Abstract

The maximal subgroups of the finite classical groups are divided by a theorem of Aschbacher into nine classes. In this paper we show how to construct those maximal subgroups of the finite classical groups of linear, symplectic or unitary type that lie in the first eight of these classes. The ninth class consists roughly of absolutely irreducible groups that are almost simple modulo scalars, other than classical groups over the same field in their natural representation. All of our constructions can be carried out in low-degree polynomial time.

Constructing maximal subgroups of classical groups

Derek F. Holt and Colva M. Roney-Dougal *

December 22, 2006

1 Introduction

With only two families of exceptions, the maximal subgroups of the finite classical groups are divided into nine classes by Aschbacher's theorem [1]. The maximal subgroups in the first eight of these classes are described in detail in [15]. The ninth class, $\mathcal{S}$, consists roughly of absolutely irreducible groups that are almost simple modulo scalars, other than classical groups over the same field in their natural representation. The two families of exceptions to Aschbacher's theorem are groups containing the graph automorphism of $\mathrm{PSp}(4, 2^e)$, whose maximal subgroups are divided into 6 classes (including $\mathcal{S}$) in [1], and groups containing the graph automorphism of $\mathrm{PSO}^+(8, q)$.

The purpose of this paper is to describe algorithms for writing down generators of all of the subgroups that are not in $\mathcal{S}$ for G a linear, symplectic or unitary group. We could do the same when G is orthogonal, but because of the large number of cases that arise in that situation, we have decided to omit the orthogonal groups for now. We plan to develop similar algorithms for the orthogonal groups in a future article.

The two main papers on the computation of maximal subgroups of an arbitrary finite permutation group G are [5, 8]. These both show that the problem can effectively be reduced to the case when G is almost simple. The vast bulk of the cases that arise for G almost simple can then be handled using

*During the work for this paper the second author was partially supported by the Australian Research Council and partially supported by EPSRC grant number GR/S30580.

the methods that we describe here, and this was our principal motivation for developing these techniques in a uniform fashion. Of course, the maximal subgroups in $\mathcal{S}$ still need to be dealt with; they are now known for degree $d \leq 250$ [12, 19] and can be constructed on a case-by-case basis.

The algorithms presented in this paper describe the maximal subgroups of the (quasi)simple linear, symplectic and unitary groups. They can be combined with subgroup conjugacy information in [1, 15] and explicit descriptions of when the maximal groups in each Aschbacher class are maximal in a classical group to produce the maximal subgroups of any group G with $\mathrm{SL}(d,q) \trianglelefteq G \leq \Gamma\mathrm{L2}(d,q)$ $(= \Gamma\langle\iota\rangle$ – see below), $\mathrm{Sp}(d,q) \trianglelefteq G \leq \Gamma\mathrm{Sp2}(d,q)$ $(= \Gamma\mathrm{Sp}(d,q)\langle\iota\rangle$ – see below) or $\mathrm{SU}(d,q) \trianglelefteq G \leq \Gamma\mathrm{U}(d,q)$, and similarly for their projective counterparts.

Our algorithms have been implemented in MAGMA [4], where they are combined with representations of groups in $\mathcal{S}$ to construct the maximal subgroups of classical groups in low dimensions over any finite field, in any permutation or matrix representation. Currently, this is roughly for $d \leq 5$, but we are actively working on increasing the families of groups for which the implementations are available. We also plan in the future to make available functions that return all maximal subgroups of specific types, such as reducible maximal subgroups, for the classical groups in all dimensions d.

One of the most significant practical consequences of our algorithms is as follows. Let G be any permutation group each of whose nonabelian simple composition factors is either one of these low-dimensional classical groups or has order less than 1.6×10^7. Then one may now compute the maximal subgroups of G, the set of all subgroups of G, and its automorphism group.

The general maximal subgroups algorithm uses constructive recognition algorithms [14] to set up a homomorphism between an arbitrary (black box) representation of the group G and a standard copy of the matrix group. So our algorithms are applicable to black box classical groups.

This paper includes complexity analyses of our algorithms. Before stating a theorem which summarises our results, we need to introduce some of the notation used in [15]. We let Ω be one of the groups $\mathrm{SL}(d,q)$, $\mathrm{Sp}(d,q)$ or $\mathrm{SU}(d,q)$, in their natural representation; we refer to these three cases as cases L, S and U, respectively. Let $\Gamma = \Gamma\mathrm{L}(d,q)$, $\Gamma\mathrm{Sp}(d,q)$ or $\Gamma\mathrm{U}(d,q)$ be the extension of Ω by its diagonal and field automorphisms. Let $A = \Gamma\mathrm{L2}(d,q) := \Gamma\langle\iota\rangle$ with ι a graph isomorphism in case L with $d \geq 3$, let $A := \Gamma\mathrm{Sp2}(4,2^e) = \Gamma\langle\iota\rangle$ in case S with $d = 4$ and q even, and $A = \Gamma$ otherwise. Let $^-$ represent reduction modulo scalars. Note that $\overline{A} = \mathrm{Aut}(\overline{\Omega})$.

Theorem 1.1 *Let G be a group with $\Omega \leq G \leq A$, where $\overline{\Omega}$ is nonabelian simple. Then generators of the intersection with Ω of all of the maximal subgroups of G that do not lie in $\mathcal{S}$, up to conjugacy in* $\mathrm{GL}(d,q)$*,* $\mathrm{GSp}(d,q)$ *or* $\mathrm{GU}(d,q)$*, can be calculated and written down in time $O(d^3 \log d \log^3 q)$.*

We briefly comment on the maximal subgroups of the other families of almost simple groups. The theory of the maximal subgroups of the alternating and symmetric groups is well-understood, and they can be divided into classes using the O'Nan–Scott Theorem. Work of Liebeck, Praeger and Saxl [17] determines the maximality of groups in each O'Nan–Scott class other than the almost simple case, as well as of the intransitive and imprimitive groups. A second paper by the same authors determines when one almost simple group is contained in another [16]. This can be combined with Dixon and Mortimer's classification [7] of the primitive almost simple groups of degree less than 1000 to give an explicit list of maximal subgroups of the alternating and symmetric groups of degree less than 1000. The usual approach when computing with the alternating and symmetric groups is to use constructive recognition [2] to find an isomorphism from the input group to the natural representation of $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$. Generic functions write down the maximal intransitive and imprimitive groups in their natural representation, and a database of primitive groups is used for the rest.

The situation with the sporadic groups is somewhat different. The maximal subgroups of all sporadics, other than the Monster, are known. To construct these subgroups, one usually finds standard generators for the sporadic, and then writes down the generators of the maximal subgroups as words in these standard generators. This can be done for all maximal subgroups of sporadics of "reasonable" permutation degree: the online Atlas of Finite Group Representations [24] is a good source of such information.

The theory of the maximal subgroups of the exceptional groups is reasonably well-understood [18], and the maximals are known explicitly in many cases. The exceptional groups are generally treated in the same way as the sporadics: since they have very few low degree permutation representations, this is perfectly appropriate.

Up to now, the classical groups have also been treated as sporadics. This is increasingly unacceptable, as too many classical groups have moderate degree permutation representations, and the relevant databases are rapidly becoming unwieldy. This paper presents a solution to this problem.

The layout of the remainder of the paper is as follows. In Section 2, we introduce some notation and state a number of general lemmas and a summary of the Aschbacher classes. In Section 3, we describe how to conjugate a group preserving a non-degenerate form of symplectic, unitary or orthogonal type on a vector space over a finite field to a group which preserves any other form of the same type. In the remaining sections, we present our algorithms for each of the eight geometric families of subgroups in Aschbacher's theorem, before finishing with the subgroups of $\Gamma\mathrm{Sp2}(4, 2^e)$.

2 Notation and mathematical preliminaries

We let (a, b) denote the greatest common divisor of integers a and b, and $[a, b]$ their least common multiple.

When describing the structure of groups, the symbol $[n]$, where $n \in \mathbb{N}$, denotes a soluble group of order n of unspecified structure.

As usual, I_r will denote the $r \times r$ identity matrix over $\mathrm{GF}(q)$. We define the elementary matrix $E_{i,j}$ to be the square matrix with 1 in position (i, j) and 0 elsewhere: the dimension of $E_{i,j}$ will always be clear from its context. A matrix A is *block diagonal* if it is a block matrix, and all nonzero blocks have their main diagonal on the main diagonal of A. We write block diagonal matrices as $\mathrm{Diag}[X_1, \ldots, X_s]$, where $X_i \in \mathrm{GL}(d/s, q)$ for $1 \leq i \leq s$.

We shall assume throughout that integer operations require constant time. We also assume that primitive polynomials, together with associated primitive field elements, are known for all finite fields that arise, and that elements of $\mathrm{GF}(p^e)$ are represented as polynomials of degree $e-1$ over $\mathrm{GF}(p)$. Thus field operations in $\mathrm{GF}(q)$ require time $O(\log q)$, elements of $\mathrm{GL}(d, q)$ can be constructed in time $O(d^2 \log q)$.

By the results proved in Chapters 15 and 16 of [3], matrix multiplication, and other basic matrix operations such as inversion, echelonization, nullspace and determinant computation, all have time complexity $\Theta(d^\Psi \log q)$ for the same value of Ψ, where $2 \leq \Psi < 3$; in fact it has been proved that $\Psi < 2.38$. The complexity estimates in many of the results in this paper will be stated in terms of this constant Ψ. For small fields the implementations of matrix multiplication usually have time complexity $O(d^3 \log q)$, for prime finite fields of size $> 2^{16}$, MAGMA uses an algorithm due to Strassen [22] for which $\Psi = \log_2(7)$. We shall not assume the availability of discrete logarithms.

The Kronecker product $A \otimes B$ of two $d \times d$ matrices A and B is the $d^2 \times d^2$ matrix C, where the $((i-1)d + k, (j-1)d + l)$ entry of C is $A_{ij}B_{kl}$

for $1 \leq i, j, k, l \leq d$. The $\otimes$ operation is associative, and $(A \otimes B)(C \otimes D) = AC \otimes BD$ for all $d \times d$ matrices A, B, C, D. Note that the Kronecker product of two $d \times d$ matrices can be written down in time $O(d^4 \log q)$, as each of the d^4 entries requires a single field operation.

Lemma 2.1 *Let $d \in \mathbb{N}$. The number of prime divisors of d is $O(\log d)$. The average number of prime divisors of d is $\log \log d$. The number of divisors of d is $O(d^\epsilon)$ for any real $\epsilon > 0$.*

PROOF: The first statement is clear. For the second, see [11, Thm 430], and for the third, see [11, Thm 315]. □

Throughout, we will let p be a prime, and set $q := p^e$.

Lemma 2.2 *Let $\alpha \in \mathrm{GF}(q)$. There are Las Vegas $O(\log q)$ time algorithms for finding $\beta \in \mathrm{GF}(q^2)$ such that $\beta + \beta^q = \alpha$ and $\gamma \in \mathrm{GF}(q^2)$ such that $\gamma^{q+1} = \alpha$.*

PROOF: For the first problem, we find an element $\delta \in \mathrm{GF}(q)$ such that the polynomial $x^2 - \alpha x + \delta$ is irreducible over $\mathrm{GF}(q)$. This is known to be the case for almost exactly half of the $\delta \in \mathrm{GF}(q)$, so we can find such a polynomial quickly by using random choices of δ. By Theorem 8.12 of [9], for example, we can test the irreducibility of the polynomial over $\mathrm{GF}(q)$ and factorise it over $\mathrm{GF}(q^2)$ in time $O(\log q)$. Since $\beta \mapsto \beta^q$ is a field automorphism of $\mathrm{GF}(q^2)$ that fixes $\mathrm{GF}(q)$, the roots of $x^2 - \alpha x + \delta$ are $\beta, \beta^q \in \mathrm{GF}(q^2)$ with $\beta + \beta^q = \alpha$.

Similarly, for the second problem, we find $\delta \in \mathrm{GF}(q)$ such that $x^2 + \delta x + \alpha$ is irreducible over $\mathrm{GF}(q)$, then the roots $\gamma, \gamma^q \in \mathrm{GF}(q^2)$ satisfy $\gamma^{q+1} = \alpha$. □

By *constructing* a group we mean producing a set of generating elements for the group: this will generally be a set of matrices. Throughout, we will let ζ be a primitive multiplicative element of $\mathrm{GF}(q)$ in cases L and S, and of $\mathrm{GF}(q^2)$ in case U. The following lemmas are taken from [21].

Lemma 2.3 *Given ζ, the groups $\mathrm{GL}(d, q)$, $\mathrm{Sp}(d, q)$ and $\mathrm{GSp}(d, q)$ can be constructed in time $O(d^2 \log q)$. The groups $\mathrm{SU}(d, q)$ and $\mathrm{GU}(d, q)$ can be constructed in time $O(d^2 \log q + \log^2 q)$.*

Lemma 2.4 *For ε in $\{+, -, \circ\}$, each of the groups $\Omega^\varepsilon(d, q)$, $\mathrm{SO}^\varepsilon(d, q)$, $\mathrm{O}^\varepsilon(d, q)$ and $\mathrm{GO}^\varepsilon(d, q)$ can be constructed in time $O(d^\Psi \log q + \log^3 q)$, given a primitive field element ζ. The generators of $\mathrm{GO}^\varepsilon(d, q)$ include matrices A and*

B generating $\mathrm{SO}^{\varepsilon}(d,q)$*, an element* $D_{\epsilon} \in \mathrm{O}^{\epsilon}(d,q)$ *of determinant* -1*, and for* $\varepsilon \in \{+,-\}$*, an element* $E_{\varepsilon} \in \mathrm{GO}^{\varepsilon}(d,q) \setminus \mathrm{O}^{\varepsilon}(d,q)$*. We have* $\mathrm{Det}(E_-) = (-\zeta)^{d/2}$ *and* $\mathrm{Det}(E_+) = \zeta^{d/2}$.

In fact, Lemma 2.4 is proved in [21] with 3 in place of Ψ in the complexity estimate. A more detailed analysis of the computations involved in this construction shows that the operations involved are all either matrix operations that are known to have time complexity $O(d^{\Psi} \log q)$, or transformations of orthogonal and quadratic forms, which will be discussed in detail in Section 3. The specific form transformations involved can all be carried out using a permutation of the basis, a scalar operation, and an operation on a 2×2 matrix so, as in Proposition 3.2 below, they can be done in time $O(d^2 \log q)$. This justifies our use of $O(d^{\Psi} \log q + \log^3 q)$ in the above lemma.

We conclude this section with a brief description of the classes of subgroups of the classical groups G that arise in Aschbacher's theorem. The maximal subgroups of $\Gamma\mathrm{Sp}2(4, 2^e)$ are described in Section 12.

Suppose that G is defined over $\mathrm{GF}(q)$ and acts on a vector space V of dimension d. Groups in $\mathcal{C}_1$ act reducibly on V. Those in $\mathcal{C}_2$ are imprimitive; that is, they preserve a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$. Groups in $\mathcal{C}_3$ are *semilinear*; that is, they can be embedded in $\Gamma\mathrm{L}(d/s, q^s)$ for some $s > 1$. Groups in $\mathcal{C}_4$ preserve a tensor product decomposition $V = V_1 \otimes V_2$. Those in $\mathcal{C}_5$ can be defined, modulo scalars, over a proper subfield of $\mathrm{GF}(q)$. Those in $\mathcal{C}_6$ normalise an extraspecial or symplectic-type group that acts irreducibly on V. Groups in $\mathcal{C}_7$ preserve a homogeneous tensor decomposition $V = V_1 \otimes \cdots \otimes V_t$ with $t > 1$, where the $\dim(V_i)$ are all equal. Those in $\mathcal{C}_8$ normalise a proper classical group over $\mathrm{GF}(q)$ in its natural representation. Finally, the groups in $\mathcal{C}_9 = \mathcal{S}$ are almost simple modulo scalars, and do not lie in any class $\mathcal{C}_i$ for $i = 3, 5$ or 8.

3 Transformation of forms

The following situation arises frequently when constructing subgroups of classical groups. We have an absolutely irreducible matrix group G of dimension d, which is known to fix a bilinear or sesquilinear form of full rank d over $\mathrm{GF}(q)$ (or $\mathrm{GF}(q^2)$ in the unitary case). The type of the fixed form, which may be symplectic, unitary, or orthogonal (of plus or minus type when d is even), is also known. In the orthogonal case with q even, G is also known to fix a quadratic form.

Our aim is to find a conjugate of G which is a subgroup of the standard copy of the relevant classical group, namely $\mathrm{Sp}(d,q)$, $\mathrm{GU}(d,q)$ or $\mathrm{O}^{\pm}(d,q)$. We first find the form fixed by G as a $d \times d$ matrix A. Then we find a basis change that transforms A to a fixed standard version F of the form. Notice that if G preserves a symplectic form A, then G^X preserves $X^{-1}AX^{-T}$, and similarly for the other types of form. In the case of orthogonal groups and even q, we also find the matrix Q of a quadratic form of plus or minus type fixed by G, and transform Q rather than A to a standard version F. In fact, since the group preserving the bilinear or quadratic form is unchanged if we multiply this form by a scalar matrix, it suffices to transform A to a scalar multiple of F.

It is convenient to choose the standard versions F of the forms as follows. In the symplectic case, $F = \mathrm{AntiDiag}[1,\ldots,1,-1,\ldots,-1]$; that is, $F_{i,d+1-i} = 1$ for $1 \le i \le d/2$, then $F_{i,d+1-i} = -1$ for $d/2+1 \le i \le d$, and $F_{ij} = 0$ otherwise. In the unitary case, $F = I_d$. In the orthogonal case with q odd, we have $F = I_d$ if d is odd, and $F = I_d$ or $I'_d := \mathrm{Diag}[1,\ldots,1,\zeta]$ when d is even.

It should be noted that the form fixed by the 'standard copy' of $\mathrm{SU}(d,q)$ as returned by MAGMA, for example, is $\mathrm{AntiDiag}[1,\ldots,1]$ rather than I_d. When writing down the subgroups of $\mathrm{SU}(d,q)$ arising in Thereom 1.1, it will sometimes be convenient to use I_d and sometimes to use $\mathrm{AntiDiag}[1,\ldots,1]$ as our standard form. We shall show in Subsection 3.2 that we can conjugate a matrix preserving one of these forms to one preserving the other in time $O(d^2 \log q)$. It will turn out that the total number of generators of all subgroups of $\mathrm{SU}(d,q)$ that arise is $O(d)$, and so we can freely move between one form and the other without affecting the result of Theorem 1.1.

Similarly, it is sometimes convenient to use $\mathrm{AntiDiag}[1,\ldots,1]$ as the standard orthogonal form of plus type in odd characteristic. Again, we can transform I_d or $\mathrm{Diag}[1,\ldots,1,\zeta]$ to $\mathrm{AntiDiag}[1,\ldots,1]$ in time $O(d^2 \log q)$.

In the orthogonal case with q even, d is necessarily even, because the groups $\mathrm{O}(2m+1,2^n)$ are reducible. We choose our standard quadratic form to be

$$\begin{pmatrix} 0_{ee} & 0_{e2} & J \\ 0_{2e} & \begin{matrix} a & b \\ 0 & c \end{matrix} & 0_{ee} \\ 0_{ee} & 0_{e2} & 0_{ee} \end{pmatrix}, \qquad (*)$$

where $e = d/2-1$, 0_{kl} denotes a $k \times l$ zero matrix, and $J := \mathrm{AntiDiag}[1,\ldots,1]$. For a form of plus type, we have $b = 1$ and $a = c = 0$, so the quadratic form is $x_1x_d + x_2x_{d-1} + \ldots + x_{d/2}x_{d/2+1}$.

For a form of minus type, we need to choose a, b, c such that $ax^2 + bx + c$ is irreducible, and there is no canonical solution. In our implementation, we use the matrix of the quadratic form fixed by $\mathrm{SO}^-(d, q)$ in MAGMA.

We shall now describe our algorithms to solve these problems for the individual types of forms. The methods used to transform A to F are all similar. First we use elementary linear algebra to transform A to F', which has zero entries wherever F does. Then we transform F' to a scalar multiple of F, which is sufficient for our requirements.

Since we know, from the results proved in Chapter 16 of [3], that the time complexity of many types of matrix operations over finite fields is $O(d^\Psi \log q)$, it seems likely that the results proved in this section could all be improved from time $O(d^3 \log q)$ to time $O(d^\Psi \log q)$. But we have been unable to find all of the necessary results of this type in the literature. In any case, our current implementations are $O(d^3 \log q)$.

In all cases, we let $g_1, \ldots, g_r$ be the generators of G, which are $d \times d$ matrices over $\mathrm{GF}(q)$, or over $\mathrm{GF}(q^2)$ in the unitary case. We let the natural basis of the vector space on which G is acting be $[e_1, \ldots, e_d]$.

3.1 Symplectic forms

First we need to find the matrix of the symplectic form $A = -A^{\mathrm{T}}$ fixed by G, which must satisfy $g_i A g_i^{\mathrm{T}} = A$ or, equivalently, $g_i A = A\,(g_i^{-1})^{\mathrm{T}}$ for $1 \le i \le r$. In other words, if M is the d-dimensional G-module over $\mathrm{GF}(q)$ defined by G, and M^* is the dual of M obtained by inverting and transposing the matrices for M, then we are looking for a module isomorphism A from M to M^*. Since we are assuming that G acts absolutely irreducibly on M, A is uniquely determined up to multiplication by a scalar. We can find A by the Las Vegas $O(d^3 \log q)$ time algorithm for testing isomorphism between irreducible modules defined over finite fields, which is described in [13, Section 4].

Proposition 3.1 *Let A be the matrix of a symplectic form preserved by a group G. In time $O(d^3 \log q)$ a matrix X can be constructed such that G^X preserves our standard symplectic form.*

PROOF: We first describe how to transform A to an antidiagonal matrix F'. By interchanging co-ordinates if necessary, we may assume that $A_{1d} \neq 0$. Let

X_1 be a change of basis matrix for this: it is clear that we may construct X_1 in time $O(d^2 \log q)$. Then, for $2 \le i \le d-1$, we replace e_i by $e_i - A_{1i}A_{1d}^{-1}e_d$, and leave e_1 and e_d unchanged. The transformed form A then has all entries in the first row and column equal to 0, except for the $(1, d)$ and $(d, 1)$ entries. By repeating this process on the other rows and columns of A, we can transform A to an antidiagonal matrix F'. The change of basis matrix to transform each row has all nondiagonal entries equal to zero except for one column, so we can construct a change of basis matrix X_2 representing the products of these $O(d)$ operations in time $O(d^2 \log q)$.

To transform F' to F, we replace e_i by $(F')^{-1}_{i,d+1-i}e_i$ for $1 \le i \le d/2$ and leave the remaining e_i unchanged. Let X_3 be the diagonal change of basis matrix for this transformation. Then $X := (X_1X_2X_3)^{-1}$. □

3.2 Unitary forms

In this case the matrices g_i are defined over $\mathrm{GF}(q^2)$. For a matrix X over $\mathrm{GF}(q^2)$, let X^* be the result of transposing X and then replacing all entries of X by their q-th power; that is by their image under the field automorphism of $\mathrm{GF}(q^2)$ that fixes $\mathrm{GF}(q)$. Then, the matrix A of the unitary form fixed by G satisfies $g_iAg_i^* = A$, or equivalently $g_iA = A(g_i^{-1})^*$, for $1 \le i \le r$. As in the symplectic case, finding A can be done by a module isomorphism test. For a unitary form, we require $A = A^*$. At this stage, we only know that some scalar multiple λA of A satisfies $\lambda A = (\lambda A)^*$.

Proposition 3.2 *Let A be the matrix of a unitary form preserved by a group G. In time $O(d^3 \log q)$ a matrix X can be constructed such that G^X preserves the standard unitary form I_d.*

We can also write down a matrix Y having at most $2d$ nonzero entries that transforms I_d to AntiDiag$[1, \ldots, 1]$*, and hence conjugate each matrix of G^X to one preserving* AntiDiag$[1, \ldots, 1]$ *in time $O(d^2 \log q)$.*

Proof: First we make a basis change to transform A to a diagonal matrix F', using a similar method to Proposition 3.1. By multiplying F' by a scalar matrix, we may assume that $F'_{11} = 1$. The fact that $\lambda F'_i = (\lambda F'_i)^*$ for some λ means that $\lambda F'$ has its entries in $\mathrm{GF}(q)$. But then $F'_{11} = 1 \in \mathrm{GF}(q)$ implies that $\lambda \in \mathrm{GF}(q)$ and so we must already have $F' = (F')^*$.

To transform F' to the identity matrix F, we replace e_i by τ_ie_i, where τ_i satisfies $\tau_i^{1+q} = (F')^{-1}_{ii}$ for $1 \le i \le d$. By Lemma 2.2, we can find such a τ_i in time $O(\log q)$ for each i, so we transform F' to F in time $O(d \log q)$.

For the final statement, observe that transforming AntiDiag$[1,\dots,1]$ to I_d reduces to $\lfloor d/2 \rfloor$ transformations. $\square$

3.3 Orthogonal forms

We find the orthogonal form A fixed by G exactly as we did in the symplectic case, but now we have $A = A^{\mathrm{T}}$.

Proposition 3.3 *Let q be odd, and let $G \leq \mathrm{GL}(d,q)$ preserve a known orthogonal form A. In time $O(d^3 \log q)$ a matrix X can be constructed such that G^X preserves our standard orthogonal form.*

PROOF: We can transform A to diagonal F' in a similar way to the symplectic and unitary cases. Then, by replacing the basis vectors e_i by multiples $\tau_i e_i$, we can effectively multiply the elements of F' by arbitrary squares in $\mathrm{GF}(q)$, and hence we can assume that all of the diagonal entries of F' are equal either to 1 or to some fixed non-square, which we can take to be our given primitive element ζ of $\mathrm{GF}(q)$.

Now, if i and j are two indices with $F'_{ii} = F'_{jj}$, by means of a basis change which maps $e_i \mapsto e_i + \lambda e_j$, and $e_j \mapsto \lambda e_i - e_j$, we can multiply both F'_{ii} and F'_{jj} by $\lambda^2 + 1$ for any $\lambda \in \mathrm{GF}(q)$. So, by choosing λ such that $\lambda^2 + 1$ is a non-square (and roughly half of the $\lambda \in \mathrm{GF}(q)$ have that property) we can change entries of F' in pairs from squares to non-squares, and vice versa. Hence, if d is odd we can transform F' to either $F = I_d$ or to ζF. If d is even, we can transform F' either to I_d or to I'_d, as defined above. $\square$

As in the proof of Proposition 3.2 we can show that, for a form of plus type, I_d or to I'_d can be transformed in time $O(d^2 \log q)$ to AntiDiag$[1,\dots,1]$, which is sometimes more convenient to use as the standard form.

Now suppose that q and d are even. If a matrix Q represents a quadratic form then, for $j \neq i$, the values of Q_{ij} and Q_{ji} are not individually significant. It is their sum $Q_{ij} + Q_{ji}$ which represents the coefficient of $x_i x_j$ in the quadratic form. We therefore replace any such Q by the unique upper triangular matrix Q^u which represents the same form as Q. Then G preserves Q if and only if $(g_i Q g_i^{\mathrm{T}})^u = Q^u$ for $1 \leq i \leq r$.

In fact the orthogonal forms preserved by the groups $\mathrm{O}^{\pm}(d, 2^n)$ are symplectic, so the matrices A satisfy $A_{ii} = 0$ for $1 \leq i \leq d$. We wish to find a quadratic form preserved by G, given that G preserves a known orthogonal form A with this property. Since A is symmetric, we can write $A = U + U^{\mathrm{T}}$, where U is strictly upper-triangular. Then

$$U + U^{\mathrm{T}} = g_i(U + U^{\mathrm{T}})g_i^{\mathrm{T}} = g_iUg_i^{\mathrm{T}} + g_iU^{\mathrm{T}}g_i^{\mathrm{T}}$$

so the off-diagonal entries of $U^u = U$ and $(g_iUg_i^{\mathrm{T}})^u$ are equal for $1 \le i \le d$.

Indeed, if D is a diagonal matrix with entries δ_i on the diagonal, then $g_iDg_i^{\mathrm{T}}$ is symmetric, so the off-diagonal entries of $U+D$ and $(g_i(U+D)g_i^{\mathrm{T}})^u$ are also equal, and requiring that their diagonal entries are equal gives rise to a system of linear equations in the n unknowns δ_i. We are assuming that G fixes a form, so the equations must have a solution, which can found in time $O(d^3 \log q)$. The required quadratic form preserved by G is $Q := U+D$.

Proposition 3.4 *Let $G \le \mathrm{GL}(d, 2^n)$ preserve a known quadratic form Q of plus or minus type. Then in time $O(d^3 \log q)$ a matrix X can be constructed such that G^X preserves our chosen quadratic form.*

PROOF: Suppose that $d > 2$, and recall our choice $(*)$ of a standard form. Since Q is non-degenerate, the off-diagonal entries are not all zero, for otherwise the form would be $(\sqrt{Q_{11}}x_1 + \ldots + \sqrt{Q_{dd}}x_d)^2$. So by interchanging co-ordinates if necessary, we may assume that $Q_{1d} \ne 0$. The form is

$$Q_{11}x_1^2+Q_{12}x_1x_2+\ldots+Q_{1d}x_1x_d+\ldots = x_1(Q_{11}x_1+Q_{12}x_2+\ldots+Q_{1n}x_d)+\ldots$$

so by replacing x_d by $Q_{11}x_1 + Q_{12}x_2 + \ldots + Q_{1d}x_d$, we make $Q_{1i} = 0$ for $1 \le i < d$ and $Q_{1d} = 1$. By a similar change to x_1, we can achieve $Q_{id} = 0$ for $2 \le i \le d$. By repeating this process, we can transform Q to a matrix with structure $(*)$ in time $O(d^3 \log q)$.

This reduces us to the case $d = 2$, where the quadratic is $\kappa x_1^2+\lambda x_1x_2+\mu x_2^2$. If this factorises to $(sx_1 + tx_2)(ux_1 + vx_2)$ then Q is of plus type, and we change co-ordinates to $sx_1 + tx_2$, $ux_1 + vx_2$ to bring Q to the standard form.

Otherwise, $\kappa x_1^2+\lambda x_1x_2+\mu x_2^2$ is irreducible over $\mathrm{GF}(q)$, the form is of minus type, and we wish to transform it to a standard irreducible $ax_1^2+bx_1x_2+cx_2^2$. In other words, we must find $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q)$ with

$$\left[\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \kappa & \lambda \\ 0 & \mu \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\right]^u = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.$$

We know that there is a solution, and the stabiliser $\mathrm{O}^-(2, q)$ of the form in $\mathrm{GL}(2, q)$ acts transitively on the one-dimensional subspaces of $\mathrm{GF}(q)^2$, so there is always a solution with $\alpha = 0$. The matrix equation then reduces to the three equations $\beta^2\mu = a$, $\gamma\beta^2 = b$, $\gamma^2\kappa + \gamma\delta\beta + \delta^2\mu = c$ which enable us to find β, γ and δ. □

4 Reducible groups

Sections 4 to 11 all have a similar structure. We first summarise the groups to be constructed in Theorem 1.1 that arise in the Aschbacher class under consideration in that section. We then go on to treat cases L, S, and U in detail. In case S with $d = 4$ and q even, we will postpone the discussion of the subgroups of groups that contain a graph automorphism until Section 12.

In case L, we shall denote the natural basis of $V := \mathrm{GF}(q)^d$ by $[e_1, \ldots, e_d]$. In case S, we put $l := d/2$, and let $[e_1, \ldots, e_l, f_l, \ldots, f_1]$ be a symplectic basis for $\mathrm{GF}(q)^d$, where the matrix F of the symplectic form fixed by $\mathrm{Sp}(d, q)$ is antidiagonal with entries 1 in the first l rows and -1 in the final l rows. In case U, we may do one of two things. We may use a basis $[e_1, \ldots, e_{d/2}, f_{d/2}, \ldots, f_1]$ if d is even, and $[e_1, \ldots, e_{\lfloor d/2 \rfloor}, w, f_{\lfloor d/2 \rfloor}, \ldots, f_1]$ if d is odd, where the matrix F of the unitary form fixed by $\mathrm{SU}(d, q)$ is $\mathrm{AntiDiag}[1, \ldots, 1]$. We may alternatively use an orthonormal basis $[v_1, \ldots, v_d]$, with form matrix $F = I_d$.

In this section we describe how to write down generators of conjugacy class representatives of the reducible subgroups G of Ω that arise in Theorem 1.1. Such a group G is the stabiliser of a space W of dimension k, or the stabiliser of spaces W and U of dimension k and $d - k$, as described in Table 1, which comes from Table 4.1.A of [15]. Note the abbreviations t.s. for totally singular, and n.d. for nondegenerate.

The meanings of the "types" in the second column of Table 1 are as follows. The groups of type P_k are *parabolic* subgroups, which are the stabilisers of totally singular k-dimensional subspaces. A group of type $P_{k,d-k}$ is the stabiliser of both a k-dimensional subspace W and a $(d-k)$-dimensional subspace U containing U: these groups are non-maximal in $\mathrm{PSL}(d, q)$ but extend to maximal subgroups of $\mathrm{PSL2}(d, q)$. Groups of type $\mathrm{GL}(k, q) \oplus \mathrm{GL}(d-k, q)$ stabilise a space W of dimension k and a $(d-k)$-dimensional complement U of W: as in the previous row these groups are only maximal in groups containing a graph automorphism. Groups of type $\mathrm{Sp}(k, q) \perp \mathrm{Sp}(d-k, q)$ stabilise a nondegenerate symplectic subspace W of dimension k and a complement U to W (which is also nondegenerate). Groups of type $\mathrm{GU}(k, q) \perp \mathrm{GU}(d-k, q)$ stabilise a nondegenerate unitary subspace W of dimension k and a complement U to W (which is also nondegenerate).

Table 1: Maximal Reducible Groups

Case	Type	Description	Conditions
L, S, U	P_k	W t.s.	$1 \leq k \leq d/2$
L	$P_{k,d-k}$	$W < U$	$1 \leq k < d/2$
L	$\mathrm{GL}(k,q) \oplus \mathrm{GL}(d-k,q)$	$W \cap U = 0$	$1 \leq k < d/2$
S	$\mathrm{Sp}(k,q) \perp \mathrm{Sp}(d-k,q)$	W n.d.	k even, $1 \leq k < d/2$
U	$\mathrm{GU}(k,q) \perp \mathrm{GU}(d-k,q)$	W n.d.	$1 \leq k < d/2$

4.1 Linear reducible groups

Proposition 4.1 *A set of representatives for the k-space stabilisers P_k in* $\mathrm{SL}(d,q)$ *can be constructed in time $O(d^3 \log q)$.*

PROOF: Let G be the stabiliser of $\langle e_1, \dots, e_k \rangle$ in $\mathrm{SL}(d,q)$, then by [15, §4.1] $G \cong [q^{k(d-k)}] : (\mathrm{SL}(k,q) \times \mathrm{SL}(d-k,q)).(q-1)$, and consists of all matrices of determinant 1 whose top right corner is a $k \times (d-k)$ block of zeros.

We generate $\mathrm{SL}(k,q) \times \mathrm{SL}(d-k,q)$ with 4 block matrices A_i, for $1 \leq i \leq 4$, in the obvious fashion, with $\mathrm{SL}(k,q)$ acting on $\langle e_1, \dots, e_k \rangle$ and $\mathrm{SL}(d-k,q)$ acting on $\langle e_{k+1}, \dots, e_d \rangle$. Identify $\mathrm{SL}(k,q)$ and $\mathrm{SL}(d-k,q)$ with the direct factors that we have just constructed.

Next we define $A_5 := \mathrm{Diag}[\zeta, 1, \dots, 1, \zeta^{-1}] \in \mathrm{SL}(d,q)$. Then $\langle A_i : 1 \leq i \leq 5 \rangle \cong (\mathrm{SL}(k,q) \times \mathrm{SL}(d-k,q)).(q-1)$.

Finally we define $T := t_{\omega_{k+1},e_1} = I_d + E_{(k+1),1}$, where $[\omega_1, \dots, \omega_d]$ is the dual basis to $[e_1, \dots, e_d]$ and, for $u \in V$ and $\omega \in V^*$, the transvection $t_{\omega,u}$ is defined by $t_{\omega,u}(v) = v + \omega(v)u$ for $v \in V$. We wish to prove that $|\langle T \rangle^{\langle A_i : 1 \leq i \leq 4 \rangle}| = q^{k(d-k)}$.

For all $X \in \mathrm{GL}(d,q)$, we have $X^{-1} t_{\omega_{k+1},e_1} X = t_{\omega_{k+1}X, e_1X}$. If $X \in \mathrm{SL}(k,q)$ then $\omega_{k+1}X = \omega_{k+1}$ and $\{e_1X : X \in \mathrm{SL}(k,q)\}$ contains a $\mathrm{GF}(p)$ basis for $\langle e_1, \dots, e_k \rangle$. Similarly, if $X \in \mathrm{SL}(d-k,q)$ then $e_iX = e_i$ for $1 \leq i \leq k$, but $\{\omega_{k+1}X : X \in \mathrm{SL}(d-k,q)\}$ contains a basis for $\langle \omega_{k+1}, \dots, \omega_d \rangle$. Thus T may be conjugated to any transvection $t_{\omega,v}$ where $v \in \langle e_1, \dots, e_k \rangle$ and $\omega \in \langle \omega_{k+1}, \dots, \omega_d \rangle$. These generate a group of order $q^{k(d-k)}$, as required.

Thus up to conjugacy $G = \langle A_i, T : 1 \leq i \leq 5 \rangle$. Since each matrix is constructed in time $O(d^2 \log q)$ and there are $O(d)$ classes of such stabilisers, the total time requirement is $O(d^3 \log q)$. □

The two types of linear reducible groups in the second section of Table 1 arise as the intersection of the maximal subgroups of $\mathrm{GL}(d,q)\langle\iota\rangle$ with $\mathrm{SL}(d,q)$, where ι is the graph automorphism.

Proposition 4.2 *A set of representatives for the intersections of the maximal reducible subgroups of* $\mathrm{GL}(d,q)\langle\iota\rangle$ *with* $\mathrm{SL}(d,q)$ *can be constructed in time* $O(d^3 \log q)$.

PROOF: There are two types of group G to construct. The first stabilises a k-space U and a $(d-k)$-space W such that $U \cap W = \{0\}$. The second stabilises a k-space U and a $(d-k)$-space W with $U < W$. In both cases $k < d/2$.

In the first case $G \cong (\mathrm{SL}(k,q) \times \mathrm{SL}(d-k,q)).(q-1)$, by [15, §4.1]. The group G consists of block diagonal matrices, where the first block has size $k\times k$ and the second block has size $(d-k)\times(d-k)$. The first block can be any matrix from $\mathrm{GL}(k,q)$. The second can then be any element of $\mathrm{GL}(d-k,q)$ whose determinant is the inverse of the determinant of the first block.

Let A_i, for $1 \leq i \leq 5$, be as in Proposition 4.1, then up to conjugacy $G = \langle A_i \ : \ 1 \leq i \leq 5\rangle$.

In the second case, let G be the stabiliser in $\mathrm{SL}(d,q)$ of the subspaces $\langle e_1,\dots,e_k\rangle$ and $\langle e_1,\dots,e_{d-k}\rangle$. Then $G \cong [q^{2dk-3k^2}].(\mathrm{SL}(k,q)^2 \times \mathrm{SL}(d-2k,q)).(q-1)^2$. The group G consists of all matrices of the form:

$$\begin{pmatrix} A & 0 & 0 \\ B & C & 0 \\ D & E & F \end{pmatrix},$$

where $A \in \mathrm{GL}(k,q)$, $C \in \mathrm{GL}(d-2k,q)$, $F \in \mathrm{GL}(k,q)$, and $\mathrm{Det}(A)\mathrm{Det}(C)\mathrm{Det}(F) = 1$.

We define $\{X_i : 1 \leq i \leq 6\}$ to generate $H := \mathrm{SL}(k,q) \times \mathrm{SL}(d-2k,q) \times \mathrm{SL}(k,q)$ in the obvious fashion. Let D_1 and D_2 be diagonal matrices, where both have ζ in row 1, matrix D_1 has ζ^{-1} in row $k+1$, matrix D_2 has ζ^{-1} in row $d-k+1$, and both have 1s elsewhere. Clearly $\langle D_1, D_2\rangle \cong (q-1)^2$ and normalises H.

Finally, we let matrix $T_1 := I_d + E_{k+1,1}$, matrix $T_2 := I_d + E_{d-k+1,1}$, and matrix $T_3 := I_d + E_{d-k+1,k+1}$. In a similar fashion to Proposition 4.1 one may show that $P_1 := \langle T_1\rangle^H$ has order $q^{k(d-2k)}$, and by symmetry that the same is true for $P_3 := \langle T_3\rangle^H$. Similarly, $P_2 := \langle T_2\rangle^H$ has order q^{k^2}. Since

$\langle H, D_1, D_2\rangle$ fixes $\langle e_1, \ldots, e_k\rangle$ and $\langle e_1, \ldots, e_{d-k}\rangle$ the groups P_i have trivial pairwise intersections, and so $G = \langle H, D_1, D_2, T_1, T_2, T_3\rangle$.

Each of the $O(d)$ groups requires at most 11 generating matrices, each of which can be written down in time $O(d^2 \log q)$. $\square$

4.2 Symplectic reducible groups

Proposition 4.3 *A set of representatives of the maximal reducible subgroups of* $\mathrm{Sp}(d, q)$ *that stabilise isotropic* k*-spaces can be constructed in time* $O(d^3 \log q)$*.*

Proof: Let G be the stabiliser in $\mathrm{Sp}(d, q)$ of the isotropic subspace $U := \langle e_1, \ldots, e_k\rangle$, then by [15, §4.1]

$$G \cong [q^{k(k+1)/2+k(d-2k)}] : (\mathrm{GL}(k, q) \times \mathrm{Sp}(d - 2k, q)).$$

The matrices in G are all matrices in $\mathrm{Sp}(d, q)$ that are of the following form:

$$\begin{pmatrix} A & 0 & 0 \\ B & C & 0 \\ D & E & F \end{pmatrix}$$

Here $A \in \mathrm{GL}(d, q)$, $F = JA^{-1\mathrm{T}J}$, for $J := \mathrm{AntiDiag}[1, \ldots, 1] \in \mathrm{GL}(k, q)$, and $C \in \mathrm{Sp}(d, q)$. The matrices B, D and E are arbitrary.

Let A_1 and A_2 generate $\mathrm{GL}(k, q)$, and define $X_i := \mathrm{Diag}[A_i, I_{d-2k}, J(A_i^{-1})^{\mathrm{T}}J]$ for $i = 1, 2$. The description in [23] of the generators A_1 and A_2 of $\mathrm{GL}(k, q)$ is particularly simple, and hence may easily be adapted to give a description of $J(A_i^{-1})^{\mathrm{T}}J$ (for $i = 1, 2$) that can be computed directly in time $O(k^2 \log q)$ rather than requiring a succession of matrix operations. We identify $\mathrm{GL}(k, q)$ with $\langle X_1, X_2\rangle$. Let B_1 and B_2 generate $\mathrm{Sp}(d - 2k, q)$, and for $i = 1, 2$ define $Y_i := \mathrm{Diag}[I_k, B_i, I_k]$. Identify $\mathrm{Sp}(d - 2k, q)$ with $\langle Y_1, Y_2\rangle$.

Next define $T_1 := I_d + E_{d,1}$. The reader may check that conjugation by elements of $\mathrm{GL}(k, q)$ can map T_1 to any matrix with 1s down the diagonal, a $(k \times k)$ block in the bottom left corner that is symmetric about the anti-diagonal, and zeros elsewhere. Conjugation by elements of $\mathrm{Sp}(d - 2k, q)$ fixes T_1. Thus $\langle T_1\rangle^{(\mathrm{GL}(k,q)\times\mathrm{Sp}(d-2k,q))}$ has order $q^{k(k+1)/2}$. If $d = 2k$ then $G = \langle X_i, Y_i, T_1 \ : \ i = 1, 2\rangle$.

If $d > 2k$ then define $T_2 := I_d + E_{d,d-k} - E_{k+1,1}$. It is routine to check that $T_2 \in \mathrm{Sp}(d, q)$, and clear that T_2 stabilises $\langle e_1, \ldots, e_k\rangle$. The argument that the normal closure of $\langle T_2 \rangle$ under $\mathrm{GL}(k,q) \times \mathrm{Sp}(d-2k,q)$ has order $q^{k(d-2k)}$ is similar to that of Proposition 4.1, as

$$\langle e_1, \ldots, e_k \rangle \perp \langle e_{k+1}, \ldots, e_l, f_l, \ldots, f_{k+1} \rangle.$$

Then $G = \langle X_i, Y_i, T_i \ : \ i = 1, 2 \rangle$.

There are $O(d)$ possibilities for G, giving a total time of $O(d^3 \log q)$. $\square$

Proposition 4.4 *A set of representatives of the maximal reducible subgroups of* $\mathrm{Sp}(d,q)$ *that stabilise symplectic subspaces may be constructed in time* $O(d^3 \log q)$*.*

Proof: Let G be the stabiliser in $\mathrm{Sp}(d,q)$ of $\langle e_1, \ldots e_k, f_k, \ldots, f_1 \rangle$, then by [15, §4.1]

$$G \cong \mathrm{Sp}(2k,q) \times \mathrm{Sp}(d-2k,q).$$

The group G consists of all matrices from $\mathrm{Sp}(d,q)$ of the form

$$\begin{pmatrix} A & 0 & B \\ 0 & C & 0 \\ D & 0 & E \end{pmatrix}, \quad \text{where} \quad \begin{pmatrix} A & B \\ D & E \end{pmatrix} \in \mathrm{Sp}(2k,q)$$

Here A, B, D, E are $k \times k$ matrices, and $C \in \mathrm{Sp}(d-2k,q)$.

Let A_1, A_2 generate $\mathrm{Sp}(2k,q)$. Let A_{ijk}, where $i,j,k \in \{1,2\}$, be $k \times k$ submatrices of A_i such that

$$A_i := \begin{pmatrix} A_{i11} & A_{i12} \\ A_{i21} & A_{i22} \end{pmatrix}.$$

For $i = 1, 2$, define $X_i \in G$ to be block matrices with A_{ijk} in the corners in the obvious fashion, and I_{d-2k} in the centre. Let B_1 and B_2 generate $\mathrm{Sp}(d-2k,q)$, and for $i = 1, 2$ define $Y_i := \mathrm{Diag}[I_k, B_i, I_k]$. Then $G = \langle X_1, X_2, Y_1, Y_2 \rangle$.

There are $O(d)$ conjugacy classes of symplectic groups stabilising isotropic subspaces, so the result follows. $\square$

4.3 Unitary reducible groups

Here we use the unitary form $F = \mathrm{AntiDiag}[1, \ldots, 1]$. Recall that, for $A \in \mathrm{GL}(d,q^2)$, we denote the matrix resulting from transposing A and then replacing all entries in A by their qth powers by A^*.

Proposition 4.5 *A set of representatives of the maximal reducible subgroups of* $\mathrm{SU}(d,q)$ *that stabilise isotropic* k*-spaces can be constructed in time* $O(d^3 \log^2 q)$.

Proof: Let $G \leq \mathrm{SU}(d,q)$ be the maximal subgroup that stabilises $U := \langle e_1, \ldots, e_k \rangle$. Then by [15, §4.1]

$$G \cong [q^{k(2d-3k)}] : (\mathrm{SL}(k,q^2) \times \mathrm{SU}(d-2k,q)).[q^2-1].$$

The group G consists of matrices of the same shape as those in Proposition 4.3.

We require various field elements. If q is odd then set $\nu := \zeta^{(q+1)/2}$, otherwise set $\nu := 1$, so that ν satisfies $\nu + \nu^q = 0$. If q is odd then let $\mu \in \mathrm{GF}(q^2)$ satisfy $\mu^{q+1} = -2$. By Lemma 2.2, μ may be found in time $O(\log q)$.

To construct G, we start by taking a direct product of $\mathrm{GL}(k,q^2)$ with $\mathrm{SU}(d-2k,q)$, where the generators A_1, A_2 of $\mathrm{GL}(k,q^2)$ act as $JA_i^{-*}J$ on $\langle f_k, \ldots, f_1 \rangle$, where $J := \mathrm{AntiDiag}[1, \ldots, 1] \in \mathrm{GL}(k,q^2)$. As in the symplectic case, we may adapt the description of the generators A_1, A_2 of $\mathrm{GL}(k,q^2)$ in [23] to describe the coefficents of $JA_i^{-*}J$, and hence we construct the direct product in time $O(d^2 \log q + \log^2 q)$.

We need two unitary transvections. The first is $T_1 := I_d + \nu E_{d,1}$. The second is $T_2 := I_d + E_{d,d-k} + E_{k+1,1}$, provided $d - 2k > 1$. If $d - 2k = 1$ then the second transvection is $T_2 := I_d + \lambda_1 E_{d,1} + \lambda_2 E_{d,\lceil d/2 \rceil} + \lambda_3 E_{\lceil d/2 \rceil,1}$, where $(\lambda_1, \lambda_2, \lambda_3) = (\zeta, 1, 1)$ if q is even, and $(1, \mu, \mu^q)$ when q is odd. The proof that the normal closure of $\langle T_1 \rangle$ has order q^{k^2}, and that the normal closure of $\langle T_2 \rangle$ has order $q^{2k(d-2k)}$, is similar to the proof of Proposition 4.3.

Finally we add a diagonal matrix, which has entry ζ in row 1, entry ζ^{-1} in row $(k+1)$, entry ζ^{-p} in row d, entry ζ^p in row $d-k$, and 1 elsewhere. If $d = 2k$ or $d = 2k+1$ we make some obvious minor variations, which we leave to the reader.

Each group is generated by at most 7 matrices, and there are $O(d)$ conjugacy classes of such groups, so the result follows. □

Proposition 4.6 *A set of representatives of the maximal reducible subgroups of* $\mathrm{SU}(d,q)$ *that fix unitary subspaces can be constructed in time* $O(d^3 \log q + \log^2 q)$.

Proof: Let $k \leq d/2$ be given, and define $U := \langle e_1, \ldots, e_{\lfloor k/2 \rfloor}, f_{\lfloor k/2 \rfloor}, \ldots, f_1 \rangle$. If k is even then let G be the stabiliser in $\mathrm{SU}(d,q)$ of $U \perp U^\perp$. If k and d

are both odd then let G stabilise $\langle U, w\rangle$ and its complement. Suppose that k is odd and d is even. Let $\alpha \in \mathrm{GF}(q^2)$ satisfy $\alpha + \alpha^q = 1$; by Lemma 2.2, α can be found in time $O(\log q)$. Let $\beta \in \mathrm{GF}(q^2)$ satisfy $\beta^{q+1} = -1$; we may set β to be $\zeta^{(q-1)/2}$ if q is odd, and 1 if q is even. The reader may verify that the vectors $w_1 := \alpha e_l + f_l$ and $w_2 := -\alpha^q \beta e_l + \beta f_l$, with $l = d/2$, are such that $U_1 := \langle U, w_1\rangle$ and $U_2 := \langle V, w_2\rangle$ are orthogonal unitary subspaces, where $V := \langle e_{\lfloor k/2\rfloor+1}, \ldots, e_{l-1}, f_{l-1}, \ldots, f_{\lfloor k/2\rfloor+1}\rangle$. We let G stabilise $U_1 \perp U_2$.

The construction of $G \cong (\mathrm{SU}(k, q)\times\mathrm{SU}(d-k, q)).(q-1)$ is straightforward, and we leave it to the reader. □

5 Imprimitive groups

In this section we describe how to construct representatives of the maximal imprimitive subgroups G of Ω that arise in Theorem 1.1. Such a group G is the stabiliser in Ω of an m-space decomposition

$$\mathcal{D} : V = V_1 \oplus \cdots \oplus V_t,$$

where $d = mt$ and $t > 1$, such that the conditions of Table 2 (Table 4.2.A of [15]) hold.

The types of the imprimitive groups are as follows. The groups of type $\mathrm{GL}(m, q) \wr \mathrm{Sym}(t)$ stabilise a decomposition of V into a direct sum of t subspaces, each of dimension m. The groups of type $\mathrm{Sp}(m, q) \wr \mathrm{Sym}(t)$ stabilise a decomposition of V into a direct sum of t nondegenerate symplectic subspaces, each of dimension m. The groups of type $\mathrm{GL}(d/2, q).2$ stabilise a decomposition of V into a direct sum of two totally singular subspaces, each of dimension $d/2$. The groups of type $\mathrm{GU}(m, q) \wr \mathrm{Sym}(t)$ stabilise a decomposition of V into a direct sum of t nondenerate unitary subspaces, each of dimension m. Finally, the groups of type $\mathrm{GL}(d/2, q^2).2$ stabilise a decomposition of V into a direct sum of two totally singular subspaces, each of dimension $d/2$ (recall that in case U the vector space V is defined over $\mathrm{GF}(q^2)$).

5.1 Linear imprimitive groups

Proposition 5.1 *A set of representatives of the maximal imprimitive subgroups of* $\mathrm{SL}(d, q)$ *can be constructed in time* $O(d^{2+\epsilon} \log q)$*, for any* $\epsilon > 0$.

Table 2: Maximal Imprimitive Groups

Case	Type	Description of V_i	Conditions
L	$\mathrm{GL}(m,q) \wr \mathrm{Sym}(t)$		
S	$\mathrm{Sp}(m,q) \wr \mathrm{Sym}(t)$	non-degenerate	
S	$\mathrm{GL}(d/2,q).2$	totally singular	q odd
U	$\mathrm{GU}(m,q) \wr \mathrm{Sym}(t)$	non-degenerate	
U	$\mathrm{GL}(d/2,q^2).2$	totally singular	

PROOF: Let $t > 1$ divide d, and for $0 \leq i \leq t-1$, set $V_{i+1} := \langle e_{im+1}, \ldots, e_{(i+1)m} \rangle$. Let G be the stabiliser in $\mathrm{SL}(d,q)$ of the decomposition $V = V_1 \oplus \cdots \oplus V_t$, and let $m := d/t$. Then by [15, §4.2]

$$G \cong \mathrm{SL}(m,q)^t.(q-1)^{(t-1)}.\mathrm{Sym}(t).$$

The group consists of all matrices in $\mathrm{SL}(d,q)$ that are composed of $m \times m$ block matrices, where each row and column can contain only one nonzero block matrix. The determinants of the first $t-1$ blocks can be chosen freely, but the final block must ensure that the determinant of the overall matrix is 1.

Let $A, B \in \mathrm{GL}(d,q)$ have the generators for $\mathrm{SL}(m,q)$ in the initial $m \times m$ block, and the identity elsewhere. Let $C, D \in \mathrm{GL}(d,q)$ be block matrices preserving $\mathcal{D}$, with blocks of size $(m \times m)$, where $C^{\mathcal{D}} := (1,2,\ldots,t)$ and $D^{\mathcal{D}} := (1,2)$. The nonzero block in rows 1 to m is defined to be $-I_m$ in C and D, unless m and t are both odd, when it is I_m in C. All other blocks in C and D are I_m, so $\mathrm{Det}(C) = \mathrm{Det}(D) = 1$. We have $\langle A,B,C,D \rangle \cong \mathrm{SL}(m,q)^t.\mathrm{Sym}(t)$ or $\mathrm{SL}(m,q)^t.2^{(t-1)}.\mathrm{Sym}(t)$.

Let $E := \mathrm{Diag}[\zeta, 1, \ldots, 1, \zeta^{-1}, 1, \ldots 1]$, with ζ^{-1} in row $m+1$. Then up to conjugacy $G = \langle A,B,C,D,E \rangle$.

The number of types of imprimitive decomposition is equal to the number of proper divisors k of d, which is $O(d^{\epsilon})$ for any real $\epsilon > 0$, by Lemma 2.1. □

5.2 Symplectic imprimitive groups

Proposition 5.2 *A set of representatives of the maximal imprimitive subgroups of* $\mathrm{Sp}(d,q)$ *that stabilise decompositions into non-degenerate subspaces can be constructed in time* $O(d^{2+\epsilon} \log q)$*, for any real* $\epsilon > 0$.

Proof: Let G be the stabiliser in $\mathrm{Sp}(d,q)$ of $\mathcal{D}: V = V_1 \oplus \cdots \oplus V_t$, where each V_i is a symplectic m-space. Then by [15, §4.2], $G \cong \mathrm{Sp}(m,q) \wr \mathrm{Sym}(t)$. Note that m is even, and set $k := m/2$. For $0 \leq i \leq t-1$ we may set $V_{i+1} := \langle e_{ik+1}, \ldots, e_{(i+1)k}, f_{(i+1)k}, \ldots, f_{ik+1} \rangle$.

Let A_1, A_2 generate $\mathrm{Sp}(m,q)$; use them to construct X_1, X_2 as in the proof of Proposition 4.4. Let $C \in \mathrm{SL}(d,q)$ interchange e_i with e_{i+k} and f_i with f_{i+k} for $1 \leq i \leq k$, and fix the other basis vectors. Let $D \in \mathrm{SL}(d,q)$ map $e_i \mapsto e_{((i+k-1) \bmod l)+1}$ and $f_i \mapsto f_{((i+k-1) \bmod l)+1}$, for $1 \leq i \leq l$. Then up to conjugacy $G = \langle X_1, X_2, C, D \rangle$.

The number of types of imprimitive decomposition is equal to the number of even proper divisors of d, namely $O(d^\epsilon)$ for any $\epsilon > 0$. □

When q is odd there is a second conjugacy class of maximal imprimitive subgroups of $\mathrm{Sp}(d,q)$.

Proposition 5.3 *A representative of the maximal imprimitive groups in* $\mathrm{Sp}(d,q)$ *that stabilise a decomposition into two isotropic subspaces can be constructed in time* $O(d^2 \log q)$.

Proof: Let G be the maximal subgroup of $\mathrm{Sp}(d,q)$ that stabilises the decomposition $\mathcal{D}: V = \langle e_1, \ldots, e_l \rangle \oplus \langle f_l, \ldots, f_1 \rangle$. Then by [15, §4.2], $G \cong \mathrm{GL}(l,q).2$. Elements of G can either stabilise each space in the decomposition, in which case they can act as any element of $\mathrm{GL}(l,q)$ on the first k-dimensional subspace provided that the action on the second k-dimensional subspace preserves the isotropic form, or they can interchange $\langle e_1, \ldots, e_l \rangle$ with $\langle f_l, \ldots, f_1 \rangle$.

Let A_1, B_1 generate $\mathrm{GL}(l,q)$, and let $J := \mathrm{AntiDiag}[1, \ldots, 1] \in \mathrm{GL}(l,q)$. Define $A := \mathrm{Diag}[A_1, J(A_1^{-1})^{\mathrm{T}} J]$ and $B := \mathrm{Diag}[B_1, J(B_1^{-1})^{\mathrm{T}} J]$. A short calculation shows that A and B preserve both F and $\mathcal{D}$, and so are in G.

Let $C := \mathrm{AntiDiag}[I_l, -I_l]$, then up to conjugacy $G = \langle A, B, C \rangle$. □

5.3 Unitary imprimitive groups

In the next proposition, we use the form $F = I_d$.

Proposition 5.4 *A set of representatives of the imprimitive maximal subgroups of* $\mathrm{SU}(d,q)$ *that stabilise decompositions into unitary subspaces can be constructed in time* $O(d^\epsilon(d^2 \log q + \log^2 q))$*, for any real* $\epsilon > 0$.

Proof: Let $t > 1$ be a divisor of d, let $m := d/t$, and for $0 \leq i \leq t-1$ set $V_{i+1} := \langle v_{im+1}, \ldots, v_{(i+1)m} \rangle$. Let G be the stabiliser in $\mathrm{SU}(d,q)$ of the decomposition $\mathcal{D} : V = V_1 \perp \cdots \perp V_t$. Then by [15, §4.2],

$$G \cong \mathrm{SU}(m,q)^t.(q+1)^{t-1}.\mathrm{Sym}(t).$$

Let A_1 and B_1 generate $\mathrm{SU}(m,q)$, and let $A := \mathrm{Diag}[A_1, I_m \ldots, I_m]$ and $B := \mathrm{Diag}[B_1, I_m, \ldots, I_m]$. Then both A and B preserve F and $\mathcal{D}$, so $A, B \in G$. Identify $\langle A, B \rangle$ with $\mathrm{SU}(m,q)$.

Let $C \in \mathrm{GL}(d,q^2)$ interchange v_i with $-v_{i+m}$, for $1 \leq i \leq m$, and fix everything else. A short calculation shows that $\mathrm{Det}(C) = 1$, and that $CC^* = I_d$, so $C \in G$. Let $D_1 \in \mathrm{GL}(d,q^2)$ map $v_i \mapsto v_{((i+m-1) \bmod d)+1}$ for $1 \leq i \leq d$. If m or q is even or t is odd, let $D = D_1$, otherwise let $D := \mathrm{Diag}[-1, 1, \ldots, 1]D_1$. It may be checked that $DD^* = I_d$ and that $\mathrm{Det}(D) = 1$.

Let $E := \mathrm{Diag}[\zeta^{q-1}, 1, \ldots, 1, \zeta^{1-q}, 1, \ldots, 1] \in \mathrm{GL}(d,q^2)$ have nontrivial entries in rows 1 and $m+1$. Then up to conjugacy $G = \langle A, B, C, D, E \rangle$.

The number of choices of t is equal to the number of proper divisors of d, which is $O(d^\epsilon)$ for any real $\epsilon > 0$. □

In the next proposition, we use the form $F := \mathrm{AntiDiag}[1, \ldots, 1]$.

Proposition 5.5 *If d is even, a representative of the maximal imprimitive subgroups of $\mathrm{SU}(d,q)$ that preserve a decomposition into two isotropic subspaces can be constructed in time $O(d^2 \log q + \log^2 q)$.*

Proof: Let G be the stabiliser in $\mathrm{SU}(d,q)$ of the decomposition $\mathcal{D} : V = \langle e_i : 1 \leq i \leq l \rangle \oplus \langle f_i : l \geq i \geq 1 \rangle$. Then by [15, §4.2] $G \cong \mathrm{SL}(l,q^2).(q-1).2$.

Let $A_1, B_1 \in \mathrm{SL}(l,q^2)$ generate $\mathrm{SL}(l,q^2)$, and let $J := \mathrm{AntiDiag}[1, \ldots, 1] \in \mathrm{GL}(l,q^2)$. Define $A := \mathrm{Diag}[A_1, JA_1^{-*}J]$ and $B := \mathrm{Diag}[B_1, JB_1^{-*}J]$. Identify $\langle A, B \rangle$ with $\mathrm{SL}(l,q^2)$. A short calculation shows that A and B preserve both F and $\mathcal{D}$, and so $A, B \in G$.

Define $C_1 := \mathrm{AntiDiag}[I_l, I_l]$ and $M := \mathrm{Diag}[\zeta^{(q+1)/2}, 1, \ldots, 1, \zeta^{-q(q+1)/2}] \in \mathrm{GU}(d,q)$, a matrix of determinant -1 that squares to I_d. If $d \equiv 0 \bmod 4$ or q is even then let $C := C_1$, otherwise set $C := C_1 M$. If $C = C_1$ then $C^2 \in \mathrm{SL}(l,q^2)$, otherwise C^2 is a diagonal matrix such that $\mathrm{Det}(C^2|_{\langle e_i : 1 \leq i \leq l \rangle}) = -1$. We see that $C \in N_G(\mathrm{SL}(l,q^2))$.

Define $D \in \mathrm{GL}(d,q^2)$ to be diagonal with entry ζ in row 1, entry ζ^q in row 2, entry ζ^{-1} in row $d-1$ and ζ^{-q} in row d. Then D preserves F and $\mathcal{D}$, so $D \in N_G(\mathrm{SL}(l,q^2)) \setminus \mathrm{SL}(l,q^2)$. Up to conjugacy, $G = \langle A, B, C, D \rangle$. □

6 Semilinear groups

In this section we describe how to write down generators for the semilinear subgroups G of Ω that arise in Theorem 1.1. Let $u := 1$ in cases L and S and $u := 2$ in case U. A group is *semilinear* if it can be embedded in $\Gamma\mathrm{L}(d/s, q^{su})$ for some divisor s of d. From Table 4.3.A of [15], we find that, for each such s, there is one maximal semilinear subgroup G having the same type (L, S or U) as Ω. In addition, in case S with q odd, there is a conjugacy class of semilinear groups isomorphic to $\mathrm{GU}(d/2, q).2$.

We denote a primitive element of $\mathrm{GF}(q^{su})$ by ω. The symbol ν_q denotes the field automorphism $x \mapsto x^q$ of $\mathrm{GF}(q^{su})$, and σ_q denotes the matrix operation $(a)_{ij} \mapsto (a^q)_{ij}$.

Lemma 6.1 *Let q be a prime power. A subgroup of $\mathrm{GL}(s, q)$ that is isomorphic to $\Gamma\mathrm{L}(1, q^s)$ may be constructed in time $O(s^2 \log q + \log^2 q)$.*

Proof: Fix a basis $\mathcal{B} := [1, \omega, \omega^2, \ldots, \omega^{s-1}]$ of $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$. This determines an embedding $\phi : \mathrm{GF}(q^s)^{(1)} \to \mathrm{GF}(q)^{(s)}$, and induces an embedding $\psi : \Gamma\mathrm{L}(1, q^s) \to \mathrm{GL}(s, q)$.

Let $f(x)$ be a primitive polynomial for $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$ with root ω, and let $A \in \mathrm{GL}(s, q)$ be the companion matrix for f. Then A acts on the natural basis in the same way as ω acts by multiplication on $\mathcal{B}$, so $A_s = \psi(\omega)$.

For $0 \leq i, j \leq s-1$ let ξ_{ij} be the coefficient of ω^j in the expression for ω^{iq}, written as a linear combination of ω^k with $0 \leq k \leq s-1$. Define $B \in \mathrm{GL}(s, q)$ by $B_{ij} := \xi_{i-1,j-1}$. Then B acts on the natural basis of $\mathrm{GF}(q)^{(s)}$ in the same way as ν_q acts on $\mathcal{B}$, so $B = \psi(\nu_q)$. Then $\langle A, B\rangle \cong \langle \omega, \nu_q\rangle = \Gamma\mathrm{L}(1, q^s)$.

We construct the field elements in time $O(\log^2 q)$ for ω^q, then $O(\log q)$ time for each additional power. Writing down the matrix B then takes an additional time $O(s^2 \log q)$, yielding a total time of $O(s^2 \log q + \log^2 q)$. □

Retaining the notation of the proof above, the map ψ can be used to construct a map $\theta : \Gamma\mathrm{L}(d/s, q^s) \to \mathrm{GL}(d, q)$, where $\theta : (\lambda\omega^i)_{jk} \mapsto (\lambda A^i)_{jk}$ and $\theta : \sigma_q \mapsto \mathrm{Diag}[B, \ldots, B]$ for $\lambda \in \mathrm{GF}(q)$. It is clear that θ is an injection. The reader may verify that θ restricted to $\mathrm{GL}(d/s, q^s)$ is a homomorphism by checking that the (m, n)-th block of $\theta(X).\theta(Y)$ is $\psi(x)$, where x is the (m, n)-th entry of XY, for $X, Y \in \mathrm{GL}(d/s, q^s)$. Furthermore, $\theta(\sigma_q)$ acts by conjugation on $\mathrm{Im}(\theta|_{\mathrm{GL}(d/s,q^s)})$ by conjugating each block by B, which corresponds to the action of σ_q on $\mathrm{GL}(d/s, q^s)$. So θ is an homomorphism.

Lemma 6.2 *Let A and B be as in Lemma 6.1. Then $|\mathrm{Det}(A)| = q - 1$ and $\mathrm{Det}(B) = 1$ if s is odd or q is even, or -1 if s is even and q is odd.*

PROOF: The first claim follows from the fact that when represented as a subgroup of $\mathrm{GL}(d,q)$ we have $|\mathrm{Det}(\mathrm{GL}(d/s,q^s))| = (q-1)$ [15, Prop.4.3.6].

The Normal Basis Theorem (see for instance [20, Thm 2.35]) states that there exists an element α in $\mathrm{GF}(q^s)$ such that $[\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{s-1}}]$ is a basis for $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$. Relative to this basis, the matrix for $\psi(\nu_q)$ is a permutation matrix with a 1 in position $(i, i+1)$ for $1 \leq i \leq s-1$ and a 1 in position $(s,1)$. Thus $\mathrm{Det}(B)$ is as stated. $\square$

6.1 Linear semilinear groups

Proposition 6.3 *A set of representatives of the maximal semilinear subgroups of* $\mathrm{SL}(d,q)$ *can be constructed in time* $O(d^\Psi \log d \log^2 q)$.

PROOF: Let G be a maximal semilinear subgroup of $\mathrm{SL}(d,q)$. Then by [15, Prop 4.3.6] there exists a prime divisor s of d such that

$$G \cong \mathrm{SL}(d/s, q^s).\frac{q^s-1}{q-1}.s$$

We use Lemma 6.1 to construct matrices $A_s, B_s \in \mathrm{GL}(s,q)$ with $\langle A_s, B_s\rangle \cong \Gamma\mathrm{L}(1,q^s)$. We compute $C_s := \psi(\omega^{q-1}) = A_s^{q-1}$ in time $O(s^\Psi \log^2 q)$.

If $s = d$ and d is odd then let $H := \langle C_s, B_s\rangle$. Since s is odd, $\mathrm{Det}(B_s) = \mathrm{Det}(C_s) = 1$, so $H \leq \mathrm{SL}(d,q)$. It is clear that $H \cong \frac{q^s-1}{q-1}.s$, so $G = H$. If $s = d = 2$ then set $F_s := B_s A_s^{(q-1)/2}$ and let $H := \langle C_s, F_s\rangle$. Then $\mathrm{Det}(F_s) = 1$ and $C_s^{F_s} = C_s^q$, so $G = H$.

If $s \neq d$ then let $X, Y \in \mathrm{GL}(d/s, q^s)$ generate $\mathrm{SL}(d/s, q^s)$. We may assume that $X = \mathrm{Diag}[\omega, \omega^{-1}, 1\ldots, 1]$ and that Y has all nonzero entries equal to ± 1 [23]. Let $A := \theta(X) \in \mathrm{GL}(d,q)$, and $B := \theta(Y) \in \mathrm{GL}(d,q)$. Then $\langle A, B\rangle \cong \mathrm{SL}(d/s, q^s) \leq \mathrm{SL}(d,q)$. Note that since all nonzero entries of X and Y lie in the set $\{\omega^{\pm 1}, \pm 1\}$ we do not have to power A_s or compute discrete logs. Thus, given A_s, we construct A and B in time $O(d^2 \log q)$.

Let $C := \theta(\mathrm{Diag}[\omega^{q-1}, 1, \ldots, 1])$. Then $C = \mathrm{Diag}[C_s, I_s, \ldots, I_s]$, and $\mathrm{Det}(C) = 1$. Finally let $D_1 := \theta(\sigma_q)$. If $s = 2$, with d/s is odd and q is odd then let $D := D_1 Z$, where Z is a block diagonal matrix with nonzero blocks equal to $A_s^{(q-1)/2}$; otherwise, set $D := D_1$. In both cases we have $G = \langle A, B, C, D\rangle$.

The generating matrices for G are written down in time $O(d^\Psi \log^2 q)$ and the number of types of semilinear group is equal to the number of prime divisors of d, which is $O(\log d)$ by Lemma 2.1. $\square$

6.2 Symplectic semilinear groups

Proposition 6.4 *A set of representatives of the maximal semilinear subgroups of* $\mathrm{Sp}(d, q)$ *of symplectic type can be constructed in time* $O(d^3 \log d \log^2 q)$

Proof: Let G be a maximal semilinear subgroup of $\mathrm{Sp}(d, q)$ of symplectic type. Then by [15, Prop 4.3.10] there exists a prime divisor s of d such that d/s is even and $G \cong \mathrm{Sp}(d/s, q^s).s$.

As in Lemma 6.1, construct $A_s := \psi(\omega)$ and $B_s := \psi(\nu_q)$ in time $O(s^2 \log q + \log^2 q)$. Then let $X_{d/s}$ and $Y_{d/s}$ be generating matrices for $\mathrm{Sp}(d/s, q^s)$, and let $A := \theta(X_{d/s})$ and $B := \theta(Y_{d/s})$. By [23] we may assume that all nonzero entries of $X_{d/s}$ and $Y_{d/s}$ are in the set $\{\pm 1, \omega^{\pm 1}\}$, so this construction takes time $O(d^2 \log q)$. Let $C := \theta(\sigma_q)$. Since if $s = 2$ then $d \equiv 0 \bmod 4$, we always have $\mathrm{Det}(C) = 1$. Then setting $H := \langle A, B, C\rangle$ gives $H \cong G$.

A short calculation shows that if $\beta(\_\,,\_)$ is a symplectic form on $\mathrm{GF}(q^s)^{d/s}$ then $\beta'(\_\,,\_) := \mathrm{Tr}(\beta(\_\,,\_))$ is a symplectic form over $\mathrm{GF}(q)$. As we have a fixed symplectic form, and know our basis for $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$, we can calculate a matrix for this form in $O(d^2 \log^2 q)$. By the results of Section 3, we conjugate H to a subgroup of $\mathrm{Sp}(d, q)$ in time $O(d^3 \log q)$. Noting that there are $O(\log d)$ groups to be constructed completes the proof. □

Proposition 6.5 *A representative of the maximal semilinear subgroups of* $\mathrm{Sp}(d, q)$ *of unitary type can be constructed in time* $O(d^3 \log^2 q)$

Proof: Let G be a maximal semilinear subgroup of $\mathrm{Sp}(d, q)$ of unitary type. Then by [15, Prop 3.2.7] $G \cong \mathrm{GU}(l, q).2$. Let ω be a primitive element of $\mathrm{GF}(q^2)$, let $A_2 := \psi(\omega) \in \mathrm{GL}(2, q)$ and $B_2 := \psi(\nu_q) \in \mathrm{GL}(2, q)$. Also, let $X, Y \in \mathrm{GL}(l, q^2)$ generate $\mathrm{GU}(l, q)$. We then construct $A := \theta(X)$ and $B := \theta(Y)$. Let i be such that $(q+1)/2^i$ is odd, and let $m := (q^2-1)/2^{i+1}$. Let $C := \mathrm{Diag}[B_2 A_2^m, \ldots, B_2 A_2^m]$, so that each block has determinant 1. Since A_2 is a (2×2) matrix we construct C in time $O(d^2 \log q + \log^2 q)$.

A short calculation shows that if $\beta(\_\,,\_)$ is a unitary form over $\mathrm{GF}(q^2)$ then $\beta'(\_\,,\_) := \mathrm{Tr}(\lambda\beta(\_\,,\_))$ is a symplectic form over $\mathrm{GF}(q)$, for $\lambda \in \mathrm{GF}(q^2)$ of trace zero. We can choose λ to be a primitive 4th root of unity, and then construct β' in time $O(d^2 \log^2 q)$. We use Proposition 3.2 to conjugate H to $G \leq \mathrm{Sp}(d, q)$. □

6.3 Unitary semilinear groups

Proposition 6.6 *A set of representatives of the maximal semilinear subgroups of* $\mathrm{SU}(d,q)$ *can be constructed in time* $O(d^3 \log d \log^2 q)$.

PROOF: Let G be a maximal semilinear subgroup of $\mathrm{SU}(d,q)$. Then

$$G \cong \mathrm{SU}(d/s, q^s).\frac{q^s+1}{q+1}.s$$

for some odd prime s dividing d. The construction of $H \cong G$ is virtually identical to that of Proposition 6.3, and we leave it to the reader.

A short calculation shows that if $\beta(\_\,,\_)$ is a unitary form over $\mathrm{GF}(q^s)$ then $\beta'(\_\,,\_) := \mathrm{Tr}(\beta(\_\,,\_))$ is a unitary form over $\mathrm{GF}(q)$. Thus we may use the results of Section 3 to conjugate H to G in time $O(d^3 \log q)$. Noting that there are $O(\log d)$ maximal semilinear subgroups completes the proof. □

7 Tensor product groups

In this section we describe how to write down generators for the tensor product subgroups G of Ω that arise in Theorem 1.1. A group is *tensor product* if it preserves a decomposition $V = V_1 \otimes V_2$. From Table 4.4.A of [15] we find that in cases L and U, for each divisor $d_1 < \sqrt{d}$ of d, there is a unique such G. Its socle mod scalars is $\mathrm{PSL}(d_1,q) \times \mathrm{PSL}(d_2,q)$ or $\mathrm{PSU}(d_1,q) \times \mathrm{PSU}(d_2,q)$, in cases L and U respectively, where $d = d_1d_2$. In case S, these groups G occur only for odd q. In this case, for each even divisor d_1 of d for which $d_2 \geq 3$ there are (one or two) groups G with socle mod scalars equal to $\mathrm{PSp}(d_1,q) \times \mathrm{P\Omega}^{\varepsilon}(d_2,q)$. We note that the determinant of $A \otimes B \in \mathrm{GL}(d_1,q) \otimes \mathrm{GL}(d_2,q)$ is $\mathrm{Det}(A)^{d_2}\mathrm{Det}(B)^{d_1}$.

7.1 Linear tensor product groups

Proposition 7.1 *A set of representatives of the maximal tensor product subgroups of* $\mathrm{SL}(d,q)$ *can be constructed in time* $O(d^{2+\epsilon}\log q)$*, for any real* $\epsilon > 0$.

PROOF: We let G be a maximal tensor product subgroup of $\mathrm{SL}(d,q)$, set $Z := Z(\mathrm{SL}(d,q))$, and let $\overline{G} := G/(G \cap Z)$. Then $Z(G) = Z$ and by [15, §4.4] there exists a divisor $d_1 < \sqrt{d}$ of d such that, with $d_2 := d/d_1$ and

$$c := (d_1, q-1)(d_2, q-1)(d_1, d_2, q-1)/(d, q-1),$$

we have $\overline{G} \cong (\mathrm{PSL}(d_1, q) \times \mathrm{PSL}(d_2, q)).[c]$. Elements of G are the Kronecker products of elements of $\mathrm{GL}(d_1, q)$ with those of $\mathrm{GL}(d_2, q)$: the quotient group of order c measures the freedom in the choice of determinant in each tensor factor.

For $i = 1, 2$ let A_i and B_i generate $\mathrm{SL}(d_i, q)$. Let S and T be the Kronecker products of A_1 and B_1 with I_{d_2}, and let U and V be the products of I_{d_1} with A_2 and B_2. Let $C_1 := \zeta^{(q-1)/(q-1,d)} I_d$, so that $\langle C \rangle = Z$, and set $H := \langle S, T, U, V, C \rangle$. If $c = 1$ then, up to $\mathrm{SL}(d, p^e)$ conjugacy, $G = H$.

When $c > 1$, G may be generated by H together with certain matrices of the form $D := D_1 \otimes D_2$, where $D_1 := \mathrm{Diag}[\zeta^x, 1, \ldots, 1] \in \mathrm{GL}(d_1, q)$ and $D_2 := \mathrm{Diag}[\zeta^y, 1, \ldots, 1] \in \mathrm{GL}(d_2, q)$. We want to make all matrices D such that $\mathrm{Det}(D) = 1$, which implies that $d_2 x + d_1 y = 0 \bmod q-1$. So the required generators D correspond to generators of the nullspace of the 3×1 matrix $[d_2, d_1, q-1]$.

Finding this nullspace involves transforming the matrix to one with a single nonzero entry, by using elementary row operations over the integers. This can be done in time polynomial in the 'size' of the entries, where 'size' here means number of bits. In fact, only one division involving $q - 1$ is required, and all other operations involve numbers of size $O(\log d)$, so the nullspace can be found in time $O(d \log q)$.

The number of groups to construct is equal to half of the number of divisors of d, which by Lemma 2.1 is $O(d^\epsilon)$ for any real $\epsilon > 0$. □

7.2 Symplectic tensor product groups

Proposition 7.2 *A set of representatives of the maximal tensor product subgroups of* $\mathrm{Sp}(d, q)$ *may be constructed in time* $O(d^{\Psi+\epsilon} \log^3 q)$.

PROOF: Let G be a maximal tensor product subgroup of $\mathrm{Sp}(d, p^e)$. Then by [15, §4.4], q is odd, there exists an even divisor d_1 of d such that $d_2 := d/d_1 \geq 3$, and

$$\overline{G} \cong (\mathrm{PSp}(d_1, q) \times \mathrm{PO}^\varepsilon(d_2, q)).(d_2, 2),$$

where $\varepsilon \in \{+, -, \circ\}$ and $Z(G) = \{\pm I\} = Z(\mathrm{Sp}(d, q))$.

Let X_1, Y_1 generate $\mathrm{Sp}(d_1, q)$, and let $Z_1 := \mathrm{Diag}[\zeta, \ldots, \zeta, 1, \ldots, 1] \in \mathrm{GL}(d_1, q)$, so that $\langle X_1, Y_1, Z_1 \rangle \cong \mathrm{GSp}(d_1, q)$. Let X, Y, Z be the Kronecker products of X_1, Y_1 and Z_1 with I_{d_2}.

Suppose that d_2 is odd, and let $A_\circ, B_\circ, D_\circ$ generate $\mathrm{O}(d_2, q)$ as in Lemma 2.4. Let A, B, D be the Kronecker products of I_{d_1} with $A_\circ$, $B_\circ$ and $D_\circ$ respectively, and set $H := \langle X, Y, A, B, D\rangle$.

Now suppose that d_2 is even, and for $\varepsilon = \pm$ let $A_\varepsilon, B_\varepsilon, D_\varepsilon, E_\varepsilon$ generate $\mathrm{GO}^\varepsilon(d_2, q)$ as in Lemma 2.4. Let $A^\varepsilon, B^\varepsilon, D^\varepsilon$, E^ε be the tensor products of I_{d_1} with A_ε, B_ε, D_ε and E_ε and let Z^ε be the product of Z^{-1} with E^ε. Finally, let $H^\varepsilon := \langle X, Y, Z^\varepsilon, A^\varepsilon, B^\varepsilon, D^\varepsilon\rangle$. Since d_1 and d_2 are even we have $H^\varepsilon \leq \mathrm{SL}(d, q)$.

The reader may check that in each case H preserves a symplectic form given by $\beta(S_1 \otimes T_1, S_2 \otimes T_2) = \beta_1(S_1, S_2).\beta_2(T_1, T_2)$, where β_1 is a symplectic form on $\mathrm{GF}(q)^{d_1}$ and β_2 is a symmetric bilinear form on $\mathrm{GF}(q)^{d_2}$. The form β_1 is the standard one and, as we discussed in the remark following Lemma 2.4, the form β_2 is almost antidiagonal (it is antidiagonal apart from a 2×2 matrix in the centre of the matrix defining the form), and can be transformed to antidiagonal in $O(\log q)$. So we can compute β and then transform it to the standard symplectic form all in time $O(d^2 \log q)$. Hence we may find M and compute G with $G := H^M \leq \mathrm{Sp}(d, q)$ in time $O(d^\Psi \log q)$.

By Lemma 2.1 there are $O(d^\epsilon)$ groups to construct, for any real $\epsilon > 0$. □

7.3 Unitary tensor product groups

We use the form $F = I_d$, and let $Z := Z(\mathrm{SU}(d, q))$.

Proposition 7.3 *A set of representatives of the maximal tensor product subgroups of* $\mathrm{SU}(d, q)$ *can be constructed in time* $O(d^{2+\epsilon} \log q + \log^2 q)$.

Proof: Let G be a maximal tensor product subgroup of $\mathrm{SU}(d, q)$, and let $\overline{G} := G/(G \cap Z)$. Then $Z(G) = Z$ and by [15, §4.4] there exists a divisor $d_1 < \sqrt{d}$ of d such that, with $d_2 := d/d_1$ and

$$c := (d_1, q + 1)(d_2, q + 1)(d_1, d_2, (q + 1))/(d, q + 1),$$

we have $\overline{G} = (\mathrm{PSU}(d_1, q) \times \mathrm{PSU}(d_2, q)).[c]$.

Let S, T, U, V generate $\mathrm{SU}(d_1, q) \circ \mathrm{SU}(d_2, q)$ as in Proposition 7.1. Let $C := \zeta^{(q^2-1)/(q+1,d)} I_d$, so that $\langle C\rangle = Z$ and set $H := \langle S, T, U, V, C\rangle$. Then H preserves a unitary form $\beta(A_1 \otimes B_1, A_2 \otimes B_2) = \beta_1(A_1, A_2).\beta_2(B_1, B_2)$, where β_i is represented by I_{d_i}. Therefore β has matrix I_d and we assume that $H \leq G$.

If $c = 1$ then, up to SU-conjugacy, $G = H$, so suppose that $c \neq 1$. A diagonal matrix preserves F if and only if all of its entries are powers of $\eta := \zeta^{q-1}$. We generate G with H together with matrices of the form $D := D_1 \otimes D_2$, where $D_1 := \mathrm{Diag}[\eta^x, 1, \ldots, 1] \in \mathrm{GU}(d_1, q)$ and $D_2 := \mathrm{Diag}[\eta^y, 1, \ldots, 1] \in \mathrm{GU}(d_2, q)$, and $\mathrm{Det}(D) = 1$. The condition $\mathrm{Det}(D) = 1$ is equivalent to $d_2 x + d_1 y = 0 \bmod (q+1)$. So the required generators D correspond to generators of the nullspace of the integral 3×1 matrix $[d_2, d_1, q+1]$ which, as in the linear case, can be found in time $O(d \log q)$.

By Lemma 2.1 there are $O(d^\epsilon)$ decompositions, for any real $\epsilon > 0$. □

8 Subfield groups

In this section we describe how to write down generators for the subfield subgroups G of the group Ω that arise in Theorem 1.1. Let $u := 1$ in cases L and S and $u := 2$ in case U. A group is *subfield* if, modulo scalars, it can be written over a proper subfield of $\mathrm{GF}(q^u)$. Throughout this section, f will denote a divisor of e (recall that $q = p^e$), and ω will denote a primitive element of $\mathrm{GF}(p^{fu})$. From Table 4.5.A of [15], we find that, for each such f for which e/f is prime, there is one maximal subfield subgroup G having the same type (L, S or U) as Ω. In addition, in case U with q odd, there are (one or two) groups G or orthogonal type and in case U with n even, there is a group of symplectic type.

Recall that $[a, b]$ denotes the lowest common multiple of integers a and b.

8.1 Linear subfield groups

Proposition 8.1 *The maximal subfield subgroups of* $\mathrm{SL}(d, q)$ *can be constructed in time* $O((d^2 \log q + \log^2 q) \log\log q)$.

Proof: Let $Z := Z(\mathrm{SL}(d, p^e))$, and let $G \leq \mathrm{SL}(d, p^e)$ be a maximal subfield group. Then $Z(G) = Z$ and by [15, §4.5] there exists a prime divisor b of e such that $|\mathrm{PGL}(d, p^f) : G/Z| = c$, where $f := e/b$, we define $k := (p^e - 1, d)$ and

$$c := k[p^f - 1, (p^e - 1)/k]/(p^e - 1).$$

The group G consists of all matrices from $\langle \mathrm{GL}(d, p^f), Z(\mathrm{GL}(d, p^e)) \rangle$ that have determinant 1.

Let A and B generate $\mathrm{SL}(d, p^f)$; then A and B may be thought of as elements of $\mathrm{SL}(d, p^e)$. Let $C := \zeta^{(p^e-1)/k} I_d$. Then $\langle C \rangle = Z$, so if $c = (p^f - 1, d)$ we may set $G = \langle A, B, C \rangle$.

Suppose then that $c \neq (p^f - 1, d)$, and define $H := \langle A, B, C \rangle$ and

$$Y := \mathrm{Diag}[\omega, 1, \ldots, 1] \in \mathrm{GL}(d, p^e).$$

Then $\langle \mathrm{SL}(d, p^f), Y \rangle = \mathrm{GL}(d, p^f)$. Let $D := Y^c$ then, since $c | (p^f - 1, d)$, we see that $|\mathrm{GL}(d, p^f) : \langle \mathrm{SL}(d, p^f), D \rangle| = c$. We compute ω^c and hence D in time $O(\log d \log q)$.

Now we construct a scalar $X \in \mathrm{GL}(d, p^e)$ such that $\mathrm{Det}(XD) = 1$. We have $\mathrm{Det}(D) = \zeta^z$ where

$$\begin{aligned} z &= \tfrac{p^e-1}{p^f-1} . \tfrac{k.[p^f-1,(p^e-1)/k]}{p^e-1} = \tfrac{k(p^f-1)(p^e-1)/k}{(p^f-1)(p^f-1,(p^e-1)/k)} \\ &= \tfrac{p^e-1}{(p^f-1,(p^e-1)/k)}. \end{aligned}$$

By [11, Thm 57], since k divides z, the equation $\lambda d = z \bmod p^e - 1$ has k solutions, and solving it is equivalent to solving $\lambda d/k = z/k \bmod (p^e - 1)/k$. We use the Euclidean algorithm to find integers x and y such that $x.(d/k) + y.((p^e - 1)/k) = 1$, in time $O(\log(d/k))$. Then $x = (d/k)^{-1} \bmod (p^e - 1)/k$. Given x, we compute λ in constant time. We set $X := \zeta^{-\lambda} I_d$, then up to conjugacy $G = \langle H, XD \rangle$. Computing $\zeta^{-\lambda}$ requires time $O(\log^2 q + \log d)$, then computing XD requires time $O(d^2 \log q)$, since X is a scalar.

By Lemma 2.1 there are $O(\log e) = O(\log \log q)$ groups to construct. □

8.2 Symplectic subfield groups

Proposition 8.2 *A set of representatives of the maximal subfield subgroups of* $\mathrm{Sp}(d, q)$ *may be constructed in time* $O((d^2 \log q + \log^2 q) \log \log q)$.

PROOF: Let G be a maximal subfield subgroup of $\mathrm{Sp}(d, p^e)$. Then by [15, Prop. 4.5.4] there exists a divisor f of e such that e/f is prime and

$$G \cong \mathrm{Sp}(d, p^f).(2, e/f, p - 1).$$

A symplectic form on $\mathrm{GF}(p^f)^d$ extends naturally to a symplectic form with the same form matrix on $\mathrm{GF}(p^e)^d$, so $\mathrm{Sp}(d, p^f)$ may be considered as a subgroup of $\mathrm{Sp}(d, p^e)$.

If $(2, e/f, p-1) = 1$ then we may set $G = \mathrm{Sp}(d, p^f)$, so suppose that $(2, e/f, p-1) = 2$. Let $D \in \mathrm{GL}(d, p^f)$ map $e_i \mapsto \omega e_i$ and $f_i \mapsto f_i$, for $1 \leq i \leq l$. Then $D \in \mathrm{GSp}(d, p^f)$, and $\mathrm{Det}(D) = \zeta^{kd/2}$, where $k := (p^e - 1)/(p^f - 1)$. Since $e/f = 2$ and p is odd, d divides $kd/2$. Let $S := \zeta^{-k/2} I_d$, and define $C := SD$. A short calculation shows that C preserves F and has determinant 1 so $C \in N_{\mathrm{Sp}(d,p^e)}(\mathrm{Sp}(d, p^f))$, and we may set $G = \langle \mathrm{Sp}(d, p^f), C \rangle$.

The matrices S and D are diagonal, so computing C takes time $O(d^2 \log q + \log^2 q)$. By Lemma 2.1 there are $O(\log \log q)$ groups to construct. □

8.3 Unitary subfield groups

Here we use the form $F = \mathrm{AntiDiag}[1, \ldots, 1]$. We let $Z := Z(\mathrm{SU}(d, q))$, and $C := \zeta^{(q^2-1)/(q+1,d)} I_d$ so that $\langle C \rangle = Z$. We define $k := (q+1, d) = (p^e+1, d)$. Recall that for a matrix $A \in \mathrm{GL}(d, q^2)$, by A^{σ_q} we mean the matrix whose entries are q-th powers of the entries of A.

Proposition 8.3 *A set of representatives of the maximal subfield subgroups of* $\mathrm{SU}(d, q)$ *of unitary type can be constructed in time* $O((d^2 \log q + \log^2 q) \log \log q)$.

Proof: Let G be a maximal subfield subgroup of $\mathrm{SU}(d, p^e)$ of unitary type. Then $Z(G) = Z$ and by [15, §4.5] there exists an odd prime divisor b of e such that $|\mathrm{PGU}(d, p^f) : G/Z| = c$, where $f := e/b$ and

$$c := k[p^f + 1, (p^e + 1)/k]/(p^e + 1).$$

A unitary form on $\mathrm{GF}(p^{2f})^d$ extends naturally to a unitary form on $\mathrm{GF}(p^{2e})^d$, so $\mathrm{GU}(d, p^f)$ may be considered as a subgroup of $\mathrm{GU}(d, p^e)$.

The construction of G is similar to Proposition 8.1: we sketch it briefly. Let A and B generate $\mathrm{SU}(d, p^f)$, and let $H := \langle A, B, C \rangle \leq \mathrm{SU}(d, p^e)$.

If $c = (p^f + 1, d)$ then we may choose $G = H$, so suppose that $c \neq (p^f + 1, d)$, let $Y := \mathrm{Diag}[\omega, 1, \ldots, 1, \omega^{-p^f}] \in \mathrm{GU}(d, p^f)$ and let $D := Y^c$. A short calculation shows that $\mathrm{Det}(D) = \zeta^z$, where $z = -(p^{2e} - 1)/(p^f + 1, (p^e+1)/k)$. We find a λ such that $\lambda(p^e - 1)d = -z \bmod p^{2e} - 1$, by finding $(d/k)^{-1} \bmod (p^e + 1)/k$ in time $O(\log(d/k))$. We then set $X := \zeta^{\lambda(p^e-1)} I_d$ so that $XD \in \mathrm{SU}(d, p^e)$, and choose $G = \langle H, XD \rangle$.

By Lemma 2.1 there are $O(\log e) = O(\log \log q)$ groups to construct. □

Proposition 8.4 *A set of representatives of the maximal subfield subgroups of* $\mathrm{SU}(d, q)$ *of orthogonal type can be constructed in time* $O(d^3 \log q + \log^3 q)$.

Proof: These occur only for q odd. For $\varepsilon \in \{+,-,\circ\}$, let F^ε denote the matrix of the symmetric bilinear form preserved by $\mathrm{O}^\varepsilon(d,q)$.

Suppose first that d is even. Then by [15, Prop 4.5.5], $G \cong Z.\mathrm{PSO}^+(d,q).2$ or $Z.\mathrm{PSO}^-(d,q).2$.

First we deal with the G of plus type. Let A, B, D_+, E_+ be the generators of $\mathrm{GO}^+(d,q)$ as in Lemma 2.4. In this case, we have $F^+ = \mathrm{AntiDiag}[1,\dots,1]$. From the remarks following the proof of Proposition 3.3, we can take this to be the standard orthogonal form. All matrices in $\mathrm{O}^+(d,q)$ are fixed by $A \mapsto A^{\sigma_q}$, so we may think of $\mathrm{O}^+(d,q)$ as a subgroup of $\mathrm{GU}(d,q)$. Therefore $H_0 := \langle A, B, C\rangle \cong Z.\mathrm{SO}^+(d,q) \leq \mathrm{SU}(d,q)$.

We construct the outer involution. Let $X := \zeta I_d$ and let $E := E_+X^{-1}$. Then $EFE^* = F$, so $E \in N_{\mathrm{GU}(d,q)}(\mathrm{SO}^+(d,q))$, and $\mathrm{Det}(E) = \zeta^{d(q-1)/2}$. Set $H_1 := \langle H_0, D_+, E, X^{q-1}\rangle \leq \mathrm{GU}(d,q)$. We construct an element W of $H_1 \setminus H_0$ of determinant 1: then up to conjugacy we will have $G = \langle H_0, W\rangle$.

First suppose that $(q+1)/k$ is even, and let $i_1 := (q^2-1)/2k$. Then $X^{i_1} \in H_1$, and $\mathrm{Det}(X^{i_1}) = -1$, so $\mathrm{Det}(X^{i_1}D_+) = 1$. We must show that $X^{i_1}D_+ \notin H_0$. Suppose otherwise, then there exists a scalar $S \in Z$ such that $SX^{i_1}D_+ \in \mathrm{SO}^+(d,q)$, so in particular $SX^{i_1}D_+F^+(SX^{i_1}D_+)^{\mathrm{T}} = F^+$. This implies that $S = \pm X^{-i_1}$, contradicting $S \in Z$. We put $W := X^{i_1}D_+$.

Next suppose that d/k is even and let $m := (q+1)/k$. Let $i_2 := (q-1)(m+1)/2$, then the exponent z of ζ in $\mathrm{Det}(X^{i_2})$ is

$$\begin{aligned} z &= d(q-1)(m+1)/2 = ((q-1)dm)/2 + d(q-1)/2 \\ &= ((q-1)(q+1)d)/(2(d/2,q+1)) + d(q-1)/2 \\ &= d(q-1)/2. \end{aligned}$$

Since $X^{-i_2} \in \mathrm{GU}(d,q)$, we see that $EX^{-i_2} \in H_1$. A short calculation shows that if there exists an S such that $EX^{-i_2}S$ preserves F^+ then $S = \pm X^{i_2+1-(q+1)/2}$. But then $S \notin Z$, a contradiction. Thus $EX^{-i_2} \notin H_0$ and we put $W := EX^{-i_2}$.

Finally, suppose that $m := d/k$ and $(q+1)/k$ are both odd. We have $\mathrm{Det}(D_+E) = \zeta^{(d+q+1)(q-1)/2}$. Since $((q+1)/k, m) = 1$ there exists an $n \in \mathbb{Z}$ such that $nm = 1 \bmod (q+1)/k$. We compute n in time $O(\log m) = O(\log d)$. Let

$$i_3 := (q-1)n(d+q+1)/2k;$$

note that i_3 is divisible by $(q-1)$. Then

$$\mathrm{Det}(X^{i_3}) = \zeta^{d(q-1)n(d+q+1)/2k} = \alpha^{nm},$$

where $\alpha := \zeta^{(d+q+1)(q-1)/2}$. Now,

$$|\alpha| = (q+1)/(q+1,(d+q+1)/2) = (q+1)/k,$$

by our assumptions on d and $(q+1)$. Then since $\alpha^{mn} = \alpha^{1+o(q+1)/k}$ for some $o \in \mathbb{Z}$, we have $\alpha^{mn} = \alpha$. Therefore $\mathrm{Det}(D_+EX^{-i_3}) = 1$. A short calculation shows that $D_+EX^{-i_3} \notin H_0$, so we may set $W := D_+EX^{-i_3}$.

Next we show how to construct $G \cong Z.\mathrm{PSO}^-(d,q).2$ of minus type. We may assume that F^- is either I_d or $\mathrm{Diag}[\omega, 1, \ldots, 1]$, according as $(q-1)d/4$ is odd or even. Let A, B, D_-, E_- be as in Lemma 2.4, let X be as before and let $E := X^{-1}E_-$ so that E preserves a unitary form with matrix F^-. If $(q+1)/k$ is even then $W := X^{i_1}D_-$. If d/k is even then $W := EX^{-i_2}$. If the same power of 2 divides $(q+1)$ and d then if $d/2$ is even, $W := D_-EX^{-i_3}$ and if $d/2$ is odd then $W := EX^{-i_3}$. We find a change of form matrix M using Proposition 3.2, then up to conjugacy $G = \langle H_0^M, W^M \rangle$.

The case when d is odd is similar but easier. It is shown in [15, Prop 4.5.5] that $G \cong Z.\mathrm{SO}^\circ(d,q)$, and we leave the construction to the reader. □

Proposition 8.5 *A representative of the maximal subfield symplectic subgroups of* $\mathrm{SU}(d,q)$ *can be constructed in time* $O(d^2 \log q + \log^2 q)$.

Proof: Let d be even, let G be a maximal subfield subgroup of $\mathrm{SU}(d,q)$ of symplectic type, and let $c := (2, q-1)(q+1, d/2)/(q+1, d)$. Then by [15, Prop. 4.5.6]

$$G \cong Z.\mathrm{PSp}(d,q).c.$$

Let F' be the symplectic form matrix $\mathrm{AntiDiag}[1, \ldots, 1, -1, \ldots, -1]$.

Let $A, B \in \mathrm{SL}(d,q)$ generate $\mathrm{Sp}(d,q)$, and consider A and B as elements of $\mathrm{SL}(d,q^2)$. If $c = 1$ then let $H := \langle A, B, C \rangle$, so that $G \cong H$.

If $c \neq 1$ then q is odd. Let $D \in \mathrm{SL}(d,q^2)$ map $e_i \mapsto \zeta^{(q+1)/2}e_i$ and $f_i \mapsto -\zeta^{-(q+1)/2}f_i$ for $1 \leq i \leq l$. Then $D \in N_{\mathrm{SL}(d,q^2)}(\mathrm{Sp}(d,q))$, as D preserves F' up to multiplication by -1. Let $H := \langle A, B, C, D \rangle$, then $H \cong G$. We use the results in Section 3 to find M with $H^M \leq \mathrm{SU}(d,q)$, then up to conjugacy $G = H^M$. In fact H preserves the form YF' with $Y := -\zeta^{(q+1)/2}I_d$, so the change of form can be carried out in time $O(d^2 \log q)$. □

9 Groups of extraspecial and symplectic type

In this section we describe how to write down generators for the maximal subgroups of $\mathrm{SL}(d,q)$, $\mathrm{Sp}(d,q)$ and $\mathrm{SU}(d,q^{1/2})$ which are normalisers of ex-

Table 3: Structure of Extraspecial Normalisers

Type	Case	Conditions
$r^{1+2m}.\mathrm{Sp}(2m,r)$	L	q nonsquare, r odd
	U	q square, r odd
$(4 \circ 2^{1+2m}).\mathrm{Sp}(2m,2)$	L	q prime, $d \geq 4$
	U	$q = p^2$
$2_-^{1+2m}.\mathrm{O}^-(2m,2)$	L	q prime, $d = 2$
	S	q prime

traspecial groups or of 2-groups of symplectic type.

9.1 Structure and conjugacy

For any prime r and any integer $m \geq 1$, there are two isomorphism types of extraspecial groups of order r^{2m+1}; see, for example, Theorem 5.2 of [10]. For r odd, we are only concerned with the isomorphism type that has exponent r, since the normaliser in $\mathrm{GL}(r^m, q)$ of the other type of extraspecial group is a proper subgroup of the normaliser of an extraspecial group of exponent r.

For $r = 2$, the extraspecial group of minus type is a central product of a quaternion group of order 8 with zero or more dihedral groups of order 8. By taking a central product of an extraspecial 2-group with a cyclic group of order 4, we obtain a 2-group of symplectic-type.

In Table 3 we describe the maximal subgroups of extraspecial normaliser type in $\mathrm{GL}(d,q)$, $\mathrm{GU}(d,q^{1/2})$ and $\mathrm{GSp}(d,q)$, taken from Table 4.6.B of [15]. The extraspecial or symplectic-type groups E are represented in $d = r^m$ dimensions over the field of $q = p^e$ elements, where e is minimal subject to $p^e \equiv 1 \bmod |Z(E)|$ $(= r$ or $4)$. Groups of type $r^{1+2m}.\mathrm{Sp}(2m,r)$ are the full normalisers in $\mathrm{GL}(r^m,q)$ or $\mathrm{GU}(r^m,q^{1/2})$ of an extraspecial r-group of order r^{1+2m} and exponent r, where r is odd. These groups are maximal in $\mathrm{GL}(d,q)$ if q is a nonsquare, and $\mathrm{GU}(d,q^{1/2})$ if q is square. Groups of type $(4 \circ 2^{1+2m}).\mathrm{Sp}(2m,2)$ are the normalisers in $\mathrm{GL}(2^m,q)$ or $\mathrm{GU}(2^m,q^{1/2})$ of a 2-group of symplectic type of order 2^{1+2m}. Such a group is maximal in $\mathrm{GL}(2^m,q)$ if q is prime, and in $\mathrm{GU}(2^m,q^{1/2})$ if q is a square of a prime. Groups of type $2_-^{1+2m}.\mathrm{O}^-(2m,2)$ are the normalisers of a 2-group of minus type and order 2_-^{1+2m} in $\mathrm{GL}(2,q)$ or $\mathrm{Sp}(2^m,q)$. Such a group is maximal in $\mathrm{GL}(2,q)$ when q is prime and $m=1$, and is maximal in $\mathrm{Sp}(2^m,q)$ for $m>1$ and q prime..

9.2 Construction of the groups

We assume throughout this subsection that $d=r^m$ where r is a prime divisor of $q-1$, and we let ω be a primitive r-th root of 1 in $\mathrm{GF}(q)$, constructed in time $O(\log^2 q)$.

We shall describe how to write down generators of E and of $N_{\mathrm{GL}(d,q)}(E)$, but we shall do this in such a way that a set X of generators of $N_{\mathrm{SL}(d,q)}(E)$ occurs as a subset. The group generated by X will necessarily preserve a form of unitary or symplectic type as appropriate. In the unitary case, the form preserved will be I_d, whereas in the symplectic case it will require a permutation of the basis to transform it to the standard antidiagonal form.

We describe this process first for the case when r is odd. The cases for $r=2$ will require minor variations of the same recipe.

Lemma 9.1 *Let $E \le \mathrm{GL}(d,q)$ be an extraspecial group of odd order and exponent r with $|E|=r^{2m+1}$. Then E can be constructed in time $O(d^2\log d\log q + \log^2 q)$.*

PROOF: Let $X\in\mathrm{GL}(r,q)$ be diagonal with $X_{ii}=\omega^{i-1}$ for $1\le i\le r$, and let $Y\in\mathrm{GL}(r,q)$ be the permutation matrix defined by the permutation $(1,2,\ldots,r)$. That is, $Y_{i(i+1)}=1$ for $1\le i<r$, entry $Y_{r1}=1$, and $Y_{ij}=0$ otherwise. Then the commutator $[Y,X]$ is equal to ωI_r, and so X and Y generate an extraspecial group M of order r^3 and of exponent r.

Now for $1\le i\le m$, we define $X_i := I_{r^{m-i}}\otimes X\otimes I_{r^{i-1}}$ and $Y_i := I_{r^{m-i}}\otimes Y\otimes I_{r^{i-1}}$, where $\otimes$ is the Kronecker product operation. The group E generated by the X_i and Y_i is a central product of m copies of $\langle X,Y\rangle$, and so it is an extraspecial group of the required type. □

If $r=2$ then the construction described above will produce an extraspecial 2-group of plus type.

Lemma 9.2 *Let E be as in Lemma 9.1. Then $N_{\mathrm{GL}(d,q)}(E)$ can be constructed in time $O(d^2\log d\log q+\log^2 q)$.*

PROOF: Let $U\in\mathrm{GL}(r,q)$ be diagonal with $U_{ii}=\omega^{\frac{i(i-1)}{2}}$, and let $V\in\mathrm{GL}(r,q)$ with $V_{ij}=\omega^{(i-1)(j-1)}$ for $1\le i,j\le r$. The reader can verify that $X^U=X$

and $Y^U = YX$. One may also check that $X^V = Y^{-1}$ and $Y^V = X$. So the group $\langle U, V\rangle$ induces $\mathrm{SL}(2,r) = \mathrm{Sp}(2,r)$ on $\overline{M} := M/Z(M)$. For $1 \le i \le m$, we define $U_i := I_{r^{m-i}} \otimes U \otimes I_{r^{i-1}}$ and $V_i := I_{r^{m-i}} \otimes V \otimes I_{r^{i-1}}$.

Then the U_i and V_i all normalise E and the group that they generate induces a direct product of m copies of $\mathrm{Sp}(2,r)$ on $\overline{E} := E/Z(E)$.

Let $W \in \mathrm{GL}(r^2,q)$ be the permutation matrix defined by the permutation $w \in S := \mathrm{Sym}(\{0,\ldots,r^2-1\})$ that maps $a \mapsto (a+((a-1) \bmod r)r) \bmod r^2$. The matrix $I_r \otimes Y$ is a permutation matrix coming from the permutation $y_1 \in S$ where $ay_1 = (((a-1) \operatorname{div} r)r + (a \bmod r) + 1) \bmod r^2$. Similarly $Y \otimes I_r$ is a permutation matrix for $y_2 \in S$, where $ay_2 = a + r \bmod r^2$. The reader can check that $wy_2 = y_2 w$ and that $y_1 w = w y_1 y_2$ satisfies

$$ay_1 w = (((a-1) \operatorname{div} r + a \bmod r)r + (a \bmod r) + 1) \bmod r^2.$$

In general, if R is a diagonal matrix, and S is a permutation matrix defined from the permutation σ, then $T := R^S$ is the diagonal matrix with $T_{i^\sigma,i^\sigma} = R_{ii}$. Using this fact, the reader can check that $I_r \otimes X$ is centralised by W, whereas $(X \otimes I_r)^W = (I_r \otimes X)(X \otimes I_r)^{-1}$.

For $1 \le i \le m-1$, we define $W_i := I_{r^{m-1-i}} \otimes W \otimes I_{r^{i-1}}$. From the relations on $(X \otimes I_r)$ and W, we see that $X_j^{W_i} = X_j$ for $j \ne i+1$ and $X_{i+1}^{W_i} = X_i X_{i+1}^{-1}$, whereas $Y_i^{W_i} = Y_j$ for $j \ne i$ and $Y_i^{W_i} = Y_i Y_{i+1}$.

We claim that all of the elements U_i, V_i, W_i, X_i, Y_i together with the scalar matrices generate $N_{\mathrm{GL}(d,q)}(E)$. We have already seen that the group induced on $\overline{E}$ by the U_i and V_i is the direct product of n copies of $\mathrm{Sp}(2,r)$. Now the only maximal subgroup of $\mathrm{Sp}(4,r)$, acting on the subspace $\overline{E}_2 := \langle X_1, X_2, Y_1, Y_2\rangle \le \overline{E}$, which contains $\mathrm{Sp}(2,r) \times \mathrm{Sp}(2,r)$ is the wreath product $\mathrm{Sp}(2,r) \wr C_2$. This latter group acts imprimitively (as a group of linear transformations) on $\overline{E}_2$, and the blocks are the subspaces spanned by X_1, Y_1 and X_2, Y_2. Now W_1 fixes $\overline{E}_2$ but does not fix or interchange these two subspaces, so X_1, X_2, Y_1, Y_2 and W_1 must generate $\mathrm{Sp}(4,r)$ on $\overline{E}_2$. Since $\mathrm{Sp}(2k,r) \times \mathrm{Sp}(2,r)$ is a maximal subgroup of $\mathrm{Sp}(2k+2,r)$ for $k > 1$, we see by induction on k that U_i, V_i, X_i, Y_i for $1 \le i \le k$ and W_i for $1 \le i < k$ generate $\mathrm{Sp}(2k,r)$ in their action on the subspace $\overline{E}_k := \langle X_i, Y_i \;:\; 1 \le i \le k\rangle \le \overline{E}$. Our claim now follows from the case $k = m$ and the known structure of the extraspecial normaliser. □

It can be shown that for $r = 2$ the group $\langle V_i, X_i, Y_i, W_i\rangle$ is the normaliser of an extraspecial 2-group of plus type.

Next we study the normaliser in $\mathrm{GL}(d,q)$ of a 2-group E of symplectic type, for $d > 2$.

Lemma 9.3 *The normaliser in* $\mathrm{GL}(d,q)$ *of a group* E *of symplectic type, where* $|E| = 2^{2m+2}$ *and* $q \equiv 1 \bmod 4$*, can be constructed in time* $O(d^2 \log d \log q + \log^2 q)$.

Proof: Let $\psi := \zeta^{(q-1)/4}$, constructed in time $O(\log^2 q)$. In addition to the generators X_i, Y_i defined as in Lemma 9.1, we include the scalar matrix $Z := \psi I_d$ as a generator of E. Then E is a central product of an extraspecial group with a cyclic group of order 4. The $O(\log d)$ generators for E are constructed in time $O(d^2 \log d \log q + \log^2 q)$.

We define V_i and W_i as in Lemma 9.2, but U is now defined to be to be the (2×2)-diagonal matrix with $U_{11} = 1$ and $U_{22} = \psi$. We find that $X^U = X$ and $Y^U = \psi XY$. Let $U_i := I_{2^{m-i}} \otimes U \otimes I_{2^{i-1}}$ for $1 \leq i \leq m$, then $Y_i^{U_i} = X_i Y_i Z$. Thus, as in the case with r odd, the U_i and V_i together induce a direct product of m copies of $\mathrm{Sp}(2,2)$ on $\overline{E}$, and it can be shown as before that the $X_i, Y_i, Z, U_i, V_i, W_i$ together generate $N_{\mathrm{GL}(d,q)}(E)$. Since we have $O(\log d)$ matrices, each requiring time $O(d^2 \log q)$ to create (after the construction of ψ), the total time is $O(d^2 \log d \log q + \log^2 q)$. □

Finally, we turn to the case when E is an extraspecial 2–group of minus type. The construction here works also when $d = 2$.

Lemma 9.4 *Let* $E \leq \mathrm{GL}(d,q)$ *be an extraspecial* 2*–group of minus type, with* $d \geq 2$*. Then* $N_{\mathrm{GL}(d,q)}(E)$ *can be constructed in time* $O(d^2 \log d \log q + \log^2 q)$.

Proof: The matrices X_i, Y_i, V_i, W_i are defined exactly as before for $i > 1$. We define X_1, Y_1, U_1, V_1, W_1 as follows.

$$
\begin{aligned}
X_1 &:= I_{2^{m-1}} \otimes \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \quad \text{where } a^2 + b^2 = -1 \\
Y_1 &:= I_{2^{m-1}} \otimes \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
U_1 &:= I_{2^{m-1}} \otimes \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\
V_1 &:= I_{2^{m-1}} \otimes \begin{pmatrix} 1+a+b & 1-a+b \\ -1-a+b & 1-a-b \end{pmatrix} \\
W_1 &:= I_{2^{m-2}} \otimes \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \end{pmatrix} \quad (\text{if } m > 1)
\end{aligned}
$$

The reader can check that the relations

$$X_1^{U_1} = Y_1 X_1,\ Y_1^{U_1} = Y_1,\ X_1^{V_1} = Y_1^{-1},\ Y_1^{V_1} = Y_1 X_1$$

hold. The proof that these matrices generate the normaliser of E is similar to Lemma 9.2. □

Proposition 9.5 *Representatives of all groups in Table 3 can be constructed in time $O(d^3 \log d \log q + \log^2 q)$.*

PROOF: We have shown that in all cases, the matrices X_i, Y_i, U_i, V_i, W_i together with scalar matrices generate $G := N_{\mathrm{GL}(d,q)}(E)$. We start by replacing our existing generators by scalar multiples which lie in $\mathrm{SL}(d, q)$.

The determinants of the $O(\log d)$ matrices above can be calculated in total time $O(d^{\Omega} \log d \log q)$. Computing the required scalar for a given matrix involves finding a d-th root in $\mathrm{GF}(q)$, which by [9, Theorem 8.12] can be done in time $O(d^3 \log d \log q)$. But $\det(X_i) = \det(Y_i) = 1$ for all i, and the determinants of U_i, V_i and W_i are all independent of i, so we only need to compute three d-th roots. Scalar multiplication is an $O(d^2 \log q)$ time operation, so this can be done to the $O(\log d)$ generators of G in time $O(d^3 \log d \log q)$.

Now the group $\mathrm{Sp}(2m, r)$ is perfect except when $m = 1$ and $r \leq 3$, or when $m = r = 2$. Whenever it is perfect, we have $G = (G \cap \mathrm{SL}(d, q))Z(G)$, where $Z(G)$ consists of all scalar matrices in $\mathrm{GL}(d, q)$, and so our modified generators X_i, Y_i, U_i, V_i, W_i will all have determinant one. Although $\mathrm{SO}^-(2m, 2)$ is not perfect (it has a perfect subgroup of index 2 in general), it is a subgroup of $\mathrm{Sp}(2m, 2)$, and so again we get $G = (G \cap \mathrm{SL}(d, q))Z(G)$ for $m > 2$.

This leaves only the cases $d = r^m = 2, 3$ and 4. If $d = 3$ and $r \equiv 1 \bmod 9$, then $G = (G \cap \mathrm{SL}(d, q))Z(G)$, whereas when $r \not\equiv 1 \bmod 9$, we append $V_1^{U_1}$ to the generating set. The situation is similar when $d = 2$ or 4, and we omit the details.

In cases S and U in Table 3, since the group that we have constructed as the normaliser of E in $\mathrm{SL}(d, q)$ has the structure specified in Table 3 and there is only one conjugacy class of groups isomorphic to E in $\mathrm{GL}(d, q)$ [15, Prop. 4.6.3], it follows that the constructed group must preserve a form of the corresponding type. By [10, Theorem 4.4] E acts absolutely irreducibly, so it preserves a unique such form up to multiplication by scalars. Thus in order to determine which form is preserved we need only consider E.

We find that in case U the matrices X_i and Y_i preserve the unitary form I_d. In the symplectic case, that is when $r = 2$ and q is prime, the form preserved is $\mathrm{Diag}[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}]$, which can be transformed to the standard symplectic form by a permutation of the basis. So to conjugate the group that we have constructed into our standard version of $\mathrm{Sp}(d, q)$, we just need to carry out this permutation of the basis, which can be done in time $O(d^2 \log q)$ for each of the $O(\log d)$ generating matrices. □

10 Tensor induced groups

In this section we describe how to write down generators for the tensor induced subgroups G of Ω that arise in Theorem 1.1. A group G is *tensor induced* if it preserves a decomposition $V = V_1 \otimes V_2 \otimes \cdots \otimes V_t$, with $\dim(V_i) = m$ for $1 \leq i \leq t$: the maximal groups in this class permute the *tensor factors* V_i transitively.

From Table 4.7.A of [15] we find that, for each divisor m of d, there is at most one such G, but they only arise for $m \geq 3$ in cases L and U, and for m even and q and t both odd in case S.

Let $H \leq \mathrm{GL}(m, q)$ be a matrix group and let $K \leq \mathrm{Sym}(t)$ be transitive. Then $H \mathrm{\ TWr\ } K := (H \circ \cdots \circ H).K$ is the *tensor wreath product* of H and K (the TWr stands for tensor wreath). It is like a standard wreath product except that we take a *central* product of t copies of the base group with amalgamated subgroup $H \cap Z(\mathrm{GL}(m, q))$. The group $H \mathrm{\ TWr\ } K$ is tensor induced, with t tensor factors of dimension m.

Denote a basis of V_i by $[v_{i1}, v_{i2}, \ldots, v_{im}]$ for $1 \leq i \leq t$. A basis of $V_1 \otimes \cdots \otimes V_t$ is then $[v_{11} \otimes v_{21} \otimes \cdots \otimes v_{t1},\ v_{11} \otimes v_{21} \otimes \cdots \otimes v_{t2},\ \ldots,\ v_{11} \otimes \cdots v_{(t-1)2} \otimes v_{t1},\ \ldots,\ v_{1m} \otimes \cdots \otimes v_{tm}]$.

If each tensor factor V_i has a bilinear or sesquilinear form F_i then we can define a bilinear or sesquilinear form F on V by defining $F(v_1 \otimes \cdots \otimes v_t, w_1 \otimes \cdots \otimes w_t) := \prod_{i=1}^{t} F_i(v_i, w_i)$ and extending by linearity.

Lemma 10.1 *Let $H \leq \mathrm{GL}(m, q)$ be generated by a set of s_1 matrices, and let $K \leq \mathrm{Sym}(t)$ be transitive and generated by a set of s_2 permutations. Then $H \mathrm{\ TWr\ } K \leq \mathrm{GL}(m^t, q)$ can be constructed in time $O((s_1 + s_2)m^{2t} \log q)$.*

PROOF: Let $\langle A_1, \ldots, A_{s_1} \rangle := H$. The base group is generated as a normal subgroup by $\{A_1 \otimes I_m \otimes \cdots \otimes I_m, \ldots, A_{s_1} \otimes I_m \otimes \cdots \otimes I_m\}$, since K is transitive. These matrices are written down in time $O(s_1 (m^t)^2 \log q)$. The top group is generated by s_2 permutation matrices. Calculating the positions of the nonzero entries involves $O(s_2 t)$ integer operations, then writing down the matrices requires time $O(s_2 m^{2t} \log q)$. $\square$

10.1 Linear tensor induced groups

Proposition 10.2 *A set of representatives for the maximal tensor induced subgroups of* $\mathrm{SL}(d,q)$ *can be constructed in time* $O(d^2 \log^\epsilon d \log q)$*, for any real* $\epsilon > 0$.

Proof: Let $d = r^s$, where r is not a proper power, and let $Z := Z(\mathrm{SL}(d,q))$. We may assume that $s > 1$. Let G be a maximal tensor induced subgroup of $\mathrm{SL}(d,q)$, and let $\overline{G} := G/(G \cap Z)$. Then $Z(G) = Z$ and by [15, Prop 4.7.3] there exists a divisor $t > 1$ of s such that $d = m^t$, where G preserves a decomposition $\mathcal{D} : V = V_1 \otimes \cdots \otimes V_t$, and $\overline{G}$ is isomorphic to one of the following.

(a) $\mathrm{PSL}(m,q)^2.[(q-1,m)^3/(q-1,d)]$ $\quad t = 2, m \equiv 2 \bmod 4,\ q \equiv 3 \bmod 4$.
(b) $\mathrm{PSL}(m,q)^t.[\frac{(q-1,d/m)(q-1,m)^t}{(q-1,d)}].\mathrm{Sym}(t)$ $\quad$ otherwise.

Let $D = \mathrm{Diag}[\zeta, 1, \ldots, 1] \in \mathrm{GL}(m,q)$ and let $C \in \mathrm{GL}(d,q)$ generate Z. Then $\langle \mathrm{SL}(m,q), D\rangle = \mathrm{GL}(m,q)$, and $D^{(q-1,m)} \in Z(\mathrm{GL}(m,q))\mathrm{SL}(m,q)$.

Suppose that (b) holds. Let $H := \mathrm{SL}(m,q) \,\mathrm{TWr}\, \mathrm{Sym}(t) \leq G$, constructed in time $O(d^2 \log q)$ by Lemma 10.1. Let $U := D \otimes D^{-1} \otimes I_m \otimes \cdots \otimes I_m \in \mathrm{GL}(d,q)$, constructed in time $O(d^2 \log q)$. Since the top group of the tensor wreath product acts transitively on $\{V_i : 1 \leq i \leq t\}$ we have

$$\overline{\langle H, C, U\rangle} \cong \mathrm{PSL}(m,q)^t.[(q-1,m)^{t-1}].\mathrm{Sym}(t).$$

Let $H_1 := \langle H, C, U\rangle$, and let $E = D^{(q-1,d)/(q-1,d/m)} \otimes I_m \otimes \cdots \otimes I_m \in \mathrm{GL}(d,q)$. Then E preserves $\mathcal{D}$, and the reader may check that $\mathrm{Det}(E) = \zeta^{(q-1,d)d/(q-1,d/m)m}$, so $E \in Z(\mathrm{GL}(d,q))G$. We use the Euclidean algorithm to find in time $O(\log d)$ a power μ of ζ such that $\mathrm{Det}(\mu I_d) = \zeta^{(q-1,d)}$. We then set $S := \mu^{-d/(q-1,d/m)m} I_d$, so that $SE \in G$. It follows from the definition of D that $[\langle H_1, SE\rangle : H_1] = (q-1,d/m)(q-1,m)/(q-1,d)$, so up to conjugacy $G = \langle H_1, SE\rangle$. We construct SE in time $O(d^2 \log q)$, as $m^{t-1} < d$ so constructing S as a scalar requires time $O(d \log d \log q)$.

Next suppose that (a) holds. Let $H = Z.(\mathrm{SL}(m,q) \circ \mathrm{SL}(m,q))$, and let $U := D \otimes D^{-1}$, then $\mathrm{Det}(U) = 1$ and $[\langle H, U\rangle : H] = (q-1,m)$. Let $E := D^{(q-1,m^2)/(q-1,m)} \otimes I_m$. Then $\mathrm{Det}(E) = \zeta^{(q-1,m^2)m/(q-1,m)}$, so

$E \in Z(\mathrm{GL}(d,q))G$. Let μ be as in the previous paragraph (with $t = 2$) and let $S := \mu^{-m/(q-1,m)} I_d$. Then $\mathrm{Det}(SE) = 1$ so $SE \in G$. Let $i \in \mathbb{N}$ be minimal subject to $(SE)^i \in \langle H, U \rangle$. Then $\zeta^{(q-1,m^2)i/(q-1,m)}$ is the determinant of a scalar of $\mathrm{GL}(m,q)$, and so $(q-1,m)$ divides $(q-1,m^2)i/(q-1,m)$. Thus i is a multiple of $(q-1,m)^2/(q-1,m^2)$, and so $G = \langle H, U, SE \rangle$. The complexity in this case is the same as before.

The result then follows from Lemma 2.1. □

10.2 Symplectic tensor induced groups

Proposition 10.3 *A set of representatives of the maximal tensor induced subgroups of* $\mathrm{Sp}(d,q)$ *may be constructed in time* $O(d^3 \log^\epsilon d \log q)$*, for any real* $\epsilon > 0$.

PROOF: Let G be a maximal tensor induced subgroup of $\mathrm{Sp}(d,q)$, and let $\overline{G} = G/Z(G)$. Then by [15, Prop 4.7.4] we have $d = m^t$ for some $m, t \in \mathbb{N}$ with $t > 1$ odd, where $(m,q) \neq (2,3)$ and

$$\overline{G} \cong \mathrm{PSp}(m,q)^t.2^{t-1}.\mathrm{Sym}(t)$$

with $Z(G) = \{\pm I\} = Z(\mathrm{Sp}(d,q))$. Denote the decomposition of V that G preserves by $\mathcal{D} : V = V_1 \otimes \cdots \otimes V_t$.

We construct $H := \mathrm{Sp}(m,q)\mathrm{TWrSym}(t)$ in time $O(d^2 \log q)$, by Lemma 10.1. Then H preserves $\mathcal{D}$, and from the discussion preceding Lemma 10.1, H preserves a symplectic form. Therefore H is $\mathrm{GL}(d,q)$-conjugate to a subgroup of G of index 2^{t-1}. Let $D = \mathrm{Diag}[\zeta, \ldots, \zeta, 1, \ldots, 1]$ so that $\langle \mathrm{Sp}(m,q), D \rangle = \mathrm{GSp}(m,q)$. Let $U := D \otimes D^{-1} \otimes I_m \otimes \cdots \otimes I_m \in \mathrm{GL}(d,q)$. We define $H_1 := \langle H, U \rangle$, then $H_1 \cong G$. By the results in Section 3, we may find a matrix M in time $O(d^3 \log q)$ such that $H_1^M = G$.

By Lemma 2.1 there are $O(\log^\epsilon d)$ groups to construct. □

10.3 Unitary tensor induced groups

We use the form $F = \mathrm{AntiDiag}[1, \ldots, 1]$, and let $Z := Z(\mathrm{SU}(d,q))$.

Proposition 10.4 *A set of representatives of the maximal tensor induced subgroups of* $\mathrm{SU}(d,q)$ *can be constructed in time* $O(d^3 \log^\epsilon d \log q)$*, for any real* $\epsilon > 0$.

Table 4: Maximal Classical Groups

Case	Type	Conditions
L	$\mathrm{Sp}(d,q)$	d even, $d \geq 4$
L	$\mathrm{SU}(d,p^{e/2})$	e even, $d \geq 3$
L	$\Omega^{\varepsilon}(d,q)$	q odd, $d \geq 3$
S	$\mathrm{SO}^{\varepsilon}(d,q)$	q even, $d \geq 4$

PROOF: Let $d = r^s$, where r is not a proper power and $s > 1$. Let G be a maximal tensor induced subgroup of $\mathrm{SU}(d,q)$, and let $\overline{G} := G/(G \cap Z)$. Then $Z(G) = Z$ and by [15, Prop 4.7.3] there exists a divisor t of s such that $d = m^t$, G preserves a decomposition $\mathcal{D} : V = V_1 \otimes \cdots \otimes V_t$, and $\overline{G}$ is isomorphic to one of the following.

(a) $\mathrm{PSL}(m,q)^2.[(q+1,m)^3/(q+1,d)]$ $\quad t = 2,\ m \equiv 2 \bmod 4, q \equiv 3 \bmod 4.$
(b) $\mathrm{PSL}(m,q)^t.[\frac{(q+1,d/m)(q+1,m)^t}{(q+1,d)}].\mathrm{Sym}(t)$ $\quad$ otherwise.

The construction of G is almost identical to that of Proposition 10.2, and we leave it to the reader. □

11 Classical subgroups

Finally, we describe how to construct the classical subgroups G of Ω arising in Theorem 1.1. These are summarised in Table 4, which comes from Table 4.8.A of [15]. The type is the quasisimple group contained in G. Note that the unitary groups have no maximal classical subgroups.

11.1 Linear classical groups

In this subsection, let $Z := Z(\mathrm{SL}(d,q))$ and let C generate Z.

Proposition 11.1 *A representative of the maximal classical subgroups of* $\mathrm{SL}(d,q)$ *of symplectic type may be constructed in time* $O(d^2 \log q + \log^2 q)$.

PROOF: Let G be a maximal symplectic subgroup of $\mathrm{SL}(d,q)$, and let $c := (q-1,2)(q-1,d/2)/(q-1,d)$. Then by [15, Prop. 4.8.3] $G \cong Z.\mathrm{PSp}(d,q).c$.

Let $A, B \in \mathrm{SL}(d,q)$ generate $\mathrm{Sp}(d,q)$, constructed in time $O(d^2 \log q)$ as in Lemma 2.3. If q is even or $(q-1, d/2) = (q-1,d)/2$ then up to conjugacy $G = \langle A, B, C\rangle$. Suppose otherwise, and let

$$D := \mathrm{Diag}[\zeta, \ldots, \zeta, 1, \ldots, 1] \in N_{\mathrm{GL}(d,q)}(\mathrm{Sp}(d,q)) \setminus \langle C, \mathrm{Sp}(d,q)\rangle.$$

Then $\mathrm{Det}(D) = \zeta^{d/2}$.

Solve $di \equiv d/2 \bmod (q-1)$ in time $O(\log(d/(d, q-1))) = O(\log d)$, as in the proof of Proposition 8.1. Compute ζ^{-i} in time $O(\log^2 q)$ and construct $E := \zeta^{-i} D$ in time $O(d^2 \log q)$. Then $E \in N_{\mathrm{SL}(d,q)}(\mathrm{Sp}(d,q))$. Since no scalar multiple of D lies in $\mathrm{Sp}(d,q)$, up to conjugacy $G = \langle A, B, C, E\rangle$. □

Proposition 11.2 *A set of representatives of the maximal orthogonal subgroups of* $\mathrm{SL}(d,q)$ *may be constructed in time* $O(d^3 \log q + \log^3 q)$.

Proof: For $\varepsilon = +, -$ or $\circ$, let G_ε be a maximal orthogonal subgroup of $\mathrm{SL}(d,q)$ of type ε. Then q is odd and $G_\varepsilon \cong Z.\mathrm{SO}^\varepsilon(d,q).(d,2)$ [15, Prop. 2.8.2].

Let A_ε and B_ε generate $\mathrm{SO}^\varepsilon(d,q)$, as in Lemma 2.4. If d is odd then up to SL-conjugacy $G = Z.\mathrm{SO}(d,q)$. Suppose that d is even, and let W_ε be as defined in Proposition 8.4. Then up to conjugacy $G_\varepsilon = \langle A_\varepsilon, B_\varepsilon, C, W_\varepsilon\rangle$. □

Proposition 11.3 *A representative of the maximal unitary subgroups of* $\mathrm{SL}(d,q)$ *may be constructed in time* $O(d^2 \log q + \log^2 q)$.

Proof: Let G be a maximal unitary subgroup of $\mathrm{SL}(d,q)$ and let $q = p^e$. Then e is even, and we let $q_0 := p^{e/2}$ and

$$c := (q_0+1, d)(q-1)/([q_0+1, (q-1)/(q-1,d)](q-1,d)).$$

By [15, Prop. 4.8.5] we have $Z(G) = Z$ and $G/Z \cong \mathrm{PSU}(d, q_0).[c]$.

Let A and B generate $\mathrm{SU}(d, q_0)$, with a form represented by the identity matrix. If $c = 1$ then up to conjugacy $G = \langle A, B, C\rangle$.

Suppose otherwise, and let $D := \mathrm{Diag}[\zeta^{q_0-1}, 1, \ldots, 1] \in \mathrm{GL}(d,q)$, so that we have $\langle A, B, D\rangle = \mathrm{GU}(d, q_0)$, and $\langle \mathrm{GU}(d,q_0), \zeta I_d\rangle = N_{\mathrm{GL}(d,q)}(\mathrm{SU}(d,q_0))$. The group of order c consists of all products of D and ζI_d of determinant 1. Similarly to the tensor product case, we find generators for the normaliser by finding a basis for the nullspace of $[q_0 - 1, d, q-1]$, in time $O(d \log q)$. This yields at most two matrices, X and Y. We may set $G = \langle A, B, C, X, Y\rangle$. □

11.2 Symplectic classical groups

Proposition 11.4 *A set of representatives of the maximal classical subgroups of* $\mathrm{Sp}(d, q)$ *may be constructed in time* $O(d^3 \log q + \log^3 q)$.

PROOF: The maximal classical subgroups of $\mathrm{Sp}(d, q)$ are orthogonal, of types $\varepsilon \in \{+, -\}$, and occur only for even q [15]. Let G_ε be a maximal classical subgroup of $\mathrm{Sp}(d, q)$ of type ε. By [15, Prop. 4.8.6], $G_\varepsilon/(G_\varepsilon \cap Z(\mathrm{Sp}(d, q))) \cong \mathrm{O}^\varepsilon(d, q)$. Since $Z(\mathrm{Sp}(d, q)) = 1$ for q even, and $\mathrm{O}^\varepsilon(d, q) = \mathrm{SO}^\varepsilon(d, q)$ for q even, we generate $H_\varepsilon \sim_{GL} G$ in time $O(d^3 \log + \log^3 q)$ by Lemma 2.4.

For even q, the matrix of the symmetric bilinear form preserved by H_ε is also the matrix of a symplectic form. Our choice of form implies that $H_+ \leq \mathrm{Sp}(d, q)$ and so up to conjugacy $G = H$. We use Proposition 3.1 to conjugate H_- to preserve our chosen symplectic form. □

12 The symplectic groups in dimension four

In dimension 4, if q is even then $\mathrm{PSp}(4, q) = \mathrm{Sp}(4, q)$ has a *graph* automorphism, arising from the Dynkin diagram for C_2. Groups which contain the graph automorphism have a different subgroup structure from other symplectic groups; they do not have the standard Aschbacher classes of subgroups, but behave as described in this section. Throughout, $q := 2^e$, and we assume that $e > 1$ since $\mathrm{Sp}(4, 2) \cong \mathrm{Sym}(6)$.

The group which consists of $\mathrm{Sp}(4, q)$ extended by a graph automorphism is denoted $\mathrm{Sp2}(4, 2^e) := \mathrm{Sp}(4, 2^e).2$. The full automorphism group of $\mathrm{Sp}(4, 2^e)$ is denoted $\Gamma\mathrm{Sp2}(4, 2^e) := \Gamma\mathrm{Sp}(4, 2^e)\langle\iota\rangle = \mathrm{Sp}(4, 2^e).e.2$. The maximal subgroups of $\mathrm{Sp2}(4, 2^e)$ all extend to maximal subgroups of $\Gamma\mathrm{Sp2}(4, 2^e)$, and *vice versa*, so it suffices to discuss the maximal subgroups of this latter group.

We give a statement of Aschbacher's theorem for this family of groups, see [1, Theorem 14.2] for more details.

Theorem 12.1 *Let* K *be a maximal subgroup of* $\Gamma\mathrm{Sp2}(4, 2^e)$ *where* $e > 2$, *and let* $G := K \cap \mathrm{Sp}(4, 2^e)$. *Then* G *lies in one of the following classes:*

- $\mathcal{A}_1$ *The stabiliser of a point and a totally singular subspace containing it. There is a unique conjugacy class of such groups in* $\mathrm{Sp}(4, 2^e)$.

- $\mathcal{A}_2$ *The stabiliser of an imprimitive decomposition and a quadratic form of plus type. There are two nonisomorphic classes of such groups in* $\mathrm{Sp}(4, 2^e)$.

$\mathcal{A}_3$ *A semilinear group, of a degree 2 field extension, that preserves a quadratic form of minus type. There is a unique conjugacy class of such groups in* $\mathrm{Sp}(4, 2^e)$.

$\mathcal{A}_4$ *A subfield group over* $\mathrm{GF}(2^f)$ *where* e/f *is prime. For each choice of* f *there is a unique conjugacy class of such groups in* $\mathrm{Sp}(4, 2^e)$.

$\mathcal{A}_5$ *The Suzuki group* $\mathrm{Sz}(2^e)$. *These occur only when* e *is odd, in which case there is a unique conjugacy class of such groups in* $\mathrm{Sp}(4, 2^e)$.

$\mathcal{S}$ *G is almost simple modulo scalars, written over a minimal field, is absolutely irreducible and not semilinear.*

In class $\mathcal{A}_2$ there are two families of groups. This is because the space $\mathrm{GF}(2^e)^4$, equipped with a quadratic form Q of plus type, has two direct sum decompositions. The first is into two 2-spaces, each of plus type. The second is into two 2-spaces, each of minus type. The stabiliser in $\mathrm{SO}^+(4, 2^e)$ of the first type of decomposition is $\mathrm{SO}^+(2, 2^e) \wr \mathrm{Sym}(2)$, and the stabiliser of the second is $\mathrm{SO}^-(2, 2^e) \wr \mathrm{Sym}(2)$.

It is the novelty subgroups in classes $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ which we must describe how to construct, as well as the Suzuki group $\mathrm{Sz}(q)$. Note that from the perspective of Aschbacher's theorem for $\mathrm{PSp}(4, q)$, the Suzuki group is considered to lie in $\mathcal{S}$. However, since it is the centraliser in $\mathrm{PSp}(4, q)$ of an outer involution, it constitutes an Aschbacher class in its own right when discussing $\Gamma\mathrm{Sp2}(4, q)$.

Lemma 12.2 *A representative of the groups in class* $\mathcal{A}_1$ *can be constructed in time* $O(e)$.

Proof: Let G be the intersection of a point stabiliser and a subspace stabiliser. Without loss of generality the point is $V := \langle e_1 \rangle$ and the subspace (which is maximal isotropic) is $W := \langle e_1, e_2 \rangle$.

Let $A_1 := \mathrm{Diag}[\zeta, 1, 1, \zeta^{-1}]$ and $A_2 := \mathrm{Diag}[1, \zeta, \zeta^{-1}, 1]$. Let T_1 be a transvection with 1 in positions $(2, 1)$ and $(4, 3)$, and zeros in all other off-diagonal entries. Let T_2 be a transvection with 1 in positions $(3, 1)$ and $(4, 2)$, and zeros in all other off-diagonal entries. Similarly let T_3 have a 1 in position $(3, 3)$, and T_4 have a 1 in position $(4, 1)$.

The reader may check that all six of these matrices lie in $\mathrm{Sp}(4, q)$. It is clear that they all stabilise V and W. The reader may check that any matrix which is in the symplectic group and stabilises V and W can be written as a product of these. $\square$

Lemma 12.3 *Representatives of the two conjugacy classes of groups in class $\mathcal{A}_2$ can be constructed in time $O(e^3)$.*

PROOF: We construct $\mathrm{SO}^+(2,q)$ in time $O(e^3)$, and then construct $\mathrm{SO}^+(2,q) \wr \mathrm{Sym}(2)$ in constant time. We use the results of Section 3 to conjugate $\mathrm{SO}^+(2,q) \wr \mathrm{Sym}(2)$ so that it preserves our standard symplectic form. Similarly for $\mathrm{SO}^-(2,q) \wr \mathrm{Sym}(2)$. $\square$

Lemma 12.4 *A representative of the groups in class $\mathcal{A}_3$ can be constructed in time $O(e^2)$.*

PROOF: We let A be the companion matrix for a primitive element of $\mathrm{GF}(q^4)$ over $\mathrm{GF}(q)$. Then A has order $q^4 - 1$. Let $B := A^{q^2-1}$, calculated in time $O(e^2)$. We let C be the image of the field automorphism $x \mapsto x^q$ of $\mathrm{GF}(q^4)$. Then C normalises B. The group $H := \langle B, C \rangle$ is isomorphic to a maximal semilinear subgroup of $\mathrm{SL}(2,q^2) \cong \mathrm{SO}^-(4,q)$, and hence is the intersection of $\mathrm{SO}^-(4,q)$ with $\mathrm{Sp}(2,q^2).2$. We use the results of Section 3 to conjugate H to a suitable group $G \leq \mathrm{Sp}(4,q)$. $\square$

Lemma 12.5 *We construct a representation of* $\mathrm{Sz}(2^e)$ *in time $O(e^2)$.*

PROOF: An explicit isomorphism between the Chevalley group $C_2(2^e)$ ($= B_2(2^e)$) and $\mathrm{Sp}(4,2^e)$ is constructed in [6, Thm 11.3.2], and the graph automorphism g of $B_2(2^e)$ is defined in [6, Prop. 12.3.3]. The Suzuki group $\mathrm{Sz}(2^e)$ for e odd is defined in [6, Section 13.4] as the subgroup of $B_2(2^e)$ fixed by the involutory automorphism gf of $B_2(2^e)$, for a suitably chosen field automorphism f. This enables us to construct explicit generators of $\mathrm{Sz}(2^e)$ as a subgroup of $\mathrm{Sp}(4,2^e)$. Let $t = 2^{(e+1)/2}$. Then, for $e > 1$, they can be chosen as

$$\begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^{t-1} & 0 & 0 \\ 0 & 0 & \zeta^{1-t} & 0 \\ 0 & 0 & 0 & \zeta^{-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & \zeta & \zeta^t \\ 0 & 1 & 0 & \zeta \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

which can be constructed in time $O(e^2) = O(\log^2 q)$.

$\square$

References

[1] Aschbacher, M. On the maximal subgroups of the finite classical groups, *Invent. Math.* 76 **1984**, 469-514.

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

[3] Bürgisser, P; Clausen, M.; Shokrollahi, M.A.; *Algebraic Complexity Theory* Springer-Verlag Berlin Heidelberg New York, **1990**.

[4] Bosma, W; and Cannon, J.J, eds. *Handbook of Magma Functions*, Edition 2.9, **2002**.

[5] Cannon, J.J; Holt, D.F. Computing maximal subgroups of finite groups, to appear in *J. Symbolic Comput.*.

[6] Carter, R.W. *Simple Groups of Lie Type.* John Wiley and Sons, **1972**.

[7] Dixon, J.D; Mortimer, B. The primitive permutation groups of degree less than 1000. *Math. Proc. Cambridge Philos. Soc.*, 103, **1988**, 213–238.

[8] Eick, B; Hulpke, A. Computing the maximal subgroups of a permutation group I. In W.M. Kantor and Á. Seress, editors, *Groups and Computation III*, Ohio, 1999, pages 155–168. Walter de Gruyter, **2001**.

[9] Geddes, K.O; Czapor, S.R; Labahn, G. *Algorithms for Computer Algebra.* Kluwer Academic Publishers, **1992**.

[10] Gorenstein, D. "Finite Groups", Harper and Row, **1968**.

[11] Hardy, G.H; Wright, E.M. *An introduction to the theory of numbers.* 5th edition. Oxford University Press: New York **1979**.

[12] Hiss, G; Malle, G. Low dimensional representations of quasi-simple groups. *LMS J. Comput. Math.*, 4, **2001**, 22–63.

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

[14] Kantor, W.M; Seress, Á. *Black box classical groups.* Mem. Amer. Math. Soc., 149, **2001**.

[15] Kleidman, P; Liebeck, M.W. *The subgroup structure of the finite classical groups*. Cambridge University Press: Cambridge, **1990**.

[16] Liebeck, M.W; Praeger, C.E; Saxl, J. The maximal factorizations of the finite simple groups and their automorphism groups. *Mem. Amer. Math. Soc.* 86, **1990**.

[17] Liebeck, M.W; Praeger, C.E; Saxl, J. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra* 111, **1987**, 365–383.

[18] Liebeck, M.W; Seitz, G.M. A survey of maximal subgroups of exceptional groups of Lie type. In A. A. Ivanov, M. W. Liebeck and J. Saxl, eds, *Groups, combinatorics & geometry (Durham, 2001)*, World Sci. Publishing, River Edge, NJ, **2003**, 139–146.

[19] Lübeck, F. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.*, 4, **2001**, 135–169.

[20] Lidl, R; Niederreiter, H. *Finite Fields*. Encyclopedia of mathematics and its applications, v20. Reading, Mass: Addison-Wesley, **1983**.

[21] Roney-Dougal, C.M. Conjugacy of subgroups of the general linear group. *Exp. Math.*, 13, **2004**, 151–163.

[22] Strassen, V. Gaussian elimination is not optimal. *Numer. Math.*, 13, **(1969)**, 354–356.

[23] Taylor, D.E. Pairs of generators for matrix groups, I. *The Cayley Bulletin*, 3, **1987**, 76–85.

[24] Wilson, R.A; Walsh, P; Tripp, J; Suleiman, I; Rogers, S; Parker, R; Norton, S; Nickerson, S; Linton, S; Bray, J; `<http://web.mat.bham.ac.uk/atlas/v2.0/>`