0$, and the change-of-basis matrix.                    */
begin
    $d :=$ the rank of the matrices in $X$;
    If $d \leq 8$ return OneEven $(X, \mathit{type}, \mathcal{F})$;
    Find, by random search, $g \in G := \langle X \rangle$ of even order such that $g$ powers to
        an involution $h$ with eigenspaces of dimensions 2 and $d-2$;
    Let $E_1$ and $E_2$ be the eigenspaces of $h$, of dimensions $d-2$ and 2 respectively;
    Find generators for the centraliser $C$ of $h$ in $G$;
    In $C$ find generating sets $X_1$ and $X_2$ for $\mathrm{SX}(E_1)$ and $\mathrm{SX}(E_2)$ respectively;
    $((s_1, t_1, \delta_1, u_1, v_1), B_1) :=$ TwoTimesFour $(X_1, \mathit{type}, \mathcal{F}|_{E_1})$;
    $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ BaseCase $(X_2, \mathit{type}, \mathcal{F}|_{E_2})$;
    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 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
```

Algorithm 7: `TwoEven`$(X, \mathit{type}, \mathcal{F})$ for non-orthogonal groups

```
/* $X$ is a generating set for the classical group $G \in \mathcal{C}$ in odd characteristic, of
   type **SL** or **Sp** or **SU**, in even dimension $d$. 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 $\mathrm{SX}(2,q) \wr S_{d/2}$, as subgroup of $G$, the SLPs for the elements of
   $Y_0$, and the change-of-basis matrix.                                              */
begin
    $d :=$ the rank of the matrices in $X$;
    if $d \bmod 4 = 2$ then
        return TwoTwiceOdd$(X, \mathit{type}, \mathcal{F})$;
    else
        return TwoTimesFour$(X, \mathit{type}, \mathcal{F})$;
    end
end
```

If d is odd, then we find an involution whose -1-eigenspace has dimension $d-3$, 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` is the same as `OneMain`, except that it calls `TwoOdd` or `TwoEven` rather than `OneOdd` or `OneEven`.

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

6 Algorithm `One` for orthogonal groups

The algorithms for orthogonal groups are more complex in design than those for other classical groups.

If $q \equiv 3 \bmod 4$, then $\Omega^+(2,q)$ has odd order and so does not contain $-I_2$. Hence we must use a new strategy to construct the involution whose centraliser contains the 'glue' element. 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 $\Omega^\epsilon(d,q)$ when $q \equiv 1 \bmod 4$, then for $\mathrm{SO}^\epsilon(d,q)$ for all odd q, and finally for $\Omega^\epsilon(d,q)$ when $q \equiv 3 \bmod 4$.

The base cases for the orthogonal groups are discussed in Section 14 and are realised via `OrthogonalBaseCase`.

6.1 Groups preserving forms of + type

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

This case is similar to Algorithm `One` for the other classical groups. Let $G = \Omega^+(2n,q)$ when $q \equiv 1 \bmod 4$, and let V denote the underlying vector space. An involution 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. Algorithm `OneOmegaPlus1` summarises the construction of standard generators for G.

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

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.

We modify `OneOmegaPlus1` to obtain the resulting algorithm, `OneSpecialPlus`, by making the following changes:

- the recursive calls are to `OneSpecialPlus`, and so construct the additional standard generator needed to generate $\mathrm{SO}^+(2n,q)$;
- in line 11, $m := (q-1)/2$ if $q \equiv 1 \bmod 4$, otherwise $m := 1$; in line 12, $a := (\sigma_1^m)^{v_1^{-1}}(\sigma_2^m)$.

```
Algorithm 8: OneOmegaPlus1 $(X, \mathcal{F})$
/* $X$ 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 OrthogonalBaseCase $(X, \mathcal{F})$;
    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 $G$;
    In $C$ find generating sets $X_1$ and $X_2$ for $\Omega^+(E_+)$ and $\Omega^+(E_-)$;
    $((s_1, t_1, \delta_1, u_1, v_1, s_1', t_1', \delta_1'), B_1) :=$ OneOmegaPlus1 $(X_1, \mathcal{F}|_{E_+})$;
    $((s_2, t_2, \delta_2, u_2, v_2, s_2', t_2', \delta_2'), B_2) :=$ OneOmegaPlus1 $(X_2, \mathcal{F}|_{E_-})$;
    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 $B_2$;
    $m := (q-1)/4$;
    $a := ((\delta_1\delta_1')^m)^{v_1^{-1}}(\delta_2\delta_2')^m$;
    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
```

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

The algorithm for $G = \Omega^+(2n, q)$ when $q \equiv 3 \bmod 4$ is more elaborate than when $q \equiv 1 \bmod 4$: now $\Omega^+(2, q)$ has odd order $(q-1)/2$ and so does not contain $-I_2$. To construct the involution whose centraliser contains the 'glue' element, we must move outside $\Omega(E)$ to $\mathrm{SO}(E)$ where E is a particular eigenspace.

Recall from Section 2 that $\mathrm{SO}(E) \times_{C_2} \mathrm{SO}(F)$ is the subgroup of $\mathrm{SO}(E) \times \mathrm{SO}(F)$ consisting of those pairs of elements whose spinor norms are equal.

We outline the steps of the algorithm, OneOmegaPlus3, which applies when $n > 2$. The remaining cases are considered in Section 14.

1. Find, by random search, an element of G that powers to a 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 for the centraliser $H = \mathrm{SO}(E) \times_{C_2} \mathrm{SO}(F)$ of i in G,

and hence generating sets X and Y for $\Omega(E)$ and $\Omega(F)$ as subgroups of H.

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. Hence both have even order. We also require one of the g_j, say g_2, to have twice odd order. Hence $|g_1| = 2^s k_1$ and $|g_2| = 2k_2$ where k_i is odd and $s \geq 1$. Assign $g := g^{k_1 k_2}$; now g has order a power of 2, and the image of g in $\mathrm{SO}(F)$ is an involution.

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

5. If z is an element of $\mathrm{SO}(E)$, then z is the projection onto E of the evaluation of an SLP on $X \cup \{g\} \subset \mathrm{SO}(E) \times \mathrm{SO}(F)$. Evaluating this SLP gives rise to an element (z, z_1), where $z_1 \in \mathrm{SO}(F)$. Since X centralises F, z_1 is a power of g_2, and hence is either the identity or g_2. But the spinor norms of z and z_1 are equal; so $z_1 = g_2$ if the spinor norm of z is -1, and $z_1 = 1$ otherwise. Thus, from Step 4, we obtain $h = (\sigma_E, g_2)$ where σ_E is the standard generator of $\mathrm{SO}(E)$ with spinor norm -1. Note that σ_E is an involution since $q \equiv 3 \bmod 4$.

6. Let $B = \langle Y, h\rangle$. Its projection onto F is $\mathrm{SO}(F)$. Using `OneSpecialPlus`, construct SLPs in the generators of B that map onto standard generators for $\mathrm{SO}(F)$. Now apply Step 5 with E and F, and also σ_E and g_2, interchanged. We thus construct (σ_E, σ_F).

7. Now conjugate (σ_E, σ_F) by a suitable power of v_1 to obtain a, the involution in whose centraliser the ‘glue’ element can be found.

The remaining steps of the algorithm are identical to those described in `OneOmegaPlus1` when $q \equiv 1 \bmod 4$. 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 standard generator $v := v_2 b v_1$.

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 in $G = \Omega^-(2n, q)$ whose centraliser contains a direct product of $\Omega^+(2n-4, q)$ and $\Omega^-(4, q)$. We then construct standard generators for each factor. Within the centraliser of an involution whose -1-eigenspace has dimension 4 and supports a form of + type, we find the ‘glue’ element.

An involution of G 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 `OneOmegaMinus1` summarises the construction of standard generators for G.

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

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. By analogous modifications to those outlined in Section 6.1.2, we modify `OneOmegaMinus1` to obtain `OneSpecialMinus`.

Algorithm 9: `OneOmegaMinus1` $(X, \mathcal{F})$

```
/* $X$ 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 OrthogonalBaseCase $(X, \mathcal{F})$;
    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 $d-4$ and let $F$ be the eigenspace
    of $h$ having dimension 4;
    Find generators for the centraliser $C$ of $h$ in $G$;
    In $C$ find generating sets $X_1$ and $X_2$ for $\Omega^+(E)$ and $\Omega^-(F)$;
    $((s_1, t_1, \delta_1, u_1, v_1, s_1', t_1', \delta_1'), B_1) :=$ OneOmegaPlus1 $(X_1, \mathcal{F}|_E)$;
    $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ OrthogonalBaseCase $(X_2, \mathcal{F}|_F)$;
    $k := (d-4)/2$;
    Let $B = (e_1, f_1, \dots, e_k, f_k, e_{k+1}, f_{k+1}, e_{d/2}, f_{d/2})$ be the concatenation of the
    hyperbolic bases defined by $B_1$ and $B_2$;
    $m := (q-1)/4$;
    $a := ((\delta_1 \delta_1')^m)^{v_1^{-1}} \delta_2^{m(q+1)}$;
    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 $(s_2, t_2, \delta_2, u_2, v)$ and the change-of-basis matrix for $B$;
end
```

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 construct standard generators for each factor. 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 to a 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 for the centraliser $H = \mathrm{SO}^+(E) \times_{C_2} \mathrm{SO}^-(F)$ of i in G, and hence generating sets X and Y for $\Omega(E)$ and $\Omega(F)$ as subgroups of H.

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 to have twice odd order. The proportion of elements of H with this property is the proportion of elements of $\mathrm{SO}^+(E)$ (if $j = 1$) or of $\mathrm{SO}^-(F)$ (if $j = 2$) of twice odd order, and of spinor norm -1. For ease of exposition we assume that $j = 2$. Hence $|g_1| = 2^s k_1$ and $|g_2| = 2k_2$ where k_i is odd and $s \geq 1$. Assign $g := g^{k_1 k_2}$; now g has order a power of 2, and the image of g in $\mathrm{SO}^-(F)$ is an involution.

With one exception, the remaining steps of this algorithm are identical to those described in `OneOmegaPlus3`: in Step 6, the projection of $B = \langle Y, h \rangle$ onto F is $\mathrm{SO}^-(F)$, and so we use `OneSpecialMinus` to construct SLPs in the generators of B that map onto standard generators for $\mathrm{SO}^-(F)$.

If $n = 3$ then the non-central involutions in $\Omega^-(6, q)$ have centralisers containing $\Omega^+(4, q) \times \Omega^-(2, q)$. Algorithms for $\Omega^-(4, q)$ and $\Omega^-(6, q)$ are presented in Section 14.

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 $G = \Omega(2n+1, q)$ whose centraliser contains $\Omega^+(2n-2, q) \times \Omega(3, q)$. We then construct standard generators for each factor. Within the centraliser of an involution whose -1-eigenspace has dimension 4 and supports a form of $+$ type, we find the 'glue' element.

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

Algorithm `OneOmegaCircle1` summarises the construction of standard generators for G.

Algorithm 10: `OneOmegaCircle1` $(X, \mathcal{F})$

```
/* $X$ 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 OrthogonalBaseCase $(X, \mathcal{F})$;
    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 $d-3$ and let $F$ be the eigenspace
    of $h$ having dimension 3;
    Find generators for the centraliser $C$ of $h$ in $G$;
    In $C$ find generating sets $X_1$ and $X_2$ for $\Omega^+(E)$ and $\Omega^0(F)$;
    $((s_1, t_1, \delta_1, u_1, v_1, s_1', t_1', \delta_1'), B_1) :=$ OneOmegaPlus1 $(X_1, \mathcal{F}|_E)$;
    $((s_2, t_2, \delta_2, u_2, v_2), B_2) :=$ OrthogonalBaseCase $(X_2, \mathcal{F}|_F)$;
    $k := (d-3)/2$;
    Let $B = (e_1, f_1, \ldots, e_k, f_k, e_{k+1}, f_{k+1}, w)$ be the concatenation of the
    hyperbolic bases defined by $B_1$ and $B_2$;
    $m := (q-1)/4$;
    $a := ((\delta_1 \delta_1')^m)^{v_1^{-1}} \delta_2^m$;
    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 $(s_2, t_2, \delta_2, s_1', v)$ and the change-of-basis matrix for $B$;
end
```

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

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. By analogous modifications to those outlined in Section 6.1.2, we modify `OneOmegaCircle1` to obtain `OneSpecialCircle`.

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 as n is odd or even. We then construct standard generators for each factor. Within the centraliser of an involution whose -1-eigenspace has dimension 4 and supports a form 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 $\Omega(3,q)$ and $\Omega(5,q)$ are presented in Section 14.

7 Algorithm `Two` for orthogonal groups

If $G = \Omega^+(d,q)$ and $q \equiv 1 \bmod 4$, or if $G = \mathrm{SO}^+(d,q)$ with no such restriction on q, then Algorithm `Two` is essentially the same as that presented for non-orthogonal groups.

If $G = \Omega^+(d,q)$ and $q \equiv 3 \bmod 4$, then the -1-eigenspace of an involution in G has dimension a multiple of 4 if it supports a form of + type (see Lemma 2.2).

Hence, if d is a multiple of 8, then we find an involution whose eigenspaces are of equal dimension, and which support forms of + type. We next find generators for the centraliser of this involution, and call Algorithm `Two` for $\mathrm{SO}^+(d/2,q)$ acting on one of the eigenspaces. We then proceed as in Algorithm `Two` for non-orthogonal groups.

If $d \equiv e \bmod 8$, where $e \in \{2,4,6\}$, and $d > 8$, then we find an involution with one eigenspace of dimension e and one of dimension $d-e$, construct generating sets for $\mathrm{SO}^+(e,q)$ and $\mathrm{SO}^+(d-e,q)$, apply Algorithm `One` to the former, and Algorithm `Two` to the latter, and glue.

For $\epsilon \in \{-,0\}$, 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 Finding and constructing involutions

Our algorithms depend heavily on finding, by random search, elements of classical groups that satisfy certain conditions. For example, we search for elements that power to certain types of involution, for elements that give rise to the “odd order” case of the algorithm of [8], and for elements in a subgroup of the direct product of two classical groups that will power to the identity in one copy and a suitable element in the other.

To estimate the proportion of elements that will power to a suitable involution or other desired element, the first step is to estimate the proportion of elements whose characteristic polynomial has a unique irreducible factor of a given degree, which we do rather accurately. Given this analysis, it is easy to obtain our estimates.

One important case is when we are seeking an element that powers to a strong involution. As mentioned in the introduction, Lübeck *et al.* [30] recently proved that the proportion of elements of a group of Lie type of Lie rank d in odd characteristic that power up to a strong involution is at least $c/\log d$ for an explicit constant c.

In Table 3 we summarise the various types of involution that we need, and give a lower bound to the proportion of elements of the group in question that power up to an involution of the given type. For strong involutions, one could replace the bounds given here by these better bounds. We include our bounds for the sake of completeness since they follow easily from results that we need in Section 11.

Recall from Section 2 that the eigenspaces of an involution are denoted by E and F, where E has dimension e, or by E_+ and E_- where these are respectively the $+1$ and -1-eigenspaces of the involution. If e is required to be the dimension of E_-, then we write e_- for e. If G is a symplectic group or an orthogonal group of $+$ or $-$ type, then clearly d and e must be even; also e_- is always even as the involution must have determinant 1. If G is an orthogonal group of type 0, then d is odd. We assume $d > e$. These restrictions on d and e are omitted from Table 3. The type of an eigenspace in an orthogonal group is the type $+$, $-$ or 0, of the form restricted to the eigenspace.

The first entry in Table 3 identifies the group G, the second entry gives restrictions on the involution, and the third entry gives a lower bound to the proportion of elements of G that power to an involution satisfying these restrictions. This lower bound is generally conservative.

Since the precise lower bounds for many of the entries are complicated, we summarise these in Table 3 using notation of the form $(c/d)(1 + O(1/q))$ where c is a specified constant. However, we stress that the actual results are in all cases strictly positive, and more precise bounds are specified in the corresponding statements, or can readily be derived from these.

The first objective of this section is to prove the following theorem.

Theorem 8.1 *The proportion of elements of the group named in the first entry of any row in Table 3 that are of even order, and power to an involution whose eigenspaces satisfy the conditions imposed in the second entry, is at least the value given in the third entry, and is strictly positive.*

The theorem will be proved in stages. We commence our analysis with $\mathrm{GL}(d, q)$.

8.1 The general linear group

We estimate the proportion of elements of $\mathrm{GL}(d, q)$ that power to an involution having an eigenspace of specified dimension within a given range.

Lemma 8.2 *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: Let k denote the number of such polynomials. We use the inclusion-exclusion principle to count the number of elements of $\mathrm{GF}(q^e)$ that do not lie in any maximal

Group	Conditions	Proportion
$\mathrm{SL}(d,q)$	$e_- \in (d/3, 2d/3]$	$(1/(2d))(1+O(1/q))$
$\mathrm{SL}(d,q)$	$d \equiv 2 \bmod 4$, $e = 2$	$(1/(2d))(1+O(1/q))$
$\mathrm{SL}(d,q)$	d odd, $e = 3$	$(1/(3d))(1+O(1/q))$
$\mathrm{Sp}(d,q)$	d even, $e_- \in (d/3, 2d/3]$	$(3/(4d))(1+O(1/q))$
$\mathrm{Sp}(d,q)$	$d \equiv 2 \bmod 4$, $e = 2$	$(1/(2d))(1+O(1/q))$
$\Omega^+(d,q)$	$q \equiv 1 \bmod 4$, $e_- \in (d/3, 2d/3]$ E and F of $+$ type	$(3/(4d))(1+O(1/q))$
$\Omega^+(d,q)$	$q \equiv 3 \bmod 4$, $e_- \in (d/3, 2d/3]$ $e_- \equiv 0 \bmod 4$, E and F of $+$ type	$(3/(4d))(1+O(1/q))$
$\Omega^+(d,q)$	$q \equiv 3 \bmod 4$, $d \bmod 8 \neq 0$ $e = d \bmod 8$, E and F of $+$ type	$(1/(2d))(1+O(1/q))$
$\Omega^-(d,q)$	$q \equiv 1 \bmod 4$, $d \geq 6$, $e = 4$ F of $+$ type	$(1/(4d))(1+O(1/q))$
$\Omega^-(d,q)$	$q \equiv 3 \bmod 4$, $d \equiv 0 \bmod 4$, $e_+ = 4$ F of $+$ type	$(1/(4d))(1+O(1/q))$
$\Omega^-(d,q)$	$q \equiv 3 \bmod 4$, $d \equiv 2 \bmod 4$, $e = 6$ F of $+$ type	$(1/(4d))(1+O(1/q))$
$\Omega^-(6,q)$	$q \equiv 3 \bmod 4$, $e = 2$, F of $+$ type	$1/8 + O(1/q)$
$\Omega^0(5,q)$	$q \equiv 3 \bmod 4$, $q > 3$, $e_+ = 1$ F of $+$ type	$3/4 + O(1/q)$
$\Omega^0(d,q)$	$q \equiv 1 \bmod 4$ or $d \equiv 3 \bmod 4$, $e = 3$ F of $+$ type	$(1/(4d))(1+O(1/q))$
$\Omega^0(d,q)$	$q \equiv 3 \bmod 4$, $d \equiv 1 \bmod 4$, $e = 5$ F of $+$ type	$(3/(16d))(1+O(1/q))$
$\mathrm{SO}^+(d,q)$	$e_- \in (d/3, 2d/3]$, E and F of $+$ type	$(3/(4d))(1+O(1/q))$
$\mathrm{SO}^-(d,q)$	$e = 4$, F of $+$ type	$(3/(8d))(1+O(1/q))$
$\mathrm{SO}^0(d,q)$	$e = 3$, F of $+$ type	$(1/(8d))(1+O(1/q))$
$\mathrm{SU}(d,q)$	$e_- \in (d/3, 2d/3]$	$(3/(4d))(1+O(1/q))$
$\mathrm{SU}(d,q)$	$d \equiv 2 \bmod 4$, $e = 2$	$(1/(2d))(1+O(1/q))$
$\mathrm{SU}(d,q)$	d odd, $e = 3$	$(1/(6d))(1+O(1/q))$

Table 3: Elements of even order and lower bounds on proportions

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

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

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 $k = (q^e - q)/e \geq q^e(1 - q^{-1})/e$, with equality if $e = 2$. Now suppose that e is composite, and let ℓ denote the largest prime dividing e. Hence, 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 8.3 *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 $(q^e - 1)/e \geq (q - 1)k(a) \geq q^e(1 - q^{-1})/e$ if $e > 2$. If $e = 2$, then $k(a) = (q \pm 1)/2$.*

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, then 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 8.2,

$$(q^e - 1)/(q - 1) > ek(a) > (q^e - 1)/(q - 1) - \sum_i q^{e/p_i} + \sum_{i<j} q^{e/p_ip_j} - \cdots$$

For the lower bound, we take the number of elements of $\mathrm{GF}(q^e)$ of norm a, and subtract 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 $ek(a) \geq q^{e-1} > q^{e-1}(1 - q^{-1})$, giving the required lower bound. □

Lemma 8.4 *Let $e > d/2$ and $d \geq 4$. The proportion of elements of $\mathrm{GL}(d, q)$ whose characteristic polynomial has an irreducible factor of degree e lies between $(1/e)(1-q^{-1})$ and $1/e$, and is independent of d. Moreover, the number of elements of $\mathrm{GL}(d, q)$ whose characteristic polynomial is a multiple of a given irreducible polynomial f of degree e depends only on e and not on f.*

Proof: Let the characteristic polynomial of $g \in \mathrm{GL}(d, q)$ have an irreducible factor $h(x)$ of degree e. Then the kernel of $h(g)$ 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 8.2. Hence $k_1k_2k_3k_4k_5 = |\mathrm{GL}(d,q)| \times k_2/(q^e-1)$. The result follows. □

Lemma 8.5 *Let $e \in (d/3, d/2]$ and $d \geq 4$. 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 $[e^{-1}(1-q^{-1}) - e^{-2}(1-q^{-1})^2, e^{-1}-e^{-2}]$. Moreover, the number of elements of* $\mathrm{GL}(d,q)$ *whose characteristic polynomial is a multiple of a given irreducible polynomial f of degree e depends only on e and not on f.*

Proof: This proportion may be estimated as in the proof of Lemma 8.4, 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 $(1/e)(1-c/q) - (1/e^2)(1-c/q)^2$, where c lies in the interval $[0,1]$. □

Lemma 8.6 *The proportion of elements of* $\mathrm{GL}(d,q)$ *whose characteristic polynomial is irreducible, and with a specified determinant, lies in the interval $((dq)^{-1}, d^{-1}(q-1)^{-1}]$ if $d > 2$ and is $d^{-1}(q \pm 1)^{-1}$ if $d = 2$.*

Proof: The proportion is $k(a)/(q^d-1)$, where a is the determinant in question, and $k(a)$ is defined and estimated in Lemma 8.3. □

8.2 The special linear group

We now show how the results of Section 8.1 must be adjusted if $\mathrm{GL}(d,q)$ is replaced by $\mathrm{SL}(d,q)$.

Lemma 8.7 *The proportion in Lemma* 8.4 *is unaltered if* $\mathrm{GL}(d,q)$ *is replaced by* $\mathrm{SL}(d,q)$*, provided that $e < d$.*

Proof: Since $e < d$, the number of elements of $\mathrm{SL}(d,q)$ 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. □

Lemma 8.8 *The proportion in Lemma* 8.5 *is unaltered if* $\mathrm{GL}(d,q)$ *is replaced by* $\mathrm{SL}(d,q)$*, provided that* $e < d/2$.

Proof: The proof is similar to that of Lemma 8.7. □

Lemma 8.9 *The proportion of elements of* $\mathrm{SL}(2e,q)$ *whose characteristic polynomial has a unique irreducible factor of degree* e *lies in the interval* $[e^{-1}(1-q^{-1}) - e^{-2}(1-q^{-1}), e^{-1} - e^{-2}(1-q^{-1})^2)$. *Moreover, the number of elements of* $\mathrm{SL}(2e,q)$ *whose characteristic polynomial is a multiple of a given irreducible polynomial* f *of degree* e *depends only on* e *and not on* f.

Proof: The proportion in question is $\alpha(1-(q-1)\beta)$, where Lemma 8.4 implies that $\alpha \in [e^{-1}(1-q^{-1}), e^{-1}]$, and Lemma 8.6 implies that $\beta \in (1/(eq), 1/(e(q-1))]$ if $e > 2$ and $\beta = 1/(e(q \pm 1))$ if $e = 2$. Thus the proportion lies in the given interval. □

If n is an integer, then we write $v_2(n)$ for the 2-adic value of n; so $2^{v_2(n)}$ is the largest power of 2 that divides n.

Lemma 8.10 *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. Now $(q^m - 1)/(q^n - 1)$ is the sum of k powers of q^n, and so is odd. □

Lemma 8.11 *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 follows that $v_2(q^{2^u} + 1) = 1$. □

We now obtain a lower bound to the proportion of $g \in \mathrm{SL}(d,q)$ such that g has even order $2n$, and g^n has an eigenspace with specified dimension in a given range.

Theorem 8.12 *Let* $d \geq 4$. *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 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 8.7, 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, by Lemma 8.8, is at least $(e^{-1}-e^{-2})(1-q^{-1})$ if $d/2 > e > d/3$. If $e = d/2$, then, by Lemma 8.9, the proportion is at least $(e^{-1}-e^{-2})(1-q^{-1}) \geq d^{-1}(1-q^{-1})$. Thus the proportion is at least $d^{-1}(1-q^{-1})$ in all cases.

Suppose now that the characteristic polynomial of g has 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 $\mathrm{GF}(q)$: namely, we map 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 do not distinguish among 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 more than half of the elements of T have order a multiple of 2^x.

The result follows, and covers the first row of Table 3. □

We now deal with the other cases of $\mathrm{SL}(d,q)$ in Theorem 8.1.

Lemma 8.13 *Let $1 < e < d-1$, where $v_2(e) \neq v_2(d-e)$. Of the elements of $\mathrm{SL}(d,q)$, the proportion that are of even order and power to an involution with an eigenspace of dimension e is at least $(1-q^{-1})^2/(e(d-e))$ if $2 < e < d-2$ and is at least $(1-q^{-1})(1-2(q+1)^{-1})/(e(d-e))$ if $e \in \{2, d-2\}$.*

Proof: We look for elements of $\mathrm{SL}(d,q)$ with one irreducible factor of degree e, and one of degree $d-e$. The proportion of elements of $\mathrm{SL}(d,q)$ with this property is $\pi := (q-1)\sum_{a\in \mathrm{GF}(q)^\times} \alpha(a)\beta(a)$, where $\alpha(a)$ is the proportion of elements of $\mathrm{GL}(e,q)$ that have an irreducible characteristic polynomial with constant term a, and $\beta(a)$ is the proportion of elements of $\mathrm{GL}(d-e,q)$ that have an irreducible characteristic polynomial with constant term a^{-1}. Lemma 8.6 implies that $\pi > (1-q^{-1})^2/(e(d-e))$ if $2 < e < d-2$ and $\pi > (1-q^{-1})(1-2(q+1)^{-1})/(e(d-e))$ if $e \in \{2, d-2\}$. If $g \in \mathrm{SL}(d,q)$ has this property, and if u and w are eigenvalues (in an algebraic closure of $\mathrm{GF}(q)$) of the restriction of g to the e and $d-e$-dimensional g-invariant subspaces of V, then $u^{(q^e-1)/(q-1)} = a$ and $w^{(q^{d-e}-1)/(q-1)} = a^{-1}$, for some $a \in \mathrm{GF}(q)^\times$. Since $v_2(e) \neq v_2(d-e)$, the orders of the restriction of g to these two spaces have unequal

2-adic values; and so g powers to an involution whose -1-eigenspace has dimension e if $v_2(e) > v_2(d-e)$, and dimension $d-e$ if $v_2(e) < v_2(d-e)$. This covers the second and third rows in Table 3. $\Box$

8.3 The symplectic and orthogonal groups

We now turn to the symplectic and orthogonal groups. If $h(x) \in \mathrm{GF}(q)[x]$ is a monic polynomial with non-zero constant term, then 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 8.14 *Let $g \in \mathrm{SL}(2n, q)$, where $n > 1$, have characteristic polynomial $f(x) = h(x)\tilde{h}(x)$, where $h(x) \neq \tilde{h}(x)$ is irreducible. Let c be the constant term of $h(x)$. Then g preserves a non-degenerate orthogonal form on the underlying space, and every such form is of $+$ type. As an element of the corresponding orthogonal group, g has spinor norm $c \bmod U^2$, where U is the multiplicative group of $\mathrm{GF}(q)$.*

Proof: Clearly g preserves an orthogonal 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. The spinor norm of g may be calculated using the definition in [41, p. 444]. This definition gives the spinor norm as the product of two terms in U/U^2. The first term is the discriminant of the quadratic form restricted to the maximum subspace W of V on which $1+g$ acts nilpotently. Since, by hypothesis, -1 is not an eigenvalue of g, this term vanishes. The second term is $\det((1+g)/2)$ restricted to the orthogonal complement of W, modulo U^2; but here $W = 0$. 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 $\mathrm{GF}(q)$. Thus $\det(1+g) = N(1+a)N(1+a^{-1})\,U^2 = N(1+a)^2N(a^{-1})\,U^2 = c\,U^2$. $\Box$

Corollary 8.15 *The proportion of elements of $\mathrm{SO}^+(2n, q)$, for $n > 1$, and $q > 3$ if $n = 2$, whose characteristic polynomial is the product of two distinct irreducible polynomials, each the reverse of the other, divided by the proportion of such elements in $\Omega^+(2n, q)$, is 1 if n is odd, lies in the interval $(1, 1 + 2/(q^{n/2} - 3))$ if n is a power of 2, and in the interval $(1, 1 + 2/(q^{n/2} - 6))$ otherwise.*

Proof: Lemma 8.14 implies that the ratio in question equals the number of irreducible polynomials of degree n over $\mathrm{GF}(q)$ not equal to their reverses, divided by twice the total number of such polynomials whose constant terms are squares.

Suppose first that n is odd. An irreducible polynomial of odd degree (greater than 1) cannot be equal to its reverse; so this ratio is the number of elements of $\mathrm{GF}(q^n)$

that lie in no proper subfield containing $\mathrm{GF}(q)$ divided by twice the number of such elements whose norm (under the norm map from $\mathrm{GF}(q^n)$ to $\mathrm{GF}(q)$) is a square. But exactly half the non-zero elements of every subfield of $\mathrm{GF}(q^n)$ containing $\mathrm{GF}(q)$ are mapped to squares, since n is odd, and the result follows in this case.

Now suppose that n is a power of 2. The proportion is now changed, since every element of $\mathrm{GF}(q^{n/2})$ has square norm, as does every element of $\mathrm{GF}(q^n)$ whose minimum polynomial is equal to its reverse, these latter being the elements of order dividing $q^{n/2}+1$. The set of elements of $\mathrm{GF}(q^n)^\times$ that do not lie in $\mathrm{GF}(q^{n/2})$, and whose order does not divide $q^{n/2}+1$, is of cardinality $q^n-2q^{n/2}+1$. Since all elements of $\mathrm{GF}(q^n)$ of non-square norm (that is to say, elements that are themselves not squares) lie in this set, the number of squares in this set is $q^n-2q^{n/2}+1-(q^n-1)/2=(q^n-4q^{n/2}+3)/2$. Thus the ratio in question is

$$q^n-2q^{n/2}+1 : q^n-4q^{n/2}+3 = q^{n/2}-1 : q^{n/2}-3 = 1+2/(q^{n/2}-3).$$

Note that $\Omega(4,3)$ has no elements of the required type, reflecting the fact that $q^{n/2}-3=0$ if $n=2$ and $q=3$.

Now suppose that n is even, but not a power of two. Consider the following disjoint subsets of $\mathrm{GF}(q^n)^\times$:

- A is the subset of elements that lie in $\mathrm{GF}(q^{n/r})$ for some odd prime r;
- $B=\mathrm{GF}(q^{n/2})^\times \setminus A$;
- C is the subset of elements of order dividing $q^{n/2}+1$ that do not lie in $A\cup B$.

Half the elements of A have spinor norm 1, but all the elements of B and C have spinor norm 1. Thus the proportion in question is

$$\frac{|\mathrm{GF}(q^n)^\times|-|A|-|B|-|C|}{2(\frac{1}{2}|\mathrm{GF}(q^n)^\times|-\frac{1}{2}|A|-|B|-|C|)}=1+\frac{|B|+|C|}{|\mathrm{GF}(q^n)^\times|-|A|-2|B|-2|C|}.$$

Since A, B and C all have fewer than $q^{n/2}$ elements, and $n\geq 6$, this proportion is less than $1+2/(q^{n/2}-6)$. The result follows. □

The following result is an analogue of Lemma 8.4.

Lemma 8.16 *Let G be one of the groups $\mathrm{Sp}(2n,q)$, $\mathrm{SO}^+(2n,q)$, $\mathrm{SO}^-(2n,q)$, $\mathrm{SO}(2n+1,q)$. 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*

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

is independent of n, and hence is strictly positive. If $q=3$ and $m=2$, then the proportion is $1/16$. Moreover, the number of elements of G whose characteristic polynomial is a multiple of a given irreducible polynomial f of degree m depends only on m and not on f.

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 $\tilde{h}(g)$ 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, ℓ_2 is the number of choices for V_0 given V_2, ℓ_3 is the number of irreducible monic polynomials $h(x)$ of degree m over $\mathrm{GF}(q)$ such that $h(x) \neq \tilde{h}(x)$, 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 $\mathrm{SX}(V_2^{\perp})$. The factor $1/2$ in the above expression arises since the symmetry between $h(x)$ and $\tilde{h}(x)$ ensures that every such element g is counted twice. In more detail:

$$\begin{aligned}
\ell_1 &= |\mathrm{GX}(V)|/|\mathrm{GX}(V_2) \times \mathrm{GX}(V_2^{\perp})| \\
\ell_2 &= |\mathrm{GX}(V_2)|/|\mathrm{GL}(V_0)| \\
\ell_3 &\sim q^m/m \\
\ell_4 &= |\mathrm{GL}(V_0)|/(q^m-1) \\
\ell_5 &= |\mathrm{SX}(V_2^{\perp})|.
\end{aligned}$$

These results are obtained as follows. By Witt's Theorem (see Theorem 2.1), $\mathrm{GX}(V)$ acts transitively on the 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 $h(x) \neq \tilde{h}(x)$. (If $h(x)$ is irreducible and of degree m, then $h(x) = \tilde{h}(x)$ if and only if m is even, and $a^{-1} = a^{q^{m/2}}$ for every zero a of $h(x)$ in $\mathrm{GF}(q^m)$. This could be used to obtain an exact formula for ℓ_3.) The estimate for $k(a)$ in Lemma 8.2 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 product of the ℓ_i is $\ell_3|G|/(q^m-1)$, and the result follows. □

The detail of adding 1 to the lower bound, proved by observing that at least one of these polynomials is reducible, ensures that the stated lower bound is strictly positive in all cases: it is the precise value, namely 1, when $q = 3$ and $m = 2$, the polynomial in question being $x^2 + x + 2$.

Lemma 8.17 *Let G be as in the previous lemma, and let $m \in (n/3, n/2]$, and $m < n/2$ if G is $\mathrm{SO}^-(2n,q)$. Let S denote the set of elements of G whose characteristic polynomial has exactly two distinct irreducible factors of degree m, each the reverse of the other. Then*

$$\frac{|S|}{|G|} = \frac{1}{2}\frac{\ell_3}{q^m-1} - \frac{1}{4}\left(\frac{\ell_3}{q^m-1}\right)^2$$

where $m^{-1}(q^m-1) > \ell_3 \geq m^{-1}q^m(1-q^{-1}) - q^{\lfloor m/2 \rfloor} + 1$. In particular,

$$\frac{|S|}{|G|} = \left(\frac{1}{2m} - \frac{1}{4m^2}\right)(1 + O(1/q)).$$

If $G = \mathrm{SO}^-(2n,q)$ and $m = n/2$, so n is even, then

$$\frac{|S|}{|G|} = \frac{1}{2}\frac{\ell_3}{q^m-1} = \left(\frac{1}{2m}\right)(1 + O(1/q)).$$

Proof: The proof is similar to that of Lemma 8.5. The case $G = \mathrm{SO}^-(2n,q)$ and $m = n/2$ is exceptional: G cannot have two pairs of distinct irreducible mutually reverse factors of degree $n/2$. □

Lemma 8.18 *If $m < n$, then Lemmas* 8.16 *and* 8.17 *apply essentially unchanged when $\mathrm{SO}^\pm(2n,q)$ is replaced by $\Omega^\pm(2n,q)$.*

Proof: Suppose first that $m > n/2$. In the notation of Lemma 8.16 let $G = \Omega(V)$. The restriction of $g \in G$ to V_2 and to $V_2^\perp$ must have equal spinor norms. But exactly half the elements of $\mathrm{SO}(V_2^\perp)$ have spinor norm 1, so the proportion of elements g satisfying the required condition is exactly the same in $\Omega(V)$ as in $\mathrm{SO}(V)$. Similarly, the proportions are exactly equal if $n/3 < m < n/2$.

This leaves the case $m = n/2$, so n is even. If $G = \Omega^-(2n,q)$, then the above argument still applies, for the same reason that $\mathrm{SO}^-(2n,q)$ was an exceptional case in Lemma 8.17. If $G = \Omega^+(2n,q)$, then we need to exclude from our count those elements of $\Omega^+(2n,q)$ whose restriction to $V_2^\perp$ has a characteristic polynomial that is the product of two distinct irreducible factors, each the reverse of the other. Corollary 8.15 implies that the required proportion is obtained by dividing the proportion given in Lemma 8.17 by a factor in the interval $(1, 1 + 2/(q^{n/2} - 3))$ if n is a power of 2, and in $(1, 1 + 2/(q^{n/2} - 6))$ otherwise. □

We now obtain the analogue of Theorem 8.12.

Theorem 8.19 *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 $n \geq 3$. The proportion of elements of G that power to an involution with -1-eigenspace having dimension in the range $(2n/3, 4n/3]$ is greater than $m^{-1}(1-q^{-1})/4 - q^{-\lceil m/2 \rceil/4}$ where $m = \lfloor 2n/3 \rfloor$, and is always positive. If G is orthogonal, then the -1-eigenspace of the involution supports a form of $+$ type.*

Proof: Using Lemmas 8.16, 8.17 and 8.18, the proof is similar to that of Theorem 8.12.

Let 2^k be the unique power of 2 in the range $(2n/3, 4n/3]$, so $k \geq 2$. We look for an element g of G whose characteristic polynomial has a unique pair of factors $h(x)$ and $\tilde{h}(x)$, where $h(x) \neq \tilde{h}(x)$ is irreducible of degree 2^{k-1}, and consider the probability that g will power to an involution whose -1-eigenspace has dimension 2^k. If U is the null space of $h(g)\tilde{h}(g)$, then the restriction of g to U has order dividing $q^{2^k} - 1$, and so, with probability slightly greater than 1/2, the 2-adic value of the order of g restricted to U will be $v_2(q^{2^k} - 1)$. Now V, regarded as a module for $\mathrm{GF}(q)[C]$, where C is the cyclic group generated by g, has a series $V = V_1 > V_2 > \cdots$, where the characteristic polynomial of g acting on V_i/V_{i+1} is either the product of two distinct irreducible factors $h_i(x)$ and $\tilde{h}_i(x)$, or an irreducible polynomial $f_i(x)$ with $f_i(x) = \tilde{f}_i(x)$. Let n_i denote the dimension of V_i/V_{i+1}. In the former case n_i is even and the order of g acting on V_i/V_{i+1} divides $q^{n_i/2} - 1$. Also, by assumption, $n_i \neq 2^k$, and so $v_2(n_i) < v_2(2^k)$, and $v_2(q^{n_1/2} - 1) < v_2(q^{2^{k-1}} - 1)$. In the latter case n_i is even or $n_i = 1$. If n_i is even, then the order of g acting on V_i/V_{i+1} divides $q^{n_i/2} + 1$, and if $n_i = 1$ this order is ± 1. Hence, in any case, the 2-adic value of this order is less than $v_2(q^{2^{k-1}} - 1)$. It follows that g will power to an involution with -1-eigenspace equal to U if the order of the restriction of g to U has 2-adic value equal to $v_2(q^{2^{k-1}} - 1)$. The proportion of elements g of G satisfying the conditions now imposed on g may be estimated using Lemmas 8.16 and 8.17. The proportion given by these lemmas, for $m \in (n/3, 2n/3]$, is least when m is the integral part of $2n/3$. Thus the proportion of elements g of G satisfying all the conditions imposed on g is greater than $m^{-1}(1-q^{-1})/4 - q^{-\lceil m/2 \rceil}/4$ where $m = \lfloor 2n/3 \rfloor$.

Note that the proportion of elements satisfying the conditions imposed on g if $G = \mathrm{SO}(V)$ is exactly the same as the proportion if $G = \Omega(V)$. The restriction of g to $U^\perp$ must be chosen to have the same spinor norm as the restriction of g to U, and half the elements of $\mathrm{SO}(U^\perp)$ will have this property.

If G is orthogonal, then the -1-eigenspace of the involution obtained by powering g supports a form of $+$ type, since the form restricted to the kernel of $h(g)$, or of $\tilde{h}(g)$, is null.

Thus the entries in Table 3 for orthogonal and symplectic groups that require e_- to lie in the range $(d/3, 2d/3]$ are valid. □

Observe that the dimension of U in the proof is a power of 2, and is at least 4. Thus the theorem is compatible with the fact that $\Omega^\epsilon(2n, q)$ does not have an involution whose -1-eigenspace is an odd multiple of 2 if both $q \equiv 3 \bmod 4$ and $\epsilon = +$, or if both $q \equiv 1 \bmod 4$ and $\epsilon = -$.

Theorem 8.20 *The remaining entries in Table* 3 *for orthogonal and symplectic groups are valid.*

Proof: Consider first the case where $d - e$ is even and $d > 2e$. Let S be the set of elements of such a group G whose characteristic polynomial contains two distinct irreducible factors $h(x)$ and $\tilde{h}(x)$, where $\tilde{h}(x)$, the reverse of $h(x)$, is not equal to $h(x)$, and where h has degree $(d-e)/2$. Lemma 8.16 implies that the proportion of elements of G with this property is $(1/(d-e))(1+O(1/q))$ and is positive for all values of q. It is a straightforward, if tedious, exercise to use the explicit lower bound given there to obtain explicit bounds for the proportions stated here.

It remains to estimate the probability that the 2-adic value of the order of such an element g restricted to the null space U of $h(g)\tilde{h}(g)$ is greater than the 2-adic value of the order of its restriction to $U^{\perp}$, since in this case g will power to an involution with -1-eigenspace $F = U$ and $+1$-eigenspace $E = F^{\perp}$. If the form is orthogonal, then the restriction of the form to F is either required or permitted to be of $+$ type.

If $G = \Omega(V)$, then the spinor norms of g restricted to E and to F must be equal. It is easy to see that the proportion of elements of G that satisfy the conditions imposed on g is higher when g is required to have spinor norm -1 in both E and F than when g is required to have spinor norm $+1$ in these spaces. This is because the condition that h be irreducible and not equal to its reverse excludes a higher proportion of polynomials whose constant terms are squares than of general polynomials; more significantly, the 2-adic value of the order of such an element (restricted to F) takes its maximum value when the constant term of $h(x)$ is not a square.

Thus, if $G = \Omega(V)$, then we define T to be the subset of S consisting of elements that act on E and on F with spinor norm $+1$, and estimate the proportion of elements of T that power to a suitable involution.

Note that the order of the restriction of g to F has 2-adic value at most $v_2(q^{(d-e)/2}-1)$, and at most $v_2(q^{(d-e)/2}-1)-1$ in the orthogonal case if g restricted to F has spinor norm $+1$. Moreover, the proportion of elements of S or of T for which this value is achieved is greater than $1/2$.

Let π denote a lower bound to the probability that the 2-adic value of the order of the restriction of a random element of S (or of T if $G = \Omega(V)$) to F exceeds the 2-adic value of its restriction to E, so that the proportion of elements of G that power to an involution as required is greater than $(\pi/(d-e))(1+O(1/q))$, a bound we often replace with $(\pi/d)(1+O(1/q))$.

We now consider the individual cases in Table 3, where we use ad-hoc arguments to handle the exceptional cases.

- $G = \mathrm{Sp}(d,q)$, $d \equiv 2 \bmod 4$; $e = 2$.

  Now $v_2(q^{(d-e)/2}-1) \geq v_2(q^2-1)$, which is greater than the 2-adic value of the restriction of g to E; so $\pi > 1/2$.

- $G = \Omega^{+}(d,q)$, $d > 8$, $q \equiv 3 \bmod 4$, $d \bmod 8 \neq 0$; $e = d \bmod 8$, so $e < 8$; E and F of $+$ type.

  Now $v_2(q^{(d-e)/2}-1)-1 \geq v_2(q^4-1)-1$, and this is greater than the 2-adic value of the restriction of g to E; so $\pi > 1/2$.

- $G = \Omega^{-}(d,q)$, $q \equiv 1 \bmod 4$, $d \geq 6$; $e = 4$; F of $+$ type.

Suppose first that $d > 8$. Since $\Omega^-(4,q) \cong \mathrm{PSL}(2,q^2)$, the proportion of elements of $\Omega^-(4,q)$ of odd order is greater than $1/2$ (see [20, p. 288]), and so $\pi > 1/4$.

If $d \leq 8$, then our assumption that $d > 2e$ fails.

Suppose that $d = 6$. Consider elements g of G whose characteristic polynomials factorise as $f(x) = h(x)(x-\alpha)(x-\alpha^{-1})$, where $h(x) = \tilde{h}(x)$ is irreducible of degree 4, and the 2-adic value of the multiplicative order of α is greater than the 2-adic value of the order of g restricted to the kernel of $h(g)$. This latter order divides q^2+1, and hence has 2-adic value at most 1. Then the involution that is a power of g has -1-eigenspace the sum of the α and α^{-1} eigenspaces of g, which is, as required, of dimension 2 and of $+$ type. The proportion of elements of $\Omega^-(6,q)$ of this type, ignoring the restriction on the order of α, but excluding the cases $\alpha = \pm 1$, is $q - 3 : 4(q+1)$, and so, allowing for this restriction, the proportion of elements of G of the required type is greater than $1/8 + O(1/q)$.

Now suppose that $d = 8$. By the exceptional case of Lemma 8.18, the proportion of elements g of G whose characteristic polynomial has exactly two irreducible factors $h(x)$ and $\tilde{h}(x)$ of degree 2 that are the reverse of each other is $1/4 + O(1/q)$. Let g be a random element of T. Now g lies in $\mathrm{SO}(F) \times \mathrm{SO}(E)$, where F is the null space of $h(g)\tilde{h}(g)$, and the probability that g powers to a suitable involution is greater than $1/2$, since the largest possible value for the 2-adic value of the order of g restricted to F is greater than the corresponding value for E. This gives the required proportion of elements of G as greater than $1/8 + O(1/q)$.

- $G = \Omega^-(d,q)$, $q \equiv 3 \bmod 4$, $d \equiv 0 \bmod 4$; $e_+ = 4$; F is of $+$ type.

  This can be dealt with exactly as the previous case.

- $G = \Omega^-(d,q)$, $q \equiv 3 \bmod 4$, $d \equiv 2 \bmod 4$; $e = 6$; F of $+$ type.

  Assume first that $d > 2e$. The proportion of elements of $\Omega^-(6,q)$ of order not a multiple of 4 is easily seen to be at least $1/2 + O(1/q)$. But $v_2(q^{(d-6)/2} - 1) - 1 \geq v_2(q^2-1) - 1 \geq 2$, so $\pi > 1/4 + O(1/q)$. Now suppose that $d \leq 2e$, so $d = 10$. We argue as in the case $d > 10$, but use Lemma 8.17 rather than Lemma 8.16. This replaces the factor $1/(d-e)$ by $1/(d-e) - 1/(d-e)^2 = 1/4 - 1/16$. Since we simplify our estimates, replacing $1/(d-e)$ by $1/d$, this value is within our general bounds.

- $\Omega^-(6,q)$, $q \equiv 3 \bmod 4$; $e = 2$; F of $+$ type.

  $v_2(q^{(d-e)/2} - 1) - 1 = v_2(q^2-1) - 1 \geq 2$. The restriction of g to E has order dividing $(q+1)/2$; so $\pi > 1/2$.

- $G = \Omega^0(5,q)$, $q \equiv 3 \bmod 4$, $q > 3$; $e_+ = 1$; F of $+$ type.

  $v_2(q^{(d-e)/2} - 1) - 1 = v_2(q^2-1) - 1 \geq 2$, so $\pi > 3/4$.

- $G = \Omega^0(d,q)$, $q \equiv 1 \bmod 4$ or $d \equiv 3 \bmod 4$; $e = 3$; F of $+$ type.

Now $v_2(q^{(d-e)/2}-1)-1$ is at least $v_2(q^2-1)-1$ if $d \equiv 3 \bmod 4$, and is at least $v_2(q-1)-1$ if $q \equiv 1 \bmod 4$, and hence is at least 1 in either case. The proportion of elements of $\Omega(3,q) \cong \mathrm{PSL}(2,q)$ of odd order is greater than 1/2; so $\pi > 1/4 + O(1/q)$.

- $G = \Omega^0(d,q)$, $q \equiv 3 \bmod 4$, $d \equiv 1 \bmod 4$; $e = 5$; F of $+$ type.

  Suppose first that $d > 2e$. Then $v_2(q^{(d-e)/2}-1)-1 \geq v_2(q^2-1)-1 \geq 2$. Elements of $\mathrm{SO}(E)$ of order not a multiple of 4 include those whose characteristic polynomials are of the form $(x-1)f(x)$, where $f(x)$ is irreducible and $f(x) = \tilde{f}(x)$. Such elements correspond to equivalence classes, under the action of the group generated by the Frobenius map, of elements of $\mathrm{GF}(q^4)$ that do not lie in $\mathrm{GF}(q^2)$, and that are of order dividing q^2+1. Such elements have centralisers in $\mathrm{SO}(E)$ of order q^2+1, so the number of such elements is $|\mathrm{SO}(E)|(q^2-1)/(4(q^2+1))$. Thus the proportion of elements of $\mathrm{SO}(E)$ of order not a multiple of 4 is at least $1/4 + O(1/q^2)$, and the same applies to $\Omega(E)$; so $\pi > 1/8 + O(1/q)$.

  This leaves the case $d = 9$, $e = 5$. Again we proceed as when $d > 2e$, but use Lemma 8.17 rather than Lemma 8.16. This replaces the factor $1/(d-e)$ by $1/(d-e) - 1/(d-e)^2 = 1/4 - 1/9$. Since this is greater than 1/9, our stated lower bound holds.

- $G = \mathrm{SO}^-(d,q)$; $e = 4$; F of $+$ type.

  If $q \equiv 1 \bmod 4$ or $d \equiv 0 \bmod 4$, then the proportion is the same as for $\Omega^-(d,q)$, since $\mathrm{SO}^-(d,q) \cong \Omega^-(d,q) \times C_2$ in this case.

  Now consider $q \equiv 3 \bmod 4$. If $d = 6$, then the analysis is similar to that for $\Omega^-(d,q)$ when $q \equiv 1 \bmod 4$ and $e = 4$. The order of α may now be a multiple of 2, but not of 4. Hence the probability of the order condition being satisfied is now slightly greater then 1/4, and the proportion of elements of the type required is now greater than $1/16 + O(1/q)$. The case $d = 8$ is covered by Lemma 8.17. If $d > 8$ then $v_2(q^{(d-e)/2}-1) \geq v_2(q^2-1) \geq 3$, so $\pi > 3/8$.

- $G = \mathrm{SO}^0(d,q)$; $e = 3$; F is of $+$ type.

  Assume $d > 5$. Since $v_2(q^{(d-e)/2}-1) \geq v_2(q-1) \geq 1$, and the proportion of elements of $\mathrm{SO}(3,q)$ of odd order is greater than 1/4, it follows that $\pi > 1/8$.

  If $d = 5$, then we look for elements whose characteristic polynomial factorises as $(x-\alpha)(x-\alpha^{-1})(x-1)h(x)$, where $h(x) = \tilde{h}(x)$ is irreducible. The factor $(x-1)h(x)$ is the characteristic polynomial of an element of $\mathrm{SO}(3,q)$. We impose the condition $\alpha \neq \pm 1$. The proportion of such elements in $\mathrm{SO}(5,q)$ is $((q-3)/2)((q^2-1)/2) : (q-1)(q^2+1) = 1/4 + O(1/q)$. □

8.4 The unitary groups

We finally turn to the unitary groups. If $h(x) \in \mathrm{GF}(q^2)[x]$ is a monic polynomial with non-zero constant term, then define $\hat{h}(x)$ to be the monic polynomial obtained from $\tilde{h}(x)$ by raising each coefficient to the power q. We call $\hat{h}(x)$ the *hermitian reverse* of $h(x)$.

Lemma 8.21 *Let $\hat{\ell}_3 := \hat{\ell}_3(q,m)$ denote the number of irreducible monic polynomials of degree m over $\mathrm{GF}(q^2)$ that are not equal to their hermitian reverse. Then*

$$\frac{q^{2m}-1}{m} > \hat{\ell}_3 > \frac{q^{2m}(1-q^{-1})}{m}.$$

Proof: If m is even, then no irreducible monic polynomial is equal to its hermitian reverse, so $(q^{2m}-1)/m > \hat{\ell}_3 \geq q^{2m}(1-q^{-2})/m$ by Lemma 8.2. If m is odd, then the number of monic polynomials over $\mathrm{GF}(q^2)$ of degree m (reducible or not) that are equal to their hermitian reverse is $q^{m-1}(q+1)$, so $\hat{\ell}_3 > q^{2m}(1-q^{-2})/m - q^{m-1}(q+1) \geq q^{2m}(1-q^{-1})/m$. □

If m is odd, then the irreducible monic polynomials over $\mathrm{GF}(q^2)$ of degree m that are equal to their hermitian reverse define elements of $\mathrm{GF}(q^{2m})$ that lie in no proper subfield containing $\mathrm{GF}(q^2)$ and have order dividing $q^m + 1$. This could be used to obtain a precise formula for $\hat{\ell}_3$.

Lemma 8.22 *Let $G = \mathrm{SU}(d,q)$, and $m > d/4$. The proportion of elements of G whose characteristic polynomial has an irreducible factor of degree m that is not equal to its hermitian reverse lies in the interval $((1-q^{-1})/(2m), 1/(2m))$, and is independent of d. Moreover, the number of elements of G whose characteristic polynomial is a multiple of a given irreducible polynomial f of degree m depends only on m and not on f.*

Proof: The proof is almost identical to that of Lemma 8.16. The proportion is $\hat{\ell}_3/(2(q^{2m}-1))$, and the result then follows from Lemma 8.21. □

Lemma 8.23 *Let $G = \mathrm{SU}(d,q)$, and let $m \in (d/6, d/4)$. Let S denote the set of elements of G whose characteristic polynomial has exactly two distinct irreducible factors of degree m, each the hermitian reverse of the other. Then*

$$\frac{|S|}{|G|} = \frac{1}{2}\frac{\hat{\ell}_3}{q^{2m}-1} - \frac{1}{4}\left(\frac{\hat{\ell}_3}{q^{2m}-1}\right)^2$$

where $(q^{2m}-1)/m > \hat{\ell}_3 \geq q^{2m}(1-q^{-2})/m$. In particular,

$$\frac{|S|}{|G|} = \left(\frac{1}{2m} - \frac{1}{4m^2}\right)(1 + O(1/q^2)).$$

Lemma 8.24 *Let $G = \mathrm{SU}(4m, q)$. The proportion of elements of G whose characteristic polynomial has exactly two distinct irreducible factors of degree m, each the hermitian reverse of the other, lies in the interval*

$$\left(\frac{1}{2}\frac{\hat{\ell}_3}{q^{2m}-1} - \frac{1}{4}\left(\frac{\hat{\ell}_3}{q^{2m}-1}\right)^2 (1-q^{-2}), \frac{1}{2}\frac{\hat{\ell}_3}{q^{2m}-1} - \frac{1}{4}\left(\frac{\hat{\ell}_3}{q^{2m}-1}\right)^2 (1-q^{-2})^{-1}\right).$$

PROOF: This case is exceptional: the constant term of $h(x)\hat{h}(x)$, where $h(x)$ is the irreducible factor in question, need not be 1. Consider the excluded case when $g \in G$ has a characteristic polynomial with two pairs of hermitian reverse factors of degree m: there is a restriction on the constant terms of these polynomials, since G is the special unitary group. By Lemma 8.3, this restriction multiplies the number of excluded cases by a factor that lies between $1 - q^{-2}$ and $(1 - q^{-2})^{-1}$. □

Theorem 8.25 *Let $d \geq 3$. The proportion of elements of $\mathrm{SU}(d, q)$ that power to an involution whose -1-eigenspace has dimension in the range $(d/3, 2d/3]$ is at least $(3/(4d))(1 - q^{-1})$.*

PROOF: Using the three previous lemmas, the analysis is similar to that for the symplectic and orthogonal groups. □

There remain two unitary cases to consider.

- $G = \mathrm{SU}(d, q)$, $d \equiv 2 \bmod 4$; $e = 2$.

  The proportion of elements of G whose characteristic polynomial has an irreducible factor of degree $(d-2)/2$ not equal to its hermitian reverse lies in the interval $((1 - q^{-1})/(d-2), 1/(d-2))$, by Lemma 8.22. Such an element will power to an involution as required with probability greater than 1/2: observe $v_2(q^{(d-2)} - 1) > v_2(q^2 - 1)$ since $d \equiv 2 \bmod 4$.

- $G = \mathrm{SU}(d, q)$, d odd; $e = 3$.

  The proportion of elements g of G whose characteristic polynomial has two distinct irreducible hermitian reverse factors $h(x)$ and $\hat{h}(x)$, each of degree $(d-3)/2$, and a third irreducible factor $k(x)$ of degree 3, is $(1/(3d))(1 + O(1/q))$. Let E denote the null space of $k(g)$, and F the null space of $h(g)\hat{h}(g)$. The order of g restricted to E divides $q^3 + 1$, and hence is an odd multiple of $q + 1$. The order of g restricted to F divides $q^{d-3} - 1$, and hence divides $q^2 - 1$. Thus the probability that g will power to an involution as required is greater than 1/2. Thus the proportion of elements of G with the required property is at least $(1/(6d))(1 + O(1/q))$.

This completes the proof of Theorem 8.1.

8.5 Constructing an involution

We now analyse the cost of determining whether a given matrix powers to a suitable involution.

Lemma 8.26 *Given $g \in \mathrm{GL}(d,q)$, one can determine whether or not g is of even order, and in the affirmative case determine an integer n such that g^n is an involution, and find bases for the eigenspaces of this involution, using a Las Vegas algorithm having complexity $O(d^3 \log d + d^2 \log d \log\log d \log q)$ measured in field operations.*

Proof: Recall from Lemma 2.7 that the characteristic polynomial $f(t)$ of g can be computed in $O(d^3 \log d)$ 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 in $O(d^2 \log d \log\log d \log q)$ field operations.

Let the 2-part of the order of $t + (f_i(t))$ in the group of units of $\mathrm{GF}(q)[t]/(f_i(t))$ be 2^{x_i}. To compute x_i, we first raise $t + (f_i(t))$ to the power a_i, where a_i is the odd part of $q^{\deg(f_i)} - 1$; now x_i is the number of times that the resulting field element needs to be squared to give rise to the identity. Computing t^k in any ring requires at most $2 \log k$ ring operations, and k is at most q^d, so this can be carried out in $O(d^2 \log d \log\log d \log q)$ field operations.

If $x := \max_i(x_i) = 0$, then g has odd order. Otherwise, n is $2^{x-1} \cdot \prod_i a_i \cdot p^{\max_i \{n_i\}}$, where $\mathrm{GF}(q)$ has characteristic p. Let $I = \{i : x_i = x\}$. Clearly the dimension of the -1-eigenspace of g^n is $\sum_{i \in I} n_i d_i$, where d_i is the degree of $f_i(t)$.

To obtain the bases for the eigenspaces, we compute g^n using the algorithm of Lemma 10.1, and evaluate the appropriate nullspaces. The claim follows. □

Observe that we learn the dimension of the -1-eigenspace of g^n without evaluating g^n, and so can decide if g^n is a strong or suitable involution without computing its eigenspaces.

We now summarise the results of Section 8.

Theorem 8.27 *There is a Las Vegas algorithm that takes as input a generating set X for G, where G is the first entry in a row in Table 3, and returns an SLP in X for $g \in G$ that powers to an involution whose eigenspaces satisfy the conditions imposed in the second entry, together with bases for these eigenspaces, and an integer n such that g^n is the involution in question. This algorithm takes $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ field operations.*

8.6 Two related results on orthogonal groups

We conclude with two results of a flavour similar to the other results of Section 8. These guarantee that the search in Step 3 of `OneOmegaPlus3` and `OneOmegaMinus3` terminates in $O(n)$ random selections.

Lemma 8.28 *If $q \equiv 3 \bmod 4$, then the proportion of elements of $\mathrm{SO}^+(2n,q)$ that are of twice odd order and have spinor norm -1 is $1/8$ if $n = 2$, and is greater than $(2n-2)^{-1}(1-q^{-1})/2 - q^{-n/2}/4$ if $n > 2$.*

Proof: Suppose first that $n = 2$. Let D denote the subgroup of $\mathrm{GL}(2,q)$ consisting of elements of determinant ± 1. Then $\mathrm{SO}^+(4,q)$ is the section of $D \times D$ obtained by taking the subgroup consisting of pairs of elements with equal determinants, and amalgamating the centres; $\Omega^+(4,q)$ is the subgroup of $\mathrm{SO}^+(4,q)$ obtained from elements of $D \times D$ whose entries in each factor have determinant 1. Thus an element of $\mathrm{SO}^+(4,q)$ of twice odd order and spinor norm -1 arises from an element (g_1, g_2) of $D_1 \times D_2$ where each of g_1 and g_2 has determinant -1, and has twice odd order. Thus each g_i is conjugate to a diagonal matrix with eigenvalues ω and $-\omega^{-1}$ for some ω in $\mathrm{GF}(q)^\times$. This gives rise to $(q-1)/2$ conjugacy classes (in $\mathrm{GL}(2,q)$) of size q^2+q, and hence $(q-1)q(q+1)/2$ choices for g_i. Squaring this gives $|\mathrm{SO}^+(4,q)|/4$. Since the centres of the two copies of D are amalgamated, the proportion in question is $1/8$.

Now suppose that $n > 2$. By Lemma 8.16, the proportion π of elements g of $\mathrm{SO}^+(2n,q)$ whose characteristic polynomial has an irreducible factor $h(x) \neq \tilde{h}(x)$ of degree $n-1$ lies in the interval $((2n-2)^{-1}(1-q^{-1}) - q^{-n/2}/2, 1/(2n-2))$. Since $q^{n-1}+1 \equiv 2 \bmod 4$, these elements, restricted to the null space of $h(g)\tilde{h}(g)$, are either of odd order, or of twice odd order; and the restriction of g to this null space has spinor norm -1 if and only if the restriction is of even order. Moreover, g acts on the orthogonal complement of the null space as an element of $\mathrm{SO}^+(2,q)$. This is a cyclic group of twice odd order, the elements with spinor norm -1 (in their action on this 2-dimensional space) being those of even order. Thus the proportion of elements of $\mathrm{SO}^+(2n,q)$ whose characteristic polynomial satisfies the above condition and have spinor norm -1 (and necessarily have twice odd order) is $\pi/2$. □

Lemma 8.29 *If $q \equiv 3 \bmod 4$, then the proportion of elements of $\mathrm{SO}^-(2n,q)$ that are of twice odd order and have spinor norm -1 is at least $1/(4n) + O(1/q)$, and is strictly positive.*

Proof: The case $n = 1$ being trivial, suppose first that $n = 2$. Now $\mathrm{SO}^-(4,q) \cong C_2 \times \mathrm{PSL}(2,q^2)$. The proportion of elements of $\mathrm{PSL}(2,q^2)$ of odd order is greater than $1/2$ (see [20, p. 288]). Thus the proportion of elements of $\mathrm{SO}^-(4,q)$ of spinor norm -1 and of twice odd order is greater than $1/4$.

If $n > 2$ is odd, then we consider elements g of $\mathrm{SO}^-(2n,q)$ whose characteristic polynomial $f(x)$ is irreducible, and hence satisfy the condition $f(x) = \tilde{f}(x)$. Such elements preserve an irreducible form of $-$ type, and have order dividing q^n+1, which is twice odd. Since $-I_{2n}$ has spinor norm -1, it follows that g has spinor norm -1 if and only if g is of even order. Hence the proportion of elements of $\mathrm{SO}^-(2n,q)$ satisfying these conditions is $1/(4n) + O(1/q)$.

If $n > 2$ is even, then we consider elements of $\mathrm{SO}^-(2n,q)$ whose characteristic polynomial has two irreducible factors $f(x)$ and $\tilde{f}(x)$, each of degree $n-1$. Again these elements have order not divisible by 4. The proportion of such elements having spinor norm -1 (and hence of twice odd order) is exactly $1/2$. Hence the proportion of elements of this type is $1/(4n-4)+O(1/q)$, as required. □

Lemma 8.28 implies that the proportion of elements g of H considered in Step 3 of `OneOmegaPlus3`, is greater than $(4f-2)^{-1}(1-q^{-1}-q^{-f})/4$. Lemma 8.29 implies that the corresponding proportion in Step 3 of `OneOmegaMinus3` is greater than $1/(4n)+$ $\mathrm{O}(1/q)$.

9 Involutions with eigenspaces of equal dimension

Let G be one of the following: $\mathrm{SL}(4n,q)$, $\mathrm{Sp}(4n,q)$, $\mathrm{SU}(4n,q)$, $\Omega^+(4n,q)$ if $q \equiv 1 \bmod 4$, $\Omega^+(8n,q)$ if $q \equiv 3 \bmod 4$, or $\mathrm{SO}^+(4n,q)$. We describe an algorithm to construct an involution in G with both eigenspaces of the same dimension. We use this as one component in Algorithm `Two`.

Our algorithm is more general in nature: it constructs an involution, each of whose eigenspaces has a specified dimension. If G is orthogonal, then the eigenspaces must support forms of $+$ type; hence the dimension of the -1-eigenspace must always be even, and a multiple of 4 if $G=\Omega^+(d,q)$ and $q \equiv 3 \bmod 4$.

Consider first the case where $G=\mathrm{SL}(d,q)$. We outline an algorithm to construct an involution with -1-eigenspace of dimension e where $0 \le e < d$. Its design ensures that recursive calls involve matrices having dimension at most $2d/3$.

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, E_- and E_+ respectively, of h_1.

3. If $r=e$ then return the involution h_1.

4. Construct the centraliser in G of h_1. Obtain generators for $\mathrm{SL}(E_-)$ and for $\mathrm{SL}(E_+)$ as subgroups of G. (See Sections 11 and 12 for details of the algorithms used.)

5. Consider the case where $s \le e < r$. By recursion, find in $\mathrm{SL}(E_-)$ an involution whose -1-eigenspace has dimension e.

6. Consider the case where $e \le \min(r,s)$. If $r<s$, then, by recursion, find in $\mathrm{SL}(E_-)$ an involution whose -1-eigenspace has dimension e. Similarly, if $s<r$, then, by recursion, find in $\mathrm{SL}(E_+)$ an involution whose -1-eigenspace has dimension e.

7. Consider the cases where $s \ge e > r$ or $e \ge \max(r,s)$. By recursion, find in $\mathrm{SL}(E_+)$ an involution h_2 whose -1-eigenspace has dimension $e-r$. Now return h_1h_2, an involution of the required type.

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

Theorem 9.1 *In $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ field operations, this Las Vegas algorithm constructs an involution in $\mathrm{SL}(4n, q)$ that has its -1-eigenspace of any even dimension in $[0, d]$.*

PROOF: Theorem 8.27 proves that the strong involution h_1 in Step 1 can be found and constructed using a Las Vegas algorithm in $O(d(\xi+d^3 \log d+d^2 \log d \log\log d \log q))$ field operations. In Sections 11 and 12, we show that generators for $\mathrm{SL}(E_-)$ and $\mathrm{SL}(E_+)$ as subgroups of G can be constructed using the same number of operations. 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. □

The other classical groups are dealt with in essentially the same way, and the corresponding algorithms have the same complexity. If G is an orthogonal group preserving a form of + type, then the involution constructed in Step 1 has both eigenspaces supporting a form of + type, so the involution returned has the same property.

10 Exponentiation

A frequent task in our algorithms is computing g^n for some $g \in \mathrm{GL}(d, q)$ and integer n where $n < q^d$. We could construct g^n with $O(\log n)$ multiplications using the familiar black-box squaring technique. Instead, we describe the following faster Las Vegas 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, read off the minimal polynomial $h(x)$ of g, and factorise $h(x)$ as a product of irreducible polynomials.
3. Following Section 2.2, compute a multiplicative upper bound, m, to the order of g.
4. If $n > m$, then replace n by $n \bmod m$. By repeated squaring, calculate $x^n \bmod h(x)$ as a polynomial of degree $k - 1$, where k is the degree of $h(x)$.
5. Evaluate this polynomial 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.

Lemma 10.1 *Let $g \in \mathrm{GL}(d, q)$ and let $0 \leq n < q^d$. This is a Las Vegas algorithm that computes g^n in $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations.*

Proof: Using the Las Vegas algorithm of [21], in $O(d^3 \log d)$ field operations we obtain the Frobenius normal form of g, the corresponding change-of-basis matrix, and thus the minimal polynomial of g. The minimal polynomial can be factored in $O(d^2 \log d \log\log d \log q)$ field operations.

Calculating $x^n \bmod h(x)$ requires $O(\log n)$ multiplications in $\mathrm{GF}(q)[x]/(h(x))$, and hence $O(d^2 \log d \log\log d \log q)$ field operations. Evaluating this 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. Conjugating g by the inverse of the change-of-basis matrix costs $O(d^3)$ field operations. □

11 Constructing direct factors

We consider the following problem.

Problem 11.1 *Let $G = \langle X \rangle$ be a subgroup of the centraliser of an involution g in $\mathrm{GX}(d,q)$, so $G \leq \mathrm{GX}(E) \times \mathrm{GX}(F)$, where E and F are the eigenspaces of g. If G contains $\Omega(E) \times \Omega(F)$, find (as* SLPs *in X) generating sets for $\Omega X(E)$ and $\Omega X(F)$.*

We prove the following result.

Theorem 11.2 *There is a Las Vegas algorithm, with complexity $O(\frac{d \log\log d}{\log d}(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ measured in 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 $\mathrm{GX}(d,q)$, such that X generates a group containing $\Omega X(E) \times \Omega X(F)$, and returns generating sets for $\Omega X(E)$ and $\Omega X(F)$ as* SLPs *in X.*

Our proof of this theorem relies heavily on the one-sided Monte Carlo recognition algorithm of Niemeyer & Praeger [33, 34]. We outline this algorithm briefly. The input is $\langle X \rangle = G \leq \mathrm{GX}(d,q)$, of known type $\mathbf{X}$, where $d > 2$. It decides whether or not G contains $\Omega X(d,q)$, 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 $\mathcal{S}$ of subsets of $\mathrm{GX}(d,q)$ is defined with the property that any irreducible subgroup of $\mathrm{GX}(d,q)$ that does not preserve any non-degenerate form not preserved by $\mathrm{GX}(d,q)$, and that contains a subset $S \in \mathcal{S}$, generates a group containing $\Omega X(d,q)$. In this case S is a *witness* to this fact. For most values of the parameters $(\mathbf{X}, d, q)$, the following is the case. A set P of pairs of primes or squares of primes, each dividing $|\Omega X(d,q)|$ but prime to $q-1$, is defined. The elements of $\mathcal{S}$ are pairs, and a pair S is in $\mathcal{S}$ if and only if there is a pair $(\ell_1, \ell_2) \in P$ such that ℓ_1 divides the order of one element of S, and ℓ_2 divides the order of the other.

We call parameters $(\mathbf{X}, d, q)$ for which $\mathcal{S}$ is defined in this way *standard*. (These include all generic cases of [33] and some of the non-generic cases of [34].) If the parameters are not standard, then the algorithm requires different types of witness. To find a witness, a sample of $O(\log\log d)$ random elements must be considered; see [33, Proposition 7.5].

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 $r\geq e+1$. If $(\ell_1,\ell_2)\in P$, then in most cases ℓ_i is a primitive prime divisor of $q^{e_i}-1$ for some $e_i>d/2$ for $i=1,2$, and $e_1\neq e_2$. Further conditions may be imposed, and in some cases ℓ_i is the square of a primitive prime divisor of $q^{e_i}-1$. We are not concerned here with the precise variations used.

A sufficient condition for $g\in \mathrm{SX}(d,q)$ to have order prime to ℓ_i is that the characteristic polynomial of g should have no irreducible factor of degree a multiple of e_i.

Before describing the algorithms to solve our problem, we present two related results which assist in our analysis.

Lemma 11.3 *Let π be a partition of $d>2$, and let $\Omega X(d,q)\leq G\leq \mathrm{GX}(d,q)$. Denote by $P(G,\pi)$ the proportion of $g\in G$ such that the degrees of the irreducible factors of the characteristic polynomial of g partition d as π.*

(i) *Let $\mathbf{X}=\mathbf{SL}$ and $\pi=(k,d-k)$: if $1\leq k<d/2$ then $P(G,\pi)>(1-q^{-1})^2/(k(d-k))$.*

(ii) *Let $\mathbf{X}=\mathbf{SL}$ and $\pi=(1,k,d-k-1)$: if $1<k<d-k-1$ then $P(G,\pi)>(1-q^{-1})^2/(k(d-k-1))$.*

(iii) *Let $\mathbf{X}\neq\mathbf{SL}$ and $\pi=(k/2,k/2,(d-k)/2,(d-k)/2)$, where d and k are even: if $1<k<d/2$ then $P(G,\pi)>(1-q^{-1})^2/(4k(d-k))$.*

(iv) *Let $\mathbf{X}=\mathbf{SU}$ or $\mathbf{SO^0}$ and $\pi=(1,k/2,k/2,(d-k-1)/2,(d-k-1)/2)$, where d is odd and k is even: if $2<k<(d-1)/2$ then $P(G,\pi)>(1-q^{-1})^2/(4k(d-k-1))$.*

The proof is an easy exercise, using the results of Section 8.

Lemma 11.4 *Let $d>2$ and $1<\ell\leq d$, and assume $\Omega X(d,q)\leq G\leq \mathrm{GX}(d,q)$. The proportion of elements of G whose characteristic polynomial has no irreducible factor of degree a multiple of ℓ is greater than $c\log d/d$ for some positive universal constant c.*

Proof: Suppose that $\mathbf{X}=\mathrm{SL}$, and $d>4$. An easy modification of Lemma 8.7 shows that if $\ell>d/2$, then the proportion of elements of G whose characteristic polynomial has no irreducible factor of degree ℓ is at least $1/2$.

We now consider smaller values of ℓ. We apply Lemma 11.3 to obtain the proportion of elements of G whose characteristic polynomial has exactly two irreducible factors of unequal degrees. Observe that, for any $a>0$, $\sum_{k=1}^{a}1/(k(d-k))=(2/d)\sum_1^a 1/k$. Taking $a=\lfloor (d-1)/2\rfloor$, and letting k denote the smaller degree, so that $k\leq a$, we see that the proportion in question is at least $c\log d/d$ for some absolute constant $c>0$.

Similarly, if the degree k is required to be congruent to some fixed value modulo ℓ, then the proportion in question is at least $c \log d/(d\ell)$ for some $c > 0$.

Now consider the values of k for which k or $d-k$ is a multiple of ℓ. If $\ell > 2$ then at least $\ell - 2$ of the ℓ residue classes give values of k that satisfy the conditions of the lemma, and complete the proof in this case.

Now assume $\ell = 2$. If k is odd, and d is even, then $d-k$ is odd; so one of the residues classes give values of k that satisfy the conditions. If $d \geq 9$ is odd, then we consider the proportion of elements of G whose characteristic polynomial has one irreducible factor of degree 1, one of degree k, and one of degree $d-k-1$, as in case (ii) above. The proof now proceeds exactly as before.

The remaining cases occur for bounded d only and there clearly exist elements which satisfy the present lemma.

The proof for the other classical groups is essentially the same. □

11.1 The standard parameter case

Our task is the following. Let $\Omega X(E) \times \Omega X(F) \leq G = \langle X \rangle \leq \mathrm{GX}(E) \times \mathrm{GX}(F)$; find (as SLPs in X) a generating set for $\Omega X(E)$. Let e and f denote the dimensions of E and F respectively. We assume that $(\mathbf{X}, e, q)$ is standard; in particular, this implies that $e > 2$.

Our algorithm, `GenerateFactor`, is the following.

1. Repeatedly construct random $(g, h) \in G$, 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 $\Omega X(E)$, with corresponding prime powers (ℓ_1, ℓ_2), and the pseudo-order n_i of h_i is prime to ℓ_i for $i = 1, 2$.

2. Let $m_i = n_i(q-1)$. Compute $g_1^{m_1} = (g_1, h_1)^{m_1}$ and $g_2^{m_2} = (g_2, h_2)^{m_2}$.

3. If $\langle g_1^{m_1}, g_2^{m_2} \rangle$ is irreducible, and it also preserves no non-degenerate bilinear form when $\mathbf{X} = \mathbf{SL}$, then return $(g_1^{m_1}, g_2^{m_2})$; else return to Step 1.

Lemma 11.5 *If the parameters $(\mathbf{X}, e, q)$ for G are standard, then* `GenerateFactor` *is a Las Vegas algorithm that constructs a generating pair for $\Omega X(E)$ in $O(\frac{d \log\log d}{\log d}(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ field operations.*

Proof: The algorithm of [33] requires $O(\log\log e)$ trials to find a pair of elements (g_1, h_1) and (g_2, h_2) of G such that (g_1, g_2) will act as a witness for $\Omega X(E)$. If (g_1, g_2) is a witness because g_i has order a multiple of ℓ_i, then Lemma 11.4 implies that the probability that h_i has pseudo-order coprime to ℓ_i is $O(\log f/f)$.

We must also consider the probability that $\langle g_1, g_2 \rangle$ is reducible, or, if $\mathbf{X} = \mathbf{SL}$, that it preserves a non-degenerate form. Since g_i acts irreducibly on a subspace of dimension $e_i > e/2$, the probability that $\langle g_1, g_2 \rangle$ is irreducible is bounded away from 0, and tends to 1 as q or d tends to infinity. The same is clearly true for the probability that $\langle g_1, g_2 \rangle$ preserves no non-degenerate form if $\mathbf{X} = \mathbf{SL}$.

Computing and factorising the characteristic polynomial of $g \in G$ takes $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations. The powering operation, which need only take place in E, is performed twice, assuming that $\langle g_1, g_2 \rangle$ is irreducible and does not preserve a form. □

11.2 The dimension 2 case

We now consider the case where $(\mathbf{X}, e, q) = (\mathbf{SL}, 2, q)$ and $q > 3$. We first show that, with high probability, $\mathrm{SL}(2, q)$ can be generated by an irreducible element and a random conjugate. Let $M(q)$ be the metacyclic group of order $2(q+1)$ defined by the presentation $\{a, b \mid a^{q+1} = 1, a^b = a^{-1}, b^2 = a^{(q+1)/2}\}$.

Lemma 11.6 *Let H be a maximal irreducible subgroup of $\mathrm{SL}(2, q)$. Then H is either conjugate to $\mathrm{SL}(2, r)$, where $q = r^\ell$ for an odd prime ℓ; or to an extension $\mathrm{SL}(2, r).2$ of $\mathrm{SL}(2, r)$ by a cyclic group of order 2, where $q = r^2$; or is isomorphic to $M(q)$; or is isomorphic to an extension of a cyclic group of order 2 by one of A_4, S_4 or A_5.*

Proof: This result can be read off from [26, Hauptsatz II.8.27]. □

Corollary 11.7 *Let $q > 3$ and let $g \in \mathrm{SL}(2, q)$ act irreducibly. The probability that a random conjugate of g, together with g, will generate $\mathrm{SL}(2, q)$ is at least $1 - q^{-2/3}$, independently of the choice of g.*

Proof: An irreducible element g of $\mathrm{SL}(2, q)$ lies in a unique cyclic subgroup of order $q+1$, since distinct cyclic subgroups of $\mathrm{PSL}(2, q)$ of order $(q+1)/2$ intersect trivially (see [26, Hauptsatz II.8.5]). Thus the probability that g and a random conjugate h of g will lie in the same copy of $M(q)$ is $1/k$, where $k = |\mathrm{SL}(2, q)|/2(q+1) = (q^2 - q)/2$, unless g has order 4. If g has order 4, there remains the possibility that $\langle g, h \rangle$ is a quaternion group of order 8.

If g has order 4 and acts irreducibly, then $q \equiv 3 \bmod 4$. The elements of $\mathrm{SL}(2, q)$ of order 4 lie in a single conjugacy class, of size $q(q-1)$, so we may assume that

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

If $\langle g, h \rangle$ is a quaternion group of order 8, then a calculation shows that h is of the form

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix},$$

where $a^2 + b^2 = -1$, giving $q+1$ possibilities. Hence the probability that g and h lie in a single copy of $M(q)$ is at most $q+3 : q(q+1)$. (We must consider the $q+1$ conjugates of h, and $g^{\pm 1}$.)

Now let $\mathrm{SL}(2,r)$ be a subgroup of $\mathrm{SL}(2,q)$ containing an element g that acts irreducibly. This implies that q is an odd power of r. Now g lies in exactly $(q+1)/(r+1)$ conjugates of $\mathrm{SL}(2,r)$, which between them contain fewer than $(q+1)r(r-1)/(r+1)$ of the $q(q-1)$ conjugates of g in $\mathrm{SL}(2,q)$. Thus the probability that h lies in one of these subgroups is less than $(q+1)r(r-1)/(q(q-1)(r+1)) < q^{-2/3}$.

The probability that g and h both lie in the same copy of $2.A_4$ or $2.S_4$ or $2.A_5$ is $O(1/q^3)$, since $\mathrm{SL}(2,q)$ contains at most two conjugacy classes of any one of these groups (see [26, Satz II.8.13-18]). □

We now describe our algorithm, `TwoFactor`, to construct a generating set for $\mathrm{SL}(2,q)$ in G, where $\Omega X(d-2,q) \times \mathrm{SL}(2,q) \leq G = \langle X \rangle \leq \mathrm{GX}(d-2,q) \times \mathrm{GL}(2,q)$. The output is a set of generators for $\mathrm{SL}(2,q)$, given as SLPs in X.

1. If $q+1$ is not a power of 2, then search for $(g,h) \in G$ where:
   - the characteristic polynomial of g has no irreducible factor of even degree;
   - h has an irreducible characteristic polynomial, and has pseudo-order divisible by an odd prime ℓ, where ℓ divides $q+1$.
2. If $q+1$ is a power of 2, then search for $(g,h) \in G$ where, if g and h have pseudo-orders a and b respectively, then $v_2(b) > v_2(a)+1$.
3. Let k be the pseudo-order of (g,h), divided by ℓ, in Case 1; and let k be the odd part of the pseudo-order of (g,h) in Case 2. Evaluate h^k to obtain $(1,x)$.
4. Now x is an irreducible element of $\mathrm{SL}(2,q)$. Find, by random search, $y \in G$ such that x and x^y generate $\mathrm{SL}(2,q)$, and return $\{x, x^y\}$.

Lemma 11.8 `TwoFactor` *is a Las Vegas algorithm that takes* $O(\frac{d}{\log d}(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ *field operations.*

Proof: The first step is to prove that, with high probability, (g,h) can be found with $O(d/\log d)$ trials. Suppose first that $q+1$ is not a power of 2. Lemma 11.4 shows that the proportion of elements of $\Omega X(d-2,q)$ with the property that every irreducible factor of their characteristic polynomials has odd degree is $O(\log d/d)$, and the result follows.

If $q+1$ is a power of 2, then we may require g to have odd order. Lemma 11.3 implies that the proportion of elements of G whose characteristic polynomial has at most 5 irreducible factors, all of odd degree, is $O(\log d/d)$. Since $q \equiv 3 \bmod 4$, it follows that if $g \in G$ has such a characteristic polynomial, then the probability of g having odd order is at least $(1/2^5)(1-O(1/q))$. In fact the probability is at least $(1/2^3)(1-O(1/q))$, since, in the cases where there are more than three factors, those of degree greater than 1 are paired as $h(x)$ and $\tilde{h}(x)$ and $k(x)$ and $\tilde{k}(x)$, or as $h(x)$ and $\hat{h}(x)$ and $k(x)$ and $\hat{k}(x)$.

Thus, in either case, we can expect to find a suitable (g, h) with $O(d/\log d)$ trials. For each pair (g, h) considered, we compute and factorise the characteristic polynomial of g in $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations. In Step 3 we compute the pseudo-order of (g, h) in $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations. We also need to raise (g, h) to a certain power, but only need to power h. (The pseudo-order of (g, h) needs to be computed, rather than the pseudo-order of h, because we need to record x as an SLP in the given generating set.) Corollary 11.7 implies that the number of trials needed in Step 4 is constant. □

11.3 Dimension 4 orthogonal cases

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

Since $\Omega^-(4, q) \cong \mathrm{PSL}(2, q^2)$, this case is essentially covered by Lemma 11.8. We need $(g, h) \in \Omega^-(4, q) \times \Omega^\epsilon(d-4, q)$ that powers to an element of $\Omega^-(4, q)$ of order not dividing $q^2 - 1$. We thus look for (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 $\mathrm{SL}(2, q)$. If $q > 3$, then we can find (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 Section 11.2.

In summary, if $\Omega(E)$ is isomorphic to $\Omega^\epsilon(4, q)$, we construct one or (if $\epsilon = +$) two suitable elements of $\Omega(E)$ by powering a suitable element or elements 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 11.9 *The above algorithm is Las Vegas and constructs a generating pair for $\Omega(E) \cong \Omega^\epsilon(4, q)$ (where $q > 3$ if $\epsilon = +$) in $O(\frac{d}{\log d}(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ field operations.*

11.4 The other non-standard cases

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 the normal closure of any one of its 8 elements of order 3, these soluble examples pose no problems.

The remaining exceptional cases are listed in [33] and are perfect, being simple modulo scalars. Since none of these groups consists 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.

11.5 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 a witness for $\Omega X(E)$ by virtue of g_i having order a multiple of some primitive prime divisor of $q^{k_i} - 1$ (or of its square), and the characteristic polynomial of h_i does not have an irreducible factor of degree a multiple of 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. Recall that the algorithm of [33] requires a sample of $O(\log \log d)$ random elements. In summary:

Theorem 11.10 *Assume that the parameters* $(\mathbf{X}, d, q)$ *are standard. There is a Las Vegas algorithm, with complexity* $O(\log \log d(\xi + d^3 \log d + d^2 \log d \log \log d \log q))$ *measured in 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 a strong involution in* $\mathrm{GX}(d, q)$*, generates a group containing* $\Omega X(E) \times \Omega X(F)$*, where the dimension of* E *is at least* $d/3$*, and returns a generating set for* $\Omega X(E)$ *as* SLPs *in* X*.*

12 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 $G = \mathrm{SX}(d, q)$ and let E_+ and E_- denote the eigenspaces of u.

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

2. Suppose that E_+ and E_- are isometric. Construct the projective centraliser in G of u.

If E_+ and E_- have the same dimension, then they are isometric, except when G is an orthogonal group of $-$ type (see Lemma 2.2). The second problem arises in Algorithm `Two` for non-orthogonal groups and for orthogonal groups of $+$ type only.

Elements of the centraliser of an involution in a black-box group having an order oracle can be constructed using an algorithm of Bray [8], which employs the following result.

Theorem 12.1 *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 [8] 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 by Bray's algorithm are involutions; but if just one of these is selected, then it is independently and uniformly distributed within that class of involutions.

Parker & Wilson [37] prove the following.

Theorem 12.2 *There is a 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 $O(d)$, we construct random elements of the centraliser of the involution. Liebeck & Shalev [29] 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 H 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, Bray's algorithm assumes the existence of an order oracle. We do not require such an oracle for a linear group. Recall, from Section 2.2, that we can deduce if an element of a linear group has even order in $O(d^3 \log d + d^2 \log d \log\log d \log q)$ field operations. Further, the construction of the centraliser of an involution requires only knowledge of pseudo-orders.

In our context, the analysis of [24] implies the following.

Theorem 12.3 *The algorithm to construct the centraliser of an involution in $\mathrm{SX}(d, q)$ is Las Vegas and has complexity $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ measured in 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 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 11 to obtain generators for the derived groups of the projections of the centralisers of the two eigenspaces.

We summarise the preceding discussion.

Theorem 12.4 *Let h be an involution in $\langle X\rangle = G$, where $\Omega X(d, q) \leq G \leq \mathrm{GX}(d, q)$. Assume that the -1-eigenspace of h has dimension e in the range $(d/3, 2d/3]$. Generating sets for the copies of $\Omega X(e, q)$ and $\Omega X(d - e, q)$ that centralise the eigenspaces can be found in $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ 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 $\Omega X(e, q) \wr C_2$ that interchanges the two copies of $\Omega X(e, q)$.*

13 The base cases for the non-orthogonal groups

We now consider the base cases for Algorithms `One` and `Two` when $\mathrm{SX}(d, q)$ is a non-orthogonal group. If $d = 2n$, then Lemma 3.6 shows that $Y_0 := \{s, t, \delta, u, v\}$ generates

$\mathrm{SX}(2,q) \wr C_n$ or $\mathrm{SX}(2,q) \wr S_n$ according to the type of $\mathrm{SX}(d,q)$. As the first and major task of each algorithm, we construct Y_0. As a final step, we construct the additional elements x, y.

Observe that the elements of Y_0 act non-trivially only on a 4-dimensional space; they 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 13.1 *Subject to the availability of a discrete logarithm oracle for* $\mathrm{GF}(q)$, SLPs *for standard generators and other elements of* $\langle X \rangle = \mathrm{SX}(d,q)$ *for* $d \leq 4$ *can be constructed in* $O(\xi \log\log q + \log q)$ *field operations.*

13.1 $\mathrm{SX}(2,q)$

The base case encountered most frequently is $\mathrm{SL}(2,q)$ in its natural representation. A Las Vegas algorithm to construct an element of $\mathrm{SL}(2,q)$ as an SLP in an arbitrary generating set is described in [18]. This algorithm requires $O(\log q + \xi \log\log q)$ field operations, and the availability of a discrete logarithm oracle for $\mathrm{GF}(q)$.

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 [22]; either requires $O(\log q)$ field operations.

13.2 $\mathrm{SL}(2,q) \wr C_2$

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

Problem 13.2 *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* G, *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 13 we construct $\mathrm{SX}(4,q)$. Now b is the permutation matrix used in line 15 to 'glue' v_1 and v_2 together to form v, the long cycle. We could use the algorithm of Section 13.3 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. Construct the projective centraliser H of u in $\mathrm{SX}(4,q)$; it 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 11, 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 has the same complexity as that for $\mathrm{SL}(2,q)$.

13.3 $\mathrm{SX}(3,q)$ and $\mathrm{SX}(4,q)$

For $\mathrm{SL}(3,q)$ we use the algorithm of [31] to construct standard generators. It assumes the existence of an oracle to recognise constructively $\mathrm{SL}(2,q)$ and its complexity is that of the oracle.

We use the *involution-centraliser algorithm* of [24] to construct standard generators for the remaining groups $\mathrm{SX}(3,q)$, 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 $g \in G$ and want to express it as an SLP in X. In our description, if we "find" an element of G, then we obtain it as an 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 or 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 SLPs for both gh and h, we can construct 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 apply 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 [18]. In this context, the complexity of the involution-centraliser algorithm is that stated in Theorem 13.1.

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 2.2.

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 from the elements of Y_0, and that both x and y are elements of $C_G(h)$.

14 Base cases for orthogonal groups

14.1 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 logarithm oracle for $\mathrm{GF}(q)$.

The remaining base cases occur in dimension 4. As we observed in Lemma 3.2, $\Omega^+(4, q)$ 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 tensor factors and, using the algorithm of [32, §4], construct the tensor factors. Subject to a discrete logarithm oracle for $\mathrm{GF}(q)$, we now use the algorithm of [18] to recognise constructively the copies of $\mathrm{SL}(2, q)$.

The complexity of this Las Vegas algorithm, measured in field operations, is constant, given a constant number of calls to the discrete logarithm oracle for $\mathrm{GF}(q)$.

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

14.2 Groups preserving forms of − type

As we observed in Lemma 3.3, $\Omega^-(4, q) \cong \mathrm{PSL}(2, q^2)$. Subject to a discrete logarithm oracle for $\mathrm{GF}(q^2)$, we use the algorithm of [18] 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 $G = \Omega^-(6, q)$ when $q \equiv 3 \bmod 4$. 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 involution i, 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 $\Omega(F)$ in $C_G(i)$.

3. Now find, by random search, $h \in G$ such that $T = E \cap E^h$ has 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 [33]. If not, repeat Steps 3 and 4 until it is true.

5. Construct a hyperbolic basis (e_2, f_2, w_1, w_2) 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 $\langle w_1, w_2\rangle$.

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 $(e_1, f_1, e_2, f_2, w_1, w_2)$ 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 is an element of K. We now construct this generator as an SLP in the generators of $K = \Omega^+(4, q)$.

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

Lemma 14.1 *This algorithm is Las Vegas and its complexity, measured in field operations, is constant, given a constant number of calls to the discrete logarithm oracle for* $\mathrm{GF}(q^2)$.

Proof: For Step 1, see Theorem 8.1. To compute the probability that $E \cap E^h$ has 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 must compute the probability that these subgroups lie in a maximal subgroup. Since $\Omega(F)$ contains an element of order $(q+1)/2$, we apply [27, Lemma 3.8]. The use of the naming algorithm in Step 4 is not necessary; we can simply start again if Step 6 fails. The discrete logarithm oracle for $\mathrm{GF}(q^2)$ is used in Step 6. The other steps clearly require a bounded number of field operations. □

14.3 Groups preserving forms of 0 type

As we observed in Lemma 3.4, $\Omega(3,q) \cong \mathrm{PSL}(2,q)$. Subject to a discrete logarithm oracle for $\mathrm{GF}(q)$, we use the algorithm of [18] to recognise constructively this group. Similar comments apply to $\mathrm{SO}(3,q)$.

We must also consider $G = \Omega(5,q)$ when $q \equiv 3 \bmod 4$. 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 i 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 in $C_G(i)$ 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, w) of T. 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 w acts as $\Omega(3,q)$ on the orthogonal complement of $\langle w \rangle$ 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 w 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 w in G, which acts as $\Omega^+(4,q)$ on the orthogonal complement of $\langle w \rangle$.
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, w) are the standard generators for $\Omega(T)$, together with v.

Lemma 14.2 *This algorithm is Las Vegas and its complexity, measured in field operations, is constant, given a constant number of calls to the discrete logarithm oracle for* $\mathrm{GF}(q)$.

Proof: For Step 1, see Theorem 8.1.

Consider Step 2. The proportion of elements h of G with the required property is $1/2+O(1/q)$. This is because the proportion of elements h of G such that $T = E \cap E^h$ has dimension 3 is $1 + O(1/q)$. Of these, the proportion for which T supports a non-degenerate form is again $1+O(1/q)$, and of these the proportion for which $T^\perp$ supports a form of + type is $1/2 + O(1/q)$.

The discrete logarithm oracle for GF(q) is used in Step 9. □

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.

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 selected, 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 oracle, and the space that it requires, are not proportional to the number of applications in a given field.

A hyperbolic basis for a vector space with a given non-degenerate bilinear form can be constructed in $O(d^3)$ field operations (see [9] for an algorithm to perform this task).

If a matrix group acts absolutely irreducible on its underlying vector space, then we can determine the classical forms it preserves in $O(d^3)$ field operations (see [25, Section 7.5.4]).

Babai [2] 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.* [14]. That this is also polynomial time was established by Pak [36]. For a discussion of both algorithms, see [38, pp. 26-30].

We now complete our analysis of the main algorithms.

Theorem 15.1 *Algorithm* `OneEven` *is Las Vegas, and its complexity, measured in field operations, is* $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$.

Proof: The proportion of elements of G with the required property in line 4 is at least k/d for some absolute constant k, as proved in Section 8. Theorem 8.27 shows that the involution can be constructed in $O(d(\xi+d^3 \log d+d^2 \log d \log\log d \log q))$ field operations.

Lines 7 and 13 require $O(d(\xi + d^3 \log d + d^2 \log d \log\log d \log q))$ field operations as proved in Section 12.

The recursive calls in lines 8 and 9 involve matrices of dimension at most $2d/3$; Lemma 2.4 implies that they increase the number of field operations by only a constant factor.

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 $\mathrm{GF}(q)$ (see [18]). Each solution to Problem 13.2 requires three 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 [24] 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.

Before we estimate their lengths, we identify other critical properties of SLPs.

1. We replace the second type of node, which defines the inverse of a previously defined element, by a node type 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 10 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 [14] to generate random elements;
- a new implementation of this algorithm by Bäärnhielm & Leedham-Green [5] which realises the properties identified in Section 16;
- our implementations of Bray's algorithm [8] and the involution-centraliser algorithm [24].
- our implementations of the algorithms of [18] and [31].

The computations reported in Table 17 were carried out using Magma V2.14 on a Pentium IV 2.8 GHz processor. We list the CPU time in seconds taken to construct the standard generators for $\mathrm{SX}(d, q)$ for the non-orthogonal groups, and for $\Omega^\epsilon(d, q)$ for a range of values of d and q. We use Algorithm `Two` for the non-orthogonal groups, Algorithm `One` for the orthogonal groups. The time is averaged over three runs.

d	q	SL	Sp	SU	Ω^+	Ω^-	Ω^0
5	5	0.1	–	1.4	–	–	2.8
6	5	0.4	2.7	1.4	3.3	2.2	–
10	5	0.5	4.5	1.6	5.4	4.8	–
20	5	0.9	6.1	2.3	14.0	12.2	–
25	5	1.5	–	4.8	–	–	17.0
40	5	1.9	31.0	6.2	31.1	32.8	–
45	5	5.4	–	12.6	–	–	41.7
60	5	6.2	13.0	26.8	51.1	64.2	–
80	5	9.8	16.5	39.3	40.3	114.2	–
100	5	16.3	24.3	83.8	120.0	203.9	–
5	5^4	0.7	–	5.1	–	–	5.2
6	5^4	1.1	7.1	8.8	7.0	5.6	–
10	5^4	2.1	18.8	13.1	12.8	12.3	–
20	5^4	3.7	25.6	19.1	32.7	32.3	–
25	5^4	7.2	–	37.3	–	–	56.4
40	5^4	11.7	39.8	41.6	48.6	128.7	–
45	5^4	18.6	–	77.4	–	–	297.9
60	5^4	37.4	74.5	121.5	128.1	332.1	–
80	5^4	60.7	106.5	202.5	290.0	555.9	–
100	5^4	98.3	151.6	404.9	530.7	983.8	–

Table 4: Performance of implementation for a sample of groups

References

[1] Sophie Ambrose. Matrix Groups: Theory, Algorithms and Applications. PhD thesis, University of Western Australia, 2006.

[2] 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.

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

[4] Henrik Bäärnhielm. Recognising the Suzuki groups in their natural representations. *J. Algebra* **300** (2006), 171–198.

[5] Henrik Bäärnhielm and C.R. Leedham-Green. Extending the product replacement algorithm. Preprint 2008.

[6] Robert Beals, Charles R. Leedham-Green, Alice C. Niemeyer, Cheryl E. Praeger and Ákos Seress. A black-box group algorithm for recognizing finite symmetric and alternating groups I, *Trans. Amer. Math. Soc.* **355** (2003), 2097–2113.

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

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

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

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

[11] Peter A. Brooksbank and William M. Kantor. On constructive recognition of a black box PSL(d, q). In *Groups and Computation, III (Columbus, OH, 1999)*, pp. 95–111. Volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, de Gruyter, Berlin, 2001.

[12] Peter A. Brooksbank and William M. Kantor. Fast constructive recognition of black box orthogonal groups. *J. Algebra* **300** (2006), 256-288.

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

[14] 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.

[15] 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*, pp. 55–60. (DIMACS, 1995), 1997.

[16] 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.*, pp. 11–26, Cambridge, 1998. Cambridge Univ. Press.

[17] Marston Conder and Charles R. Leedham-Green. Fast recognition of classical groups over large fields. In *Groups and Computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pp. 113–121, Berlin, 2001. de Gruyter.

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

[19] Elliot Mark Costi. Constructive membership testing in classical groups. PhD thesis, Queen Mary, University of London, 2009.

[20] L. Dornhoff, *Group Representation Theory, Part A*. Marcel Dekker, 1971.

[21] Mark Giesbrecht. Nearly optimal algorithms for canonical matrix forms. PhD thesis, University of Toronto, 1993.

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

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

[24] P.E. Holmes, S.A. Linton, E.A. O'Brien, A.J.E. Ryba and R.A. Wilson. Constructive membership in black-box groups. *J. Group Theory* **11** (2008), 747-763.

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

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

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

[28] W. Keller-Gehrig. Fast algorithms for the characteristic polynomial. *Theoret. Comput. Sci.* **36** (1985), 309–317.

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

[30] Frank Lübeck, Alice C. Niemeyer, and Cheryl E. Praeger. Finding involutions in finite Lie type groups of odd characteristic. *J. Algebra* **321** (2009), 3397-3417.

[31] F. Lübeck, K. Magaard, and E.A. O'Brien. Constructive recognition of $\mathrm{SL}_3(q)$. *J. Algebra* **316** (2007), 619–633.

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

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

[34] Alice C. Niemeyer and Cheryl E. Praeger. A recognition algorithm for non-generic classical groups over finite fields. J. Aust. Math. Soc. Ser. A **67** (1999), 223–253.

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

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

[37] Christopher W. Parker and Robert A. Wilson. Recognising simplicity of black-box groups. Preprint 2009.

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

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

[40] Joachim von zur Gathen and Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2003.

[41] 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