LMS J. Comput. Math. 13 (2010) 164–191 © 2010 Authors
doi:10.1112/S1461157009000035

Constructing maximal subgroups of orthogonal groups

Derek F. Holt and Colva M. Roney-Dougal

Abstract

In this paper we construct the maximal subgroups of geometric type of the orthogonal groups in dimension d over $\mathrm{GF}(q)$ in $O(d^3 + d^2 \log q + \log q \log \log q)$ finite field operations.

1. *Introduction*

With only two families of exceptions, the subgroups of the almost simple extensions of the finite simple classical groups are divided into nine (not mutually exclusive) classes by Aschbacher's theorem [**1**]. The maximal subgroups in the first eight of these classes are the *geometric* maximal subgroups, and are described in detail in [**14**]. The ninth class, $\mathcal{S}$, consists roughly of absolutely irreducible groups that are almost simple modulo scalars, other than classical groups in their natural representation.

The two families of exceptions to Aschbacher's theorem are: almost simple extensions of $\mathrm{PSp}(4, 2^e)$ containing the graph automorphism, whose maximal subgroups are described in [**1**]; and almost simple extensions of $\mathrm{P}\Omega^+(8, q)$ containing the triality graph automorphism, whose maximal subgroups are described in [**13**]. Although Aschbacher's theorem does not apply to these families (the specified graph automorphism interchanges subgroups from different Aschbacher classes), we shall call a subgroup of such a group *geometric* if its intersection with the simple group is geometric.

This paper describes algorithms for writing down generators of the geometric maximal subgroups of the finite simple orthogonal groups and their almost simple extensions. More precisely, we write down canonical generators of the pre-images in $\Omega^\epsilon(d, q)$ of the intersections of these maximal subgroups with $\mathrm{P}\Omega^\epsilon(d, q)$. This paper builds on [**10**], where we presented similar algorithms for the other almost simple classical groups.

The two main papers on the computation of maximal subgroups of an arbitrary finite permutation group G are [**4**, **7**]. These both show that the problem can effectively be reduced to the case that G is almost simple. The vast bulk of the cases that arise for G almost simple can then be handled using the methods that we describe here and in [**10**], 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; a complete list of quasisimple groups in $\mathcal{S}$ is known for degree $d \leqslant 250$ [**9**, **15**], although the question of maximality is still in general open.

The algorithms presented in this paper construct the geometric maximal subgroups of the (quasi)simple orthogonal groups. They can be combined with the subgroup conjugacy information in [**1**, **13**, **14**], and with explicit descriptions of when the groups of each type are maximal, to produce the geometric maximal subgroups of every group G with $\Omega^\epsilon(d, q) \trianglelefteq G \leqslant \mathrm{C\Gamma O}^\epsilon(d, q) = \mathrm{N}_{\Gamma\mathrm{L}(d,q)}(\Omega^\epsilon(d, q))$, and similarly for their projective counterparts, as well as the geometric maximal subgroups of eight-dimensional orthogonal groups of plus type. Note that if $(d, \epsilon) \neq (8, +)$, then $\mathrm{PC\Gamma O}^\epsilon(d, q) = \mathrm{Aut}(\mathrm{P}\Omega^\epsilon(d, q))$.

Received 5 February 2009; revised 6 October 2009.

2000 Mathematics Subject Classification 20D06, 20E28 (primary), 20G40, 68Q25 (secondary).

The second author would like to acknowledge the support of the Nuffield Foundation, and of EPSRC grant EP/C523229/1.

Our algorithms have been implemented in Magma [2] and are publicly available as part of the standard release of Magma. They can be used in two ways. The function ClassicalMaximals constructs the geometric maximal subgroups of $\Omega^\epsilon(d, q)$, $\mathrm{SO}^\epsilon(d, q)$, $\mathrm{GO}^\epsilon(d, q)$ or $\mathrm{CO}^\epsilon(d, q)$ $(= \mathrm{N}_{\mathrm{GL}(d,q)}(\mathrm{GO}^\epsilon(d, q)))$ in their natural representations (as well as producing the maximal subgroups of the classical groups that are studied in [10]). It runs in under a minute on an average laptop machine for d less than around 70 and moderate q.

Secondly, our algorithms are combined with representations of groups in $\mathcal{S}$ to construct the maximal subgroups of orthogonal groups in low dimensions over an arbitrary finite field. This algorithm uses constructive recognition algorithms [12] 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.

The subgroups that we construct are *canonical* in the sense that different calls to the same algorithm will return the same generating matrices each time. To create canonical subgroups, we will need certain canonical field elements for their matrix entries, and by this we mean that different calls to the same algorithm will return the same field element each time. This is often useful, for example, when investigating containments between subgroups, and removes one of the major problems with randomised algorithms: the non-reproducibility of the output.

The following theorem is our main result.

Theorem 1.1. *Let G be a group with $\mathrm{P}\Omega^\epsilon(d, q) \leqslant G \leqslant \mathrm{Aut}(\mathrm{P}\Omega^\epsilon(d, q))$, where $d \geqslant 7$. Let $\mathcal{M}$ be the set of geometric maximal subgroups of G, up to conjugacy in $\mathrm{PCO}^\epsilon(d, q)$. Let $\mathcal{M}_1$ be the set of intersections of groups in $\mathcal{M}$ with $\mathrm{P}\Omega^\epsilon(d, q)$ and let $\mathcal{M}_2$ be the set of pre-images in $\Omega^\epsilon(d, q)$ of groups in $\mathcal{M}_1$. Then canonical generators of all groups in $\mathcal{M}_2$ can be calculated and written down in $O(d^3 + d^2 \log q + \log q \log\log q)$ elementary operations in $\mathrm{GF}(q)$.*

We calculate representatives up to conjugacy in $\mathrm{PCO}^\epsilon(d, q)$ because [1, Theorem $B\Delta$] states that, except in the type + dimension eight case, the orbits of $\mathrm{PCO}^\epsilon(d, q)$ on conjugacy classes of subgroups are the same as those of $\mathrm{Aut}(\mathrm{P}\Omega^\epsilon(d, q))$, and that these groups are transitive on each of the 'types' of group for each Aschbacher class; see also [14, Proposition 4.0.2]. The types in each class are presented at the beginning of the corresponding section of this paper. We deal with the exceptional dimension eight case separately. Note that if $d < 7$, then $\Omega^\epsilon(d, q)$ is either not simple or is isomorphic to a classical group of linear, symplectic or unitary type and hence has been dealt with in [10].

To write down generators of maximal subgroups of $\mathrm{SO}^\epsilon(d, q)$, $\mathrm{GO}^\epsilon(d, q)$ and $\mathrm{CO}^\epsilon(d, q)$ in their natural representations, we need appropriate elements of these groups that lie outside of $\Omega^\epsilon(d, q)$ and normalise the intersection of the maximal subgroup with $\Omega^\epsilon(d, q)$. Generally, this is straightforward, and often these normalising elements are already used in our algorithms. When their construction is not so clear (Lemmas 5.5 and 6.4), we explain it briefly in a remark following the proof.

The layout of this paper is as follows. In § 2, we introduce some notation and state a number of general lemmas. We then present various results on classical groups and forms in § 3. In the remaining sections, we present our algorithms for each of the seven geometric families of subgroups of $\mathrm{P}\Omega^\epsilon(d, q)$, before finishing with the additional geometric subgroups of extensions of $\mathrm{Aut}(\mathrm{P}\Omega^+(8, q))$ that contain the triality automorphism. We will frequently refer to [14], and the reader may find it useful to have a copy to hand.

2. *Notation and mathematical preliminaries*

In this section we collect our notation, as well as giving some basic results on finite fields and complexity.

Throughout, let p be a prime and set $q = p^e$. Let ζ be a primitive multiplicative element of $\mathrm{GF}(q)$ and let ξ denote a primitive element of $\mathrm{GF}(q^2)$ with $\xi^{q+1} = \zeta$. Let $V = \mathrm{GF}(q)^d$ with standard basis $v_1, \ldots, v_d$.

We measure our complexity in terms of the number of elementary finite field operations, namely addition, negation, multiplication and inversion. So, whenever we say that an operation involving matrices over $\mathrm{GF}(q)$ is $O(f(d,q))$, we mean that it can be carried out using $O(f(d,q))$ elementary field operations in $\mathrm{GF}(q)$. So, for example, elements of $\mathrm{GL}(d,q)$ can generally be constructed in $O(d^2)$ field operations. Matrix multiplication, and other basic operations such as matrix inversion, nullspace and determinant computation, are $O(d^\omega)$ field operations (see for example [**3**]). The current best known bounds for ω are $2 \leqslant \omega \leqslant 2.376$ [**5**], whilst Magma uses the $\omega = \log_2 7$ algorithm of [**19**] (for sufficiently large d, depending on the value of q). We shall not assume the availability of discrete logarithms.

We assume that primitive polynomials, together with associated primitive (multiplicative) field elements, are fixed for all finite fields that arise, so that ζ and ξ are canonical. The elements of $\mathrm{GF}(p^e)$ are represented as polynomials in $1, \zeta, \ldots, \zeta^{e-1}$ with coefficients in $\mathrm{GF}(p)$. Assume that all defining polynomials respect inclusion of finite fields in one another, so that if $f \mid e$ then $\zeta^{(p^e-1)/(p^f-1)}$ is the chosen primitive element of $\mathrm{GF}(p^f)$. Further, assume that defining polynomials are known for all extensions of finite fields that we encounter.

By ordering the elements of $\mathrm{GF}(p)$ as $0, \ldots, p-1$, we can order the elements of $\mathrm{GF}(q)$ by lexicographically ordering the polynomials by their coefficients. Thus, if we know the roots of some polynomial over $\mathrm{GF}(q)$, then we can fix a canonical root by taking the first root with respect to this ordering.

LEMMA 2.1.

(1) *If* $\alpha \in \mathrm{GF}(p^{2e}) = \mathrm{GF}(q^2)$ *lies in* $\mathrm{GF}(q)$, *then* α *can be represented as an element of* $\mathrm{GF}(q)$ *in* $O(e)$ *field operations in* $\mathrm{GF}(q)$.

(2) *Let* $\alpha \in \mathrm{GF}(p^{se}) = \mathrm{GF}(q^s)$ *and let* ν *be the primitive element of* $\mathrm{GF}(q^s)$. *Then* α *can be written as a* $\mathrm{GF}(q)$*-linear combination of* $1, \nu, \ldots, \nu^{s-1}$ *in* $O(s^2 e)$ *field operations in* $\mathrm{GF}(q)$.

Proof.

(1) Let $x^2 - \beta x - \gamma$ with $\beta, \gamma \in \mathrm{GF}(q)$ be the minimal polynomial of ξ over $\mathrm{GF}(q)$. So, $\xi^2 = \beta\xi + \gamma$. We are given $\alpha = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{2e-1}\xi^{2e-1}$, with $a_i \in \mathrm{GF}(p)$ for all i. To represent α as a polynomial of degree e in ζ, calculate the powers $\xi^2 = \beta\xi + \gamma$, $\xi^3 = (\beta^2 + \gamma)\xi + \beta\gamma, \ldots, \xi^{2e-1}$, multiply by the appropriate coefficients and sum. Since $\alpha \in \mathrm{GF}(q)$, the coefficients of ξ will sum to zero, thus representing α as an element of $\mathrm{GF}(q)$.

(2) We are given the minimal polynomial of ν over $\mathrm{GF}(q)$, and hence we can write ν^s as a $\mathrm{GF}(q)$-linear combination of $1, \nu, \ldots, \nu^{s-1}$ in $O(s)$ field operations. Let $\alpha = b_0 + b_1\nu + \ldots + b_{se-1}\nu^{se-1}$, with $b_i \in \mathrm{GF}(p)$ for all i. For $s+1 \leqslant i \leqslant se-1$, write $b_i\nu^i = b_i\nu\nu^{i-1}$, then substitute the found expression for ν^{i-1}. This requires $O(s)$ field operations for each step, so $O(s^2 e)$ field operations in total. □

LEMMA 2.2. *Let* $d \in \mathbb{N}$.

(1) *The number of distinct prime divisors of* d *is* $O(\log d)$.
(2) *The number of divisors of* d *is* $O(d^\varepsilon)$ *for every real* $\varepsilon > 0$.

Proof. The first statement is clear: if d is a product of k distinct primes, then $d \geqslant 2^k$. For the second, see [**8**, Theorem 315]. □

Let (a,b) denote the greatest common divisor of integers a and b, and $[a,b]$ their least common multiple. Write $\mathrm{Diag}[a_1, \ldots, a_d]$ for the $d \times d$ matrix B with $b_{ii} = a_i$ and $b_{ij} = 0$ for $i \neq j$, and

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

write $\mathrm{AntiDiag}[a_1, \ldots, a_d]$ for the matrix B with $b_{i,d-i+1} = a_i$ and 0 elsewhere. Define the elementary matrix $E_{i,j}$ to be square, with 1 in position (i, j) and 0 elsewhere. A matrix A is *block diagonal* if the non-zero blocks of A are $X_1, \ldots, X_s$ with $s > 1$, and the main diagonals of $X_1, \ldots, X_s$ are on the main diagonal of A. We write $A = X_1 \oplus \ldots \oplus X_s$. As usual, I_d is the identity of $\mathrm{GL}(d, q)$ and $J_d = \mathrm{AntiDiag}[1, \ldots, 1] \in \mathrm{GL}(d, q)$. If A denotes a matrix, then A^{T} denotes the transpose of A.

The Kronecker product $A \otimes B$ of a $k \times k$ matrix A and an $l \times l$ matrix B is the $kl \times kl$ matrix C, where the $((i-1)l + s, (j-1)l + t)$th entry of C is $A_{ij}B_{st}$ for $1 \leqslant i, j \leqslant k$ and $1 \leqslant s, t \leqslant l$. The $\otimes$ operation is associative, and $(A \otimes B)(C \otimes D) = AC \otimes BD$. The matrix $A \otimes B$ can be written down in $O(k^2 l^2)$.

By *constructing* a group, we mean producing a set of generating elements for the group: this will generally be a set of matrices. When describing groups, the symbol $[n]$ denotes a soluble group of order n.

3. *Classical groups and forms*

In this section we define various concepts needed for the orthogonal groups, as well as presenting results on generation of the classical groups and the construction of similarities from one form to another. See [20] for more background information on this section.

3.1. *Quadratic forms and standard bases*

DEFINITION 3.1. A map $F : V \times V \to \mathrm{GF}(q)$ is a *symmetric bilinear form* if $F(u, v) = F(v, u)$ and $F(u + \lambda v, w) = F(u, w) + \lambda F(v, w)$ for all $u, v, w \in V$ and $\lambda \in \mathrm{GF}(q)$. A map $Q : V \to \mathrm{GF}(q)$ is a *quadratic form* if $Q(\lambda v) = \lambda^2 Q(v)$ for all $v \in V$ and $\lambda \in \mathrm{GF}(q)$ and the polar form $F_Q(u, v) := Q(u + v) - Q(u) - Q(v)$ is a symmetric bilinear form. The form F is *non-degenerate* if $F(u, v) = 0$ for all $v \in V$ implies that $u = 0$, and the quadratic form Q is non-degenerate if and only if its polarisation F_Q is non-degenerate.

For F bilinear, define the matrix M_F of F by $m_{ij} = F(v_i, v_j)$. Then $F(u, v) = uM_F v^{\mathrm{T}}$ for all $u, v \in V$ (recall that T denotes transpose). For Q quadratic, define the matrix T_Q of Q by setting $t_{ii} = Q(v_i)$, $t_{ij} = F_Q(v_i, v_j)$ for $i < j$ and $t_{ij} = 0$ for $i > j$, so that $Q(v) = vT_Q v^{\mathrm{T}}$. Then $M_{F_Q} = T_Q + T_Q^{\mathrm{T}}$. We write F for F_Q when the quadratic form Q is clear. We abuse notation and often refer to M_F and T_Q as forms, rather than matrices of forms: we also write F and Q for M_F and T_Q, when the context is clear. If q is odd then Q and F_Q determine each other, but if q is even then F_Q does not determine Q.

Let (V, Q) be a vector space equipped with a non-degenerate quadratic form Q and corresponding bilinear form F. A subspace $U \leqslant V$ is *non-degenerate* if, whenever $F(u, v) = 0$ for some fixed $u \in U$ and all $v \in U$, then $u = 0$; otherwise, U is *degenerate*. A vector $v \in V$ is *singular* if $Q(v) = 0$ and the subspace U is *totally singular* if $F(u, v) = Q(u) = 0$ for all $u, v \in U$. If $W \leqslant V$, then W and U are *isometric* if there exists an invertible linear map $f : U \to W$ such that $Q(uf) = Q(u)$ for all $u \in U$.

Two quadratic forms Q_1 and Q_2 are *similar* if there exist $g \in \mathrm{GL}(d, q)$ and $\lambda \in \mathrm{GF}(q)$ such that $Q_1(vg) = \lambda Q_2(v)$ for all $v \in V$. If $\lambda = 1$ then they are *isometric*. If d is odd, then there is a single similarity type of non-degenerate quadratic form, denoted $\circ$, but two isometry types. However, if a group $G \leqslant \mathrm{GL}(2m + 1, q)$ preserves a quadratic form Q, then G also preserves λQ for all $\lambda \in \mathrm{GF}(q)$, so every group preserving a non-degenerate quadratic form preserves one of each isometry type. If d is even, then there are two similarity types of non-degenerate quadratic form, corresponding to two isometry types. One type has all maximal totally singular subspaces of dimension $d/2$, and is *type* $+$. The other has all maximal totally singular subspaces of dimension $d/2 - 1$, and is *type* $-$.

Denote the stabiliser in $\mathrm{GL}(d, q)$ of a quadratic form Q by $\mathrm{GO}(d, q, Q)$. The normaliser of $\mathrm{GO}(d, q, Q)$ in $\mathrm{GL}(d, q)$ is the *conformal group* $\mathrm{CO}(d, q, Q)$, consisting of those elements of $\mathrm{GL}(d, q)$ that transform Q to λQ for some $\lambda \in F$.

We define the following *standard bases* and corresponding *standard forms*, denoted $Q_d^\epsilon(q)$ and $F_d^\epsilon(q)$, where $\epsilon \in \{\circ, +, -\}$. We omit q when the context makes it clear. Let $m = \lfloor d/2 \rfloor$.

dq odd: $\{e_1, \ldots, e_m, z, f_m, \ldots, f_1\}$ such that $F_d^\circ = J_d$ and Q_d° is antidiagonal, with m entries 1, then one entry $1/2$ and then m entries 0.

d even and $\epsilon = +$: $\{e_1, \ldots, e_m, f_m, \ldots, f_1\}$, with $F_d^+ = J_d$ and Q_d^+ antidiagonal, with m entries 1 and then m entries 0.

d even and $\epsilon = -$: $\{e_1, \ldots, e_{m-1}, x, y, f_{m-1}, \ldots, f_1\}$, with

$$Q_2^- = (Q_d^-)_{\langle x,y\rangle} = \begin{pmatrix} 1 & 1 \\ 0 & \gamma \end{pmatrix} \quad F_2^- = (F_d^-)_{\langle x,y\rangle} = \begin{pmatrix} 2 & 1 \\ 1 & 2\gamma \end{pmatrix}.$$

If q is even, then γ is chosen such that $x^2 + x + \gamma$ is irreducible; a canonical γ may be constructed in $O(\log q)$ field operations [16]. If q is odd then $\gamma = \xi^{q+1}(\xi + \xi^q)^{-2}$ (recall that ξ is the primitive element of $\mathrm{GF}(q^2)$) [16]. The matrix Q_d^- is a block matrix with top right entry J_{m-1}, middle 2×2 block Q_2^- and all other entries 0. The matrix F_d^- is a block matrix with top right and bottom left entries J_{m-1}, middle 2×2 block F_2^- and all other entries 0.

When a group preserves one of our standard forms, then we will omit the form from the description, writing for instance $\mathrm{GO}^\epsilon(d, q)$ instead of $\mathrm{GO}(d, q, Q_d^\epsilon(q))$.

A second set of symmetric bilinear forms that we will use in odd characteristic are the identity matrix, denoted F_d^{S}, and the form $(\zeta) \oplus I_{d-1}$, denoted F_d^{N}: see Definition 3.2 for an interpretation of the symbols S and N.

3.2. *The discriminant and spinor norm*

In this subsection we define two important maps associated with the orthogonal groups and recall some of their properties.

DEFINITION 3.2. For q odd, the *discriminant* $D(Q)$ or $D(F)$ of a quadratic form or its polarisation is *square*, written $D(Q) = \mathsf{S}$, if $\det(M_{F_Q})$ is a square in $\mathrm{GF}(q)$. Otherwise, it is *non-square*, written $D(Q) = \mathsf{N}$.

The structure of the geometric maximal subgroups of $\mathrm{P}\Omega^\epsilon(d, q)$ is presented in detail in [14]. It is straightforward to deduce the structure of their inverse images in $\Omega^\epsilon(d, q)$ using the following lemma.

LEMMA 3.3 [14, Propositions 2.5.10, 2.5.13].

(1) *A form of plus type has square discriminant if and only if $d(q-1)/4$ is even. A form of minus type has square discriminant if and only if $d(q-1)/4$ is odd.*

(2) *The scalar subgroup of $\mathrm{GO}^\epsilon(d, q)$ is $\langle \pm I \rangle$. If d is even, then $-I \in \Omega^\epsilon(d, q)$ if and only if $D(F_d^\epsilon(q)) = \mathsf{S}$.*

It is well known (see for instance [14, Proposition 2.5.6]) that if $(d, q, \epsilon) \neq (4, 2, +)$, then every element of $\mathrm{GO}^\epsilon(d, q)$ is a product of reflections. The following definition can be extended to $\mathrm{GO}^+(4, 2)$, but we omit the details.

DEFINITION 3.4. Let r be a reflection in a non-singular vector v and let $\alpha = F(v, v)$. For q odd, let $\mathrm{sp}(r) = 1$ if $\alpha \in \mathrm{GF}(q)^{\times 2}$ and $\mathrm{sp}(r) = -1$ otherwise. For q even, let $\mathrm{sp}(r) = -1$.

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

Let $\mathrm{sp}(r_1 \ldots r_k) = \Pi_{i=1}^{k} \mathrm{sp}(r_i)$. Then $\mathrm{sp} : \mathrm{GO}^{\epsilon}(d, q) \rightarrow \{\pm 1\}^{\times}$ is a homomorphism called the *spinor norm*. Furthermore, the kernel of the restriction of sp to $\mathrm{SO}^{\epsilon}(d, q)$ is $\Omega^{\epsilon}(d, q)$.

LEMMA 3.5.

(1) *Let q be odd and let $g \in \mathrm{GO}^{\epsilon}(d, q, F)$. Define $A(g) = \{v \in V : \text{there exists an } n \in \mathbb{N} \text{ such that } v(I_d + g)^n = 0\}$, $B(g) = \bigcap_{n=1}^{\infty} V(I_d + g)^n$, and $\alpha(g) = \det(F_{A(g)}) \det(\frac{1}{2}(I_d + g)_{B(g)})$. Then the spinor norm of g is 1 if and only if $\alpha(g) \in \mathrm{GF}(q)^{\times 2}$.*

(2) *For q even, the spinor norm of $g \in \mathrm{GO}(d, q, Q)$ is 1 if and only if the rank of $(g + I_d)$ is even.*

(3) *Suppose $g \in \mathrm{GO}^{+}(d, q, Q)$ stabilises W_1 and W_2, two maximal totally singular subspaces with trivial intersection. Then $g \in \Omega^{+}(d, q, Q)$ if and only if $\det_{W_1}(g)$ is square.*

Proof. For (1), see [**21**], for (2) see [**6**] and for (3) see [**14**, Lemma 4.1.9]. □

PROPOSITION 3.6 [**16**]. *Let Q and $g \in \mathrm{GO}(d, q, Q)$ be given. Then $\mathrm{sp}(g)$ can be found in $O(d^{\omega})$ if q is even and $O(d^{\omega} + \log q)$ if q is odd.*

3.3. *Canonical isometries*

Let $G = \langle g_1, \ldots, g_s \rangle \leqslant \mathrm{GO}(d, q, Q)$. By *converting* G to preserve the form Q', we mean producing a set of s canonical matrices that generate a $\mathrm{GL}(d, q)$-conjugate of G that preserves Q'. Similarly, by *converting* Q to Q', we mean producing a matrix A such that if G preserves Q, then G^A preserves Q'. Recall the definitions in § 3.1 of Q_d^{ϵ}, F_d^{ϵ} and F_d^{k}, where $\epsilon \in \{\circ, +, -\}$ and $k \in \{\mathsf{N}, \mathsf{S}\}$.

The following result is proved in [**16**] for q odd and in [**10**, Proposition 3.4] for q even.

PROPOSITION 3.7. *The group $G = \langle g_1, \ldots, g_s \rangle \leqslant \mathrm{GO}(d, q, Q)$ can be converted to preserve Q_d^{ϵ} in $O(sd^{\omega} + d \log q)$ field operations if q is odd and $O(sd^3 + d \log q)$ field operations if q is even.*

In most situations that arise in this paper, the form Q has a very restricted structure. The following proposition enables us to perform the conversion more efficiently in these cases.

PROPOSITION 3.8. *Let $Q = (q_{ij})$ with $G = \langle g_1, \ldots, g_s \rangle \leqslant \mathrm{GO}(d, q, Q)$ and let $F = Q + Q^{\mathrm{T}} = (f_{ij})$. Assume that, after a permutation of the basis vectors, the space V on which G acts decomposes as an orthogonal direct sum of two-dimensional spaces W_i $(1 \leqslant i \leqslant t)$ and a $(d - 2t)$-dimensional space W, where the matrices Q_{W_i}, representing the restrictions of Q to the two-dimensional spaces, are all the same.*

(1) *Suppose that the matrices F' and Q' define a form isometric to and satisfying the same hypotheses as F and Q, and that $Q_W = (Q')_{W'}$. Then G can be converted to preserve Q' in $O(std + \log q)$ field operations.*

(2) *Let q be even and suppose that F_W and Q_W both have at most one non-zero entry in each row and in each column. Then G can be converted to preserve Q_d^{ϵ} in $O(sd^2 + \log q)$ field operations.*

(3) *Let q be odd and suppose that F_W has at most one non-zero entry in each row and in each column, and that at most c values from $\mathrm{GF}(q)$ occur in Q. Then G can be converted to preserve F_d^{k} or F_d^{ϵ} in $O(sd^2 + c \log q)$ field operations.*

Proof. In all cases, we begin by reordering the basis of V to exhibit the direct sum decomposition $V = W_1 \oplus \ldots \oplus W_t \oplus W$, and in Part 1 we do the same for the second form,

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

to give $V = W_1' \oplus \ldots \oplus W_t' \oplus W'$. This involves up to $4t$ row and column swaps, and is an $O(std)$ operation.

(1) Since Q is non-degenerate, Q_{W_i} is non-degenerate for each i. To effect the form conversion, if the types of Q_{W_1} and $Q'_{W_1'}$ are the same, then simply convert one to the other, whereas, if they are different, then convert the 4×4 matrix representing the action of Q on $W_1 \oplus W_2$ to the corresponding matrix for Q'. In either case, this can be done in $O(\log q)$ field operations by [**10**, 3.3, 3.4]. (The $\log q$ in the complexity is for finding square roots.) Since the restrictions of Q to the W_i are all the same, and similarly for Q', only one 2×2 or 4×4 form transformation matrix need be calculated, so the conversion requires $O(\log q + st)$ field operations, and the result follows.

(2) Since Q is non-degenerate and q is even, the single non-zero entry hypothesis implies that the diagonal entries of Q_W are all zero. If $q_{2t+1,d} \neq 0$, then replace v_d by $q_{2t+1,d}^{-1} v_d$ to get $q_{2t+1,d} = 1$. Otherwise, if $q_{2t+1,i}$ is the non-zero entry in row $2t+1$, where $i > 2t+1$, then interchange v_d and $q_{2t+1,i}^{-1} v_i$ to produce a form $R = (r_{ij})$, where $r_{2t+1,d} = 1$ and R_W and $(R + R^{\mathrm{T}})_W$ still have at most one non-zero entry in each row and each column. Iterating, convert Q_W to the standard form matrix of plus type in $O(sd^2)$ field operations. The 2-spaces are converted as in Part 1 (except that, for forms of minus type, convert to $t-1$ 2×2 blocks of plus type and one of minus type), and a final basis permutation completes the conversion to Q_d^ϵ.

(3) We first describe how to diagonalise F. Convert all of the 2×2 blocks to diagonal, as in Part 1, in $O(std + \log q)$ field operations. Note that at most two distinct values will be placed on the diagonal during this process, since all 2×2 blocks are identical. If $f_{2t+1,2t+1} \neq 0$, there is nothing to do to row $2t+1$. Otherwise, there exist $i > 2t+1$ and $\alpha := f_{2t+1,i} = f_{i,2t+1} \neq 0$. Replace v_{2t+1} by $v_{2t+1} + v_i$ and v_i by $v_{2t+1} - v_i$ to diagonalise rows $2t+1$ and i. Apply this diagonalisation process to rows $2t+1$ to d in $O(sd^2)$ field operations. Since each such conversion replaces each non-zero entry of F by two non-zero entries, there are still $O(c)$ distinct values in the new form matrix $F' = (f'_{ij})$ after the conversion.

Now we convert the diagonal form F' to F_d^k with $k \in \{\mathsf{S}, \mathsf{N}\}$. If $f'_{ii} = \lambda^2$, replace v_i by $\lambda^{-1} v_i$ (using canonical roots). If f'_{ii} is non-square, find a second non-square entry f'_{jj}, and convert f'_{jj} to equal f'_{ii}, similarly to the square case. Let $\nu = 2\xi^{(q+1)/2}(\xi - \xi^q)^{-1}$. Then $1 + \nu^2$ is non-square in $\mathrm{GF}(q)$. Replace v_i by $v_i + \nu v_j$ and v_j by $\nu v_i - v_j$ in $O(sd + \log q)$. Now both diagonal form entries are square, and can be converted as before to 1. If the form is now F_d^{S}, then stop. Otherwise, a single non-square entry remains, so interchange the corresponding vector with v_1 and scale it to produce F_d^{N}. A total of $O(c)$ square roots need be found, so the whole process requires $O(sd^2 + c \log q)$ field operations.

By using the method just described, we can convert F_d^ϵ to F_d^k with $k \in \{\mathsf{S}, \mathsf{N}\}$ using at most $2d$ steps, each of which involves only a 1×1 or 2×2 basis change matrix. These can all be inverted in $O(1)$, so we can also perform the reverse conversions from F_d^k to F_d^ϵ in $O(sd^2 + \log q)$ field operations. □

3.4. *Generation of classical groups*

We will consistently use the following symbols for canonical generators of the orthogonal groups preserving our standard form. The two generators of $\Omega^\epsilon(d, q)$ are $A_d^\epsilon(q)$ and $B_d^\epsilon(q)$, where $B_d^\epsilon(q) = I_2$ if $d = 2$. Our canonical elements of $\mathrm{SO}^\epsilon(d, q) \setminus \Omega^\epsilon(d, q)$ and of $\mathrm{GO}^\epsilon(d, q) \setminus \mathrm{SO}^\epsilon(d, q)$ are denoted by $S_d^\epsilon(q)$ and $G_d^\epsilon(q)$, where $G_d^\epsilon(q)$ is undefined if q is even, and $\mathrm{sp}(G_d^\epsilon(q)) = 1$ if q is odd. We denote by $D_d^\epsilon(q)$ a generator for $\mathrm{CO}^\epsilon(d, q)$ modulo $\mathrm{GO}^\epsilon(d, q)$. When q is clear, it will be omitted.

Recall that $m = \lfloor d/2 \rfloor$, and that ζ and ξ are primitive multiplicative elements of $\mathrm{GF}(q)$ and $\mathrm{GF}(q^2)$, respectively.

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

THEOREM 3.9. *Canonical matrices $A_d^\epsilon(q)$, $B_d^\epsilon(q)$, $S_d^\epsilon(q)$, $G_d^\epsilon(q)$ and $D_d^\epsilon(q)$ can be constructed in $O(d^2 + \log q)$ field operations. In each case, they have $O(d)$ non-zero entries, and the number of values in* $\mathrm{GF}(q)$ *taken by their entries is bounded above by a constant that does not depend on d or q.*

Proof. We first consider A_d^ϵ and B_d^ϵ. Our strategy is to use matrices $\overline{A_d^\epsilon}$ and $\overline{B_d^\epsilon}$ as given in [**18**], which generate a group conjugate to $\Omega^\epsilon(d,q)$ that preserves a form which we will denote by $\overline{Q_d^\epsilon}$. There are two main modifications that we must make to the work of [**18**]. Firstly, we need to convert $\overline{Q_d^\epsilon}$ to Q_d^ϵ: we discuss how to do this on a case-by-case basis. Secondly, $\overline{A_d^\epsilon}$ and $\overline{B_d^\epsilon}$ are sometimes defined in [**18**] as a product of matrices: to get complexity $O(d^2 + \log q)$ we must show that in each case this product can be computed in $O(d^2)$ field operations and that each matrix entry can be constructed in $O(\log q)$ field operations.

Explicit matrices $\overline{A_d^\epsilon}$ and $\overline{B_d^\epsilon}$ are given in [**18**] for (ϵ, d, q) equal to: $(\circ, 3, q)$, $(\circ, d, 3)$, $(+, 2, q)$, $(+, 4, q)$, $(+, \text{even } m > 2, 2)$ and $(+, \text{odd } m > 2, q \leqslant 3)$. In each case the result holds, since Q_d^+ is equal to $\overline{Q_d^+}$ and, except for $\overline{Q_d^\circ}(z) = 1$, the form Q_d° is equal to $\overline{Q_d^\circ}$.

If $d > 3$ and $q > 3$, then $\overline{A_d^\circ}$ is diagonal with entries in $\{1, \zeta^{\pm 1}\}$ and $\overline{B_d^\circ}$ has all entries in the subset $\{n \mod p \mid n \in \mathbb{Z},\ -6 \leqslant n \leqslant 6\}$ of $\mathrm{GF}(p)$ and, apart from a central 3×3 block, has one non-zero entry in each row, equal to ± 1. Both $\overline{A_d^\circ}$ and $\overline{B_d^\circ}$ can be computed in $O(d^2)$ field operations. The form $\overline{Q_d^\circ}$ is converted to Q_d° in $O(d + \log q)$ field operations by Proposition 3.8(3). There is at most one non-zero entry in each row of $\overline{A_d^\circ}$ and $\overline{B_d^\circ}$ outside their central 3×3 blocks, so the result holds.

Since the form Q_d^+ is equal to $\overline{Q_d^+}$, the matrices satisfy $\overline{A_d^+} = A_d^+$ and $\overline{B_d^+} = B_d^+$. If $m > 2$ is even and $q > 2$, or $m > 2$ is odd and $q > 3$, then A_d^+ is diagonal with entries in $\{1, \zeta^{\pm 1}\}$. In the former case, let $X = I + E_{m-2,m-1} - E_{m+1,m-1} + E_{m+2,m} - E_{m+2,m+3}$, and in the latter case let $X = I - E_{m-1,m+1} + E_{m,m+2}$. Then B_d^+ is the product of X with a matrix with $O(d)$ non-zero entries, all equal to ± 1; hence, A_d^+ and B_d^+ can be constructed in $O(d^2)$ field operations.

The form Q_d^- is the same as $\overline{Q_d^-}$, except on $\langle x, y \rangle$. Here $\overline{A_d^-} = I_{m-2} \oplus X \oplus I_{m-2}$, where X is a 4×4 matrix whose entries can be constructed, using Lemma 2.1(1), in $O(\log q)$ field operations. Finally, $\overline{B_d^-}$ has a non-trivial central 4×4 block, three non-zero entries in $\{b_{i1} : m - 1 \leqslant i \leqslant m + 2\}$, with $b_{md} \neq 0$, and exactly one non-zero entry, equal to ± 1, in every other row and column. Convert $\overline{A_d^-}$ and $\overline{B_d^-}$ to preserve Q_d^- in $O(d + \log q)$ field operations by Proposition 3.8(1).

This completes the cases for A_d^ϵ and B_d^ϵ.

If $(d, \epsilon) = (2, -)$ and q is odd, let R_0 and R_1 be the reflections in x and y, respectively, if $2 \in \mathrm{GF}(q)^{\times 2}$, and y and x, respectively, otherwise. Otherwise, if q is odd, let R_0 and R_1 be the reflections in $e_1 + (1/2)f_1$ and $e_1 + (\zeta/2)f_1$. Then let $S_d^\epsilon = R_0 R_1$ and $G_d^\epsilon = R_0$. If q is even, let S_d^ϵ be the reflection in $e_1 + f_1$ or in x (in the $(2, -)$ case).

By [**16**], we can let $D_d^\circ = \zeta^2 I_m \oplus (\zeta) \oplus I_m$ and $D_d^+ = \zeta I_m \oplus I_m$. We let $D_2^- = \mathrm{AntiDiag}[\xi + \xi^q, \zeta(\xi + \xi^q)^{-1}]$ and, for $d > 2$, we let $D_d^- = \zeta I_{m-1} \oplus D_2^- \oplus I_{m-1}$. □

If q is odd, then ${}^*X_d^\epsilon(q)$, where $X \in \{A, B, S, G, D\}$, denotes a conjugate of $X_d^\epsilon(q)$ that preserves $F_d^{D(F_d^\epsilon(q))}$. The following is a consequence of Theorem 3.9 and Proposition 3.8(3).

COROLLARY 3.10. *The matrices ${}^*X_d^\epsilon(q)$, where $X \in \{A, B, S, G, D\}$, may all be constructed in $O(d^2 + \log q)$ field operations.*

Note that G_d^ϵ and ${}^*G_d^\epsilon$ have order two and hence are inverted in $O(1)$. Furthermore, the inverses of S_d^ϵ and ${}^*S_d^\epsilon$ can be constructed in $O(d^2 + \log q)$ field operations by multiplying the reflections R_0 and R_1 in a different order.

We briefly record some information about standard generators and forms for other classical groups. See [**17**] for more information.

THEOREM 3.11. *Canonical generators* L_1 *and* $L_2 = \mathrm{Diag}[\zeta, 1, \ldots, 1]$ *of* $\mathrm{GL}(d, q)$ *can be constructed in* $O(d^2)$ *field operations, with* $\det(L_1) = 1$*. A canonical matrix* L_3 *such that* $\mathrm{SL}(d, q) = \langle L_1, L_3\rangle$ *can be constructed in* $O(d^2)$ *operations. Canonical generators of* $\mathrm{Sp}(d, q)$ *can be constructed in* $O(d^2)$ *field operations, preserving the symplectic form with matrix*

$$\mathrm{AntiDiag}[1, \ldots, 1, -1, \ldots, -1].$$

Canonical generators of $\mathrm{GU}(d, q)$ *and* $\mathrm{SU}(d, q)$ *can be constructed in* $O(d^2 + \log q)$ *field operations, preserving the unitary form with matrix* J_d*. In the linear and symplectic cases, all entries lie in* $S := \{0, \pm 1, \pm\zeta^{\pm 1}\}$*, whilst in the unitary case they lie in*

$$S \cup \{\xi^{\pm q}, \xi^{q-1}, \xi^{\pm(q+1)/2}, \pm(1 + \xi^{q-1})^{\pm 1}\}.$$

If q is odd, then $\mathrm{GL}(d, q)$ has a unique subgroup of index two, denoted by $\frac{1}{2}\mathrm{GL}(d, q)$. For $q \neq 3$, the group $\frac{1}{2}\mathrm{GL}(d, q)$ is generated by L_1 and L_2^2, which can be computed in $O(d^2)$ field operations since L_2 is diagonal. If $q = 3$ then $\frac{1}{2}\mathrm{GL}(d, 3) = \mathrm{SL}(d, 3)$. Note that L_1 and L_2 each have $O(d)$ non-zero entries, and so may be inverted in $O(d^2)$ field operations.

4. *Reducible groups*

Sections 4 to 10 all have a similar structure. They each concern the groups that arise in Theorem 1.1 in one of the seven non-empty geometric Aschbacher classes, and they start with a proposition stating the complexity of their construction. In each of these propositions, by 'the subgroups of G that arise' we mean the pre-images in $\Omega^\epsilon(d, q)$ of the intersections of these subgroups with $\mathrm{P}\Omega^\epsilon(d, q)$.

After stating the proposition, we describe the types of group that arise in the relevant Aschbacher class, and then present generating matrices for canonical representatives of each such group. We assume throughout that $d \geqslant 7$ and that q is odd if d is odd, since if either of these fails then $\mathrm{P}\Omega^\epsilon(d, q)$ is either not simple or is isomorphic to another classical group. In each of these cases, the results of [**10**] are therefore applicable.

When constructing generating matrices of some maximal subgroup H, we usually will start by constructing some large subgroup $K = \langle A_1, \ldots, A_n\rangle$ of H. By *adjoining* a generator X to K we mean creating the group $K_1 = \langle A_1, \ldots, A_n, X\rangle$.

In this section we shall prove the following proposition.

PROPOSITION 4.1. *Let* $\mathrm{P}\Omega^\epsilon(d, q) \trianglelefteq G \leqslant \mathrm{PC\Gamma O}^\epsilon(d, q)$*. Canonical representatives of the reducible subgroups of* G *that arise in Theorem* 1.1 *can be constructed in* $O(d^3 + d \log q)$ *field operations.*

The groups to be constructed are described in Table 1 (see [**14**, Table 4.1.A]). Recall that $m = \lfloor d/2\rfloor$. In the table, a group is of type P_k if it is the stabiliser of a totally singular subspace U of dimension k. A group is of type $\mathrm{GO}^{\epsilon_1}(k, q) \perp \mathrm{GO}^{\epsilon_2}(d - k, q)$ if it is the stabiliser of a non-degenerate subspace U of dimension k and type ϵ_1. Such groups automatically also stabilise a subspace W of dimension $d - k$ and type ϵ_2, such that $F_d^\epsilon(u, w) = 0$ for all $u \in U, w \in W$, and $U \cap W = \{0\}$. A group is of type $\mathrm{Sp}(d - 2, q)$ if it is the stabiliser of a non-singular vector v (recall that v is non-singular if $Q_d^\epsilon(v) \neq 0$).

LEMMA 4.2. *A canonical subgroup* H *of* $\Omega^\epsilon(d, q)$ *of type* P_k*, where* k *is as in Table* 1*, can be constructed in* $O(d^2 + \log q)$ *field operations.*

Proof. Let H be the stabiliser of $\langle e_1, \ldots, e_k\rangle$ in $\Omega^\epsilon(d, q)$. We first generate a complement to the p-core of H. Let L_1 and L_2 be the standard generators of $\mathrm{GL}(k, q)$ as defined in Theorem 3.11.

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

By [14, Proposition 4.1.20], if q is even, then d is even and

$$H \cong [q^{kd-k(3k+1)/2}]{:}(\mathrm{GL}(k,q) \times \Omega^{\epsilon}(d-2k,q)).$$

For $i=1,2$, let $H_i = L_i \oplus I_{d-2k} \oplus J_k L_i^{-\mathrm{T}} J_k$ and, if $k \neq m$, let $H_3 = I_k \oplus A^{\epsilon}_{d-2k} \oplus I_k$ and $H_4 = I_k \oplus B^{\epsilon}_{d-2k} \oplus I_k$. A short calculation shows that H_1 and H_2 preserve Q^{ϵ}_d, and they lie in $\Omega^{\epsilon}(d,q)$ because $H_1 + I_d$ and $H_2 + I_d$ have even rank. It is clear that H_3 and H_4 lie in H.

By [14, Proposition 4.1.20], if q is odd and $k=m$, then

$$H \cong [q^{k(k+t)/2}]{:}\tfrac{1}{2}\mathrm{GL}(k,q),$$

where $t=-1$ if d is even and $+1$ otherwise. We construct the subgroup $\frac{1}{2}\mathrm{GL}(k,q)$ of H. Let L_1 and L_2 generate $\frac{1}{2}\mathrm{GL}(k,q)$ in its natural representation and, for $i=1,2$, let $H_i = L_i \oplus I_1 \oplus J_k L_i^{-\mathrm{T}} J_k$ if d is odd, and $H_i = L_i \oplus J_k L_i^{-\mathrm{T}} J_k$ otherwise. Since in this representation $\mathrm{GL}(k,q) \leqslant \mathrm{SO}^{\epsilon}(d,q)$, its unique subgroup $\langle H_1, H_2\rangle$ of index 2 is contained in $\Omega^{\epsilon}(d,q)$.

Otherwise,

$$H \cong [q^{kd-k(3k+1)/2}]{:}(\tfrac{1}{2}\mathrm{GL}(k,q) \times \Omega^{\epsilon}(d-2k,q)).2.$$

First construct a subgroup of H that projects onto $\mathrm{GL}(k,q)$. Let L_1, L_2 be the standard generators of $\mathrm{GL}(k,q)$. Define $H_1 := L_1 \oplus I_{d-2k} \oplus J_k L_1^{-\mathrm{T}} J_k$ and note that $H_1 \in \Omega^{\epsilon}(d,q)$, as $\mathrm{SO}^{\epsilon}(d,q)$ contains $\mathrm{GL}(k,q)$ acting on $\langle e_1, \ldots, e_k\rangle$. Define $H_2 := L_2 \oplus S^{\epsilon}_{d-2k} \oplus J_k L_2^{-\mathrm{T}} J_k$. We show that $H_2 \in \Omega^{\epsilon}(d,q)$ by calculating the spinor norm of $H_2^* = L_2 \oplus I_{d-2k} \oplus J_k L_2^{-\mathrm{T}} J_k$. To do this, note that if $q \neq 3$ then, in the notation of Lemma 3.5(1), $A(H_2^*) = \{0\}$ and $B(H_2^*) = \mathrm{GF}(q)^d$: so $\mathrm{sp}(H_2^*) = -1$ if and only if $\det(\frac{1}{2}(I_d + H_2^*))$ is non-square. Now,

$$\det(\tfrac{1}{2}(I_d + H_2^*)) = (4\zeta)^{-1}(1 + 2\zeta + \zeta^2),$$

so $\mathrm{sp}(H_2^*) = -1$. If $q=3$, then $A(H_2^*) = \langle e_1, f_1\rangle$ and $\det((F^{\epsilon}_d)_A) = -1$, which is non-square, while $\det(\frac{1}{2}(I_d + H_2^*)_{B(H_2^*)}) = 1$. Therefore, in both cases $\mathrm{sp}(H_2^*) = 1$, so $\mathrm{sp}(H_2) = 1$, and hence $H_2 \in \Omega^{\epsilon}(d,q)$. Then $\langle H_1, H_2\rangle$ projects onto $\mathrm{GL}(k,q)$. Define $H_3 = I_k \oplus A^{\epsilon}_{d-2k} \oplus I_k$ and $H_4 = I_k \oplus B^{\epsilon}_{d-2k} \oplus I_k$. It is clear that both H_3 and H_4 lie in $\Omega^{\epsilon}(d,q)$, so $\langle H_1, \ldots, H_4\rangle$ is a complement to the p-core of H.

In all cases, we now add $O_p(H)$. The Sylow p-subgroups of $\mathrm{GO}^{\epsilon}(d,q)$ lie in $\Omega^{\epsilon}(d,q)$, so, if a matrix M of p-power order fixes $Q^{\epsilon}_d(q)$, then $M \in \Omega^{\epsilon}(d,q)$. The p-elements are generated in two sets. The first set is acted on by both $\Omega^{\epsilon}(d-2k,q)$ and $\mathrm{SL}(k,q)$. Its elements have non-zero off-diagonal entries in the first k columns of rows $k+1, \ldots, d-k$, balanced by entries in columns $k+1, \ldots, d-k$ of rows $d-k+1, \ldots, d$. The second set is acted on only by $\mathrm{SL}(k,q)$, and contains matrices with non-zero off-diagonal entries in the first k columns of the last k rows.

If $k=1$, then $|O_p(H)| = q^{d-2}$, and the normal closure of $H_5 = I + E_{2,1} - E_{d,d-1}$ under $\langle H_3, H_4\rangle$ has order q^{d-2}, as required.

Next suppose that $1 < k < m-1$ for d even, or $1 < k < m$ for d odd. Generate $O_p(H)$ with $H_5 = I + E_{d-1,1} - E_{d,2}$ for the subgroup acted on by $\langle H_1, H_2\rangle$, and $H_6 = I + E_{k+1,1} - E_{d,d-k}$

Table 1. *Types of reducible group.*

ϵ	Type	Conditions
$\circ, +, -$	P_k	$1 \leqslant k \leqslant m$, $k < m$ if $\epsilon = -$
$\circ$	$\mathrm{GO}^{\circ}(k,q) \perp \mathrm{GO}^{\epsilon_1}(d-k,q)$	$1 \leqslant k < d$, k odd, $\epsilon_1 \in \{+,-\}$
$+$	$\mathrm{GO}^{\epsilon_1}(k,q) \perp \mathrm{GO}^{\epsilon_1}(d-k,q)$	$1 \leqslant k < m$, $\epsilon_1 \in \{\circ,+,-\}$, q odd if k odd
$-$	$\mathrm{GO}^{\epsilon_1}(k,q) \perp \mathrm{GO}^{-\epsilon_1}(d-k,q)$	$1 \leqslant k \leqslant m$, $\epsilon_1 \in \{\circ,+,-\}$, $(k,\epsilon_1) \neq (m,\circ)$, q odd if k odd
$+, -$	$\mathrm{Sp}(d-2,q)$	q even

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

for the subgroup acted on by $\langle H_1, \dots, H_4\rangle$. Since the action on each p-group is irreducible, $\langle H_5, H_6\rangle^H$ has order $q^{k(d-2k)} \cdot q^{k(k-1)/2} = q^{k(d-(3k+1)/2)}$, as required.

Next suppose that d is even and $k = m - 1 > 1$. If $\epsilon = +$, then generate $O_p(H)$ with $H_5 = I + E_{d-1,1} - E_{d,2}$, $H_6 = I + E_{k+1,1} - E_{d,d-k}$ and $H_7 = I + E_{k+2,1} - E_{d-k-1,1}$. Even though the action of $\Omega^+(2, q)$ is reducible, the order of $\langle H_6, H_7\rangle^H$ is q^{2k}, as required. For $\epsilon = -$, one may check that the matrix

$$H_6 = I + E_{k+1,1} + \gamma(1-4\gamma)^{-1}E_{d,1} + 2\gamma(1-4\gamma)^{-1}E_{d,k+1} - (1-4\gamma)^{-1}E_{d,k+2}$$

preserves Q_d^-. The p-core is generated as a normal subgroup by H_5 and H_6.

Finally, suppose that $k = m$. The normal closure P_1 of $H_5 = I + E_{d-1,1} - E_{d,2}$ under $\langle H_1, H_2\rangle$ has order $q^{k(k-1)/2}$, as before. If d is odd, then $|O_p(H)|/|P_1| = q^k$, otherwise $P_1 = O_p(H)$. For odd d, one may check that $H_6 = I + E_{k+1,1} - E_{d,d-k} - (1/2)E_{d,1}$ preserves Q_d^ϵ. The order of $P_2 = \langle H_6\rangle^{\langle H_1, H_2\rangle}$ is q^k and $P_1 \cap P_2 = \{1\}$, so we are done.

In each case H has $O(1)$ generators, which are calculated in $O(d^2 + \log q)$ field operations. □

LEMMA 4.3. *The stabiliser H in $\Omega^\epsilon(d, q)$ of a canonical non-degenerate k-space, as in Table 1, can be constructed in $O(d^2 + \log q)$ field operations.*

Proof. If $k = 1$ or q is even, then $H \cong (\Omega^{\epsilon_1}(k, q) \times \Omega^{\epsilon_2}(d-k, q)).2$, and otherwise $H \cong (\Omega^{\epsilon_1}(k, q) \times \Omega^{\epsilon_2}(d-k, q)).[4]$, by [**14**, Proposition 4.1.6].

If q is even, then k is even. Construct generators $H_1, \dots, H_4$ as block matrices in the obvious manner. Define $H_5 := S_k^{\epsilon_1} \oplus S_{d-k}^{\epsilon_2}$. The resulting group preserves $Q_{d_1}^{\epsilon_1} \oplus Q_{d_2}^{\epsilon_2}$, which, together with the matrix of its polar form, has at most one non-zero entry in each row and column apart from at most two blocks which form -2-spaces. So, it can be converted to preserve Q_d^ϵ in $O(d^2 + \log q)$ field operations by Proposition 3.8(2).

Now assume that q is odd, and let $F_1 = F_{d_1}^{\epsilon_1} \oplus F_{d_2}^{\epsilon_2}$. Construct block diagonal matrices $H_1, \dots, H_4$ for $\Omega^{\epsilon_1}(k, q) \times \Omega^{\epsilon_2}(d-k, q)$, as for q even. Now create the normalising elements, by first letting $H_5 = G_k^{\epsilon_1} \oplus G_{d-k}^{\epsilon_2}$. Since $G_k^{\epsilon_1}$ and $G_{d-k}^{\epsilon_2}$ have spinor norm 1 and determinant -1, the matrix $H_5 \in \Omega(d, q, F_1)$. If $k > 1$, let $H_6 = S_k^\epsilon \oplus S_{d-k}^\epsilon \in \Omega(d, q, F_1)$. Finally, convert F_1 to F_d^ϵ, in $O(d^2 + \log q)$ field operations, by Proposition 3.8(3), since F_1 has at most two blocks of dimension two and otherwise a single entry 1 in each row and column. □

LEMMA 4.4. *A canonical subgroup H of $\Omega^\epsilon(d, q)$ of type* $\mathrm{Sp}(d-2, q)$, *as in Table 1, can be constructed in $O(d^\omega + d\log q)$ field operations.*

Proof. By [**14**, Proposition 4.1.7], $H \cong \mathrm{Sp}(d-2, q)$. Recall that q is even. Let $w = v_1 + v_d$ and let $W = \langle w\rangle$ be the space to stabilise, where $Q_d^\epsilon(w) = 1$. We generate a group isomorphic to $\mathrm{Sp}(d-2, q)$ acting on $U := \langle w, v_2, \dots, v_{d-1}\rangle = W^\perp$ that preserves the restriction of Q_d^ϵ to U.

The group $\mathrm{Sp}(d-2, q)$ acts naturally on U/W, preserving a symplectic form $F_1 = J_{d-2} = F_{d-2}^+$ given by $F_1(a + W, b + W) = F_d^\epsilon(a, b)$. The isomorphism from $\mathrm{Sp}(d-2, q)$ to H is given by mapping $g \in \mathrm{Sp}(d-2, q)$ to the unique $h \in \Omega^\epsilon(d, q)$ that fixes w and, for $2 \leqslant j \leqslant d-1$, sends v_j to the only w_j in $(v_j + W)g$ with $Q_d^\epsilon(v_j) = Q_d^\epsilon(w_j)$.

Let L_1 and L_2 be the standard generators of $\mathrm{Sp}(d-2, q)$ from Theorem 3.11. For $i = 1, 2$, let $H_i^* = [0] \oplus L_i \oplus [0]$ and let $N_i = Q_d^\epsilon + H_i^* Q_d^\epsilon (H_i^*)^{\mathrm{T}}$, calculated in $O(d^\omega)$. For $2 \leqslant j \leqslant d-1$, let w_j (which will be the image of v_j) be the sum of row j of H_i^* and $\alpha_j^{1/2} w$, where $\alpha_j^{1/2}$ is the canonical square root of the (j, j)th entry of N_i. Then $w_j \in v_j H_i^* + W$ and $Q_d^\epsilon(w_j) = Q_d^\epsilon(v_j H_i^*) + (Q_d^\epsilon(v_j) + Q_d^\epsilon(v_j H_i^*))Q_d^\epsilon(w) = Q_d^\epsilon(v_j)$, since $F_d^\epsilon(v_j H_i^*, w) = 0$ for all i and j. Furthermore, a short calculation shows that $F_d^\epsilon(w_i, w_j) = F_d^\epsilon(v_i, v_j)$, as required. The vectors $w_2, \dots, w_{d-1}$ are constructed in $O(d^\omega + d\log q)$ field operations.

Next use linear algebra to find a vector $z \notin U$ that is orthogonal to $w_2, \ldots, w_{d-1}$ and such that $F_d^\epsilon(w, z) = 1$, in $O(d^\omega)$ field operations. Let α be a root of $x^2 + x + Q_d^\epsilon(z)$. Then, setting $w_d = z + \alpha w$, one may check that $Q_d^\epsilon(w_d) = Q_d^\epsilon(v_d) = 0$, $F_d^\epsilon(w, w_d) = 1$ and $F_d^\epsilon(w_j, w_d) = F_d^\epsilon(v_j, v_d) = 0$ for $1 \leqslant j \leqslant d-1$. Note that the existence of α is guaranteed by the isomorphism between H and $\mathrm{Sp}(d-2, q)$. Let H_i have $w + w_d, w_2, \ldots, w_{d-1}, w_d$ as rows. Then H_i preserves Q_d^ϵ and fixes $w = v_1 + v_d$. Calculate the spinor norm of H_i in $O(d^\omega + \log q)$ field operations by Proposition 3.6, and replace H_i by its product with the reflection in w_2 if $H_i \notin \Omega^\epsilon(d, q)$. Then $H = \langle H_1, H_2 \rangle$, as required. □

Proposition 4.1 now follows from the fact that there are $O(d)$ classes of groups of type P_k and of type $\mathrm{GO}^{\epsilon_1}(k, q) \perp \mathrm{GO}^{\epsilon_2}(d-k, q)$, and $O(1)$ groups of type $\mathrm{Sp}(d-2, q)$.

5. *Imprimitive groups*

A group is *imprimitive* if it stabilises a direct sum decomposition of V into $t > 1$ subspaces of dimension m:

$$V = V_1 \oplus \ldots \oplus V_t.$$

In this section we shall prove the following proposition.

PROPOSITION 5.1. *Let $\mathrm{P}\Omega^\epsilon(d, q) \trianglelefteq G \leqslant \mathrm{PC\Gamma O}^\epsilon(d, q)$. Canonical representatives of the imprimitive subgroups of G that arise in Theorem 1.1 can be constructed in $O(d^{2+\varepsilon} + d^{1+\varepsilon} \log q)$ field operations, for every real $\varepsilon > 0$.*

The types of imprimitive group are in Table 2, taken from [**14**, Table 4.2.A]. Here the symbol $\wr$ denotes a wreath product, so that

$$\mathrm{GO}^{\epsilon_1}(m, q) \wr \mathrm{Sym}(t) \cong (\mathrm{GO}^{\epsilon_1}(m, q) \times \ldots \times \mathrm{GO}^{\epsilon_1}(m, q)){:}\mathrm{Sym}(t),$$

with the $\mathrm{Sym}(t)$ permuting the t copies of $\mathrm{GO}^{\epsilon_1}(m, q)$.

LEMMA 5.2. *A set of canonical representatives of the subgroups of $\Omega^\epsilon(d, q)$ of type $\mathrm{GO}^{\epsilon_1}(m, q) \wr \mathrm{Sym}(t)$ with $m > 1$, satisfying the conditions of Table 2, can be constructed in $O(d^{2+\varepsilon} + d^\varepsilon \log q)$ field operations, for every $\varepsilon > 0$.*

Proof. There are $O(d^\varepsilon)$ such groups, by Lemma 2.2(2). For fixed m and ϵ_1, we construct the corresponding group in $O(d^2 + \log q)$ field operations.

If q is even, then

$$H \cong \Omega^{\epsilon_1}(m, q)^t.2^{t-1}.\mathrm{Sym}(t),$$

TABLE 2. *Types of imprimitive group.*

Case	Type	Description of V_i	Conditions
$\circ, +, -$	$\mathrm{GO}^{\epsilon_1}(m, q) \wr \mathrm{Sym}(t)$	Non-degenerate, $m > 1$	m even $\Rightarrow$ $\epsilon = \epsilon_1^t$; m odd and t even $\Rightarrow D(F_d^\epsilon) = \mathsf{S}$
$\circ, +, -$	$\mathrm{GO}(1, q) \wr \mathrm{Sym}(d)$	Non-degenerate	$q = p \geqslant 3$; $D(F_d^\epsilon) = \mathsf{S}$ if d even
$+$	$\mathrm{GL}(d/2, q).2$	Totally singular	
$+, -$	$\mathrm{GO}^\circ(d/2, q)^2$	Non-degenerate, non-isometric	$qd/2$ odd, $D(F_d^\epsilon) = \mathsf{N}$

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

by [**14**, Proposition 4.2.11]. Construct $H_1 := \Omega^{\epsilon_1}(m, q) \wr \mathrm{Sym}(t)$, preserving the quadratic form $Q_1 := Q_m^{\epsilon_1} \oplus \ldots \oplus Q_m^{\epsilon_1}$, in $O(d^2 + \log q)$ field operations. Since q is even, m is even, so the rank of all permutation matrices is even and hence they all have spinor norm 1 by Lemma 3.5(2). Next, adjoin $S_m^{\epsilon_1} \oplus (S_m^{\epsilon_1})^{-1} \oplus I_m \oplus \ldots \oplus I_m$, a product of an even number of reflections, in $O(d^2)$ field operations since $|S_m^{\epsilon_1}| = 2$. Now, Q_1 contains at most t identical blocks of size two, and otherwise both Q_1 and F_{Q_1} have at most one non-zero entry in each row and column, so Q_1 can be converted to Q_d^{ϵ} in $O(d^2 + \log q)$ field operations by Proposition 3.8(2).

If q is odd, then a short calculation based on [**14**, Propositions 4.2.11, 4.2.14] shows that in all cases

$$H \cong \Omega^{\epsilon_1}(m, q)^t.2^{2t-2}.\mathrm{Sym}(t).$$

Let $k = D(F_m^{\epsilon_1})$ and construct $H_1 := \Omega^{\epsilon_1}(m, q, F_m^k) \wr \mathrm{Alt}(t)$ in $O(d^2 + \log q)$ field operations, preserving a diagonal bilinear form $F_1 := F_m^k \oplus \ldots \oplus F_m^k$. Since $\mathrm{Alt}(t)$ contains only even permutations, $\mathrm{sp}(h) = 1$ for all $h \in H_1$. Next, adjoin $S := {}^*S_m^{\epsilon_1} \oplus ({}^*S_m^{\epsilon_1})^{-1} \oplus I_m \oplus \ldots \oplus I_m$ and $G := {}^*G_m^{\epsilon_1} \oplus ({}^*G_m^{\epsilon_1})^{-1} \oplus I_m \oplus \ldots \oplus I_m$, both of which have determinant and spinor norm 1. Then

$$H_2 := \langle H_1, S, G\rangle \cong \Omega^{\epsilon_1}(m, q)^t.2^{2t-2}.\mathrm{Alt}(t).$$

If m is even, then the permutation matrix P corresponding to $(1, 2)$ has determinant 1. If $D(F_m^{\epsilon_1}(q)) = \mathsf{S}$, then P is a product of m reflections in vectors of norm 2. Thus, $\mathrm{sp}(P) = 1$, so adjoin P to H_2. If $D(F_m^{\epsilon_1}(q)) = \mathsf{N}$, then $\mathrm{sp}(P) = -1$, so adjoin $({}^*S_m^{\epsilon_1} \oplus I_m \oplus \ldots \oplus I_m)P$ to H_2.

If m is odd, then $\det(P) = -1$, so let $P_1 := ({}^*G_m^{\epsilon_1} \oplus \ldots \oplus I_m \oplus I_m)P$. Then $\det(P_1) = 1$. If 2 is a square (so $q \equiv \pm 1 \bmod 8$), then $\mathrm{sp}(P_1) = 1$, so adjoin P_1. If 2 is non-square, then adjoin $({}^*S_m^{\epsilon_1} \oplus I_m \oplus \ldots \oplus I_m)P_1$.

Finally, convert F_1 to F_d^{ϵ} in $O(d^2 + \log q)$ field operations by Proposition 3.8(3), since F_1 has at most two distinct non-zero entries. □

LEMMA 5.3. *If $p = q$ is an odd prime, then a canonical representative H of the subgroups of $\Omega^{\epsilon}(d, q)$ of type $\mathrm{GO}_1(q) \wr \mathrm{Sym}(d)$ can be constructed in $O(d^2 + \log q)$ field operations.*

Proof. By [**14**, Proposition 4.2.15],

$$\begin{aligned} H &\cong 2^{d-1}.\mathrm{Alt}(d) && \text{if } p \equiv \pm 3 \bmod 8, \\ &\cong 2^{d-1}.\mathrm{Sym}(d) && \text{if } p \equiv \pm 1 \bmod 8. \end{aligned}$$

First construct a group preserving $F_d^{\mathsf{S}} = I_d$. Let X and Y be permutation matrices generating $\mathrm{Alt}(d)$, and let $Z := \mathrm{Diag}[-1, -1, 1, \ldots, 1]$. Each of X, Y, Z has determinant 1 and preserves the form I_d. The group $\mathrm{Alt}(d)$ is perfect, since $d \geqslant 7$, so X and Y have spinor norm 1. The matrix Z is a product of two reflections in vectors of norm 2, and so has spinor norm 1.

If $p \equiv \pm 1 \bmod 8$, then let P be the permutation matrix corresponding to $(1, 2) \in \mathrm{Sym}(d)$ and let $R := \mathrm{Diag}[-1, 1, \ldots, 1]$. Then $\det(P) = \det(R) = -1$, and writing RP as a product of reflections shows that $\mathrm{sp}(RP) = 1$, since 2 is a square. Add RP as an additional generator in $O(d^2)$.

Finally, convert F_d^{S} to F_d^{ϵ} in $O(d^2 + \log q)$ field operations, by Proposition 3.8(3). □

LEMMA 5.4. *A canonical representative H of the subgroups of $\Omega^+(d, q)$ of type $\mathrm{GL}(d/2, q).2$ can be constructed in $O(d^2)$ field operations.*

Proof. By [**14**, Proposition 4.2.7],

$$H \cong \frac{1}{(q-1, 2)}\mathrm{GL}(d/2, q).(d/2, 2),$$

where, if q is odd, then $\frac{1}{2}\mathrm{GL}(d/2, q)$ is the unique subgroup of index two in $\mathrm{GL}(d/2, q)$, described after Theorem 3.11. Let A, B be generators for $\frac{1}{(q-1,2)}\mathrm{GL}(d/2, q)$, constructed in $O(d^2)$ field operations. As we remarked earlier, A^{-1} and B^{-1} can be constructed in $O(d^2)$ field operations. Let $A_1 := A \oplus J_{d/2}A^{-\mathrm{T}}J_{d/2}$ and $B_1 := B \oplus J_{d/2}B^{-\mathrm{T}}J_{d/2}$ (here $A^{-\mathrm{T}}$ denotes the transpose of A^{-1}). The spinor norm of A_1 and B_1 is 1 by Lemma 3.5(3). If $(d/2, 2) = 1$, then $H = \langle A_1, B_1\rangle$. If $(d/2, 2) = 2$, then $\det(J_d) = 1$, and J_d is a product of an even number of reflections, all of the same spinor norm, so $\mathrm{sp}(J_d) = 1$ and $H = \langle A_1, B_1, J_d\rangle$. □

LEMMA 5.5. *A canonical subgroup H of $\Omega^\epsilon(d, q)$ of type $\mathrm{GO}(d/2, q)^2$, as in Table 2, can be constructed in $O(d^2 + \log q)$ field operations.*

Proof. By [**14**, Proposition 4.2.16],

$$H \cong \mathrm{SO}^\circ(d/2, q) \times \mathrm{SO}^\circ(d/2, q).$$

Construct $\Omega(d/2, q, I_{d/2}) \times \Omega(d/2, q, \zeta I_{d/2})$, preserving $F_1 = I_{d/2} \oplus \zeta I_{d/2}$, in $O(d^2 + \log q)$ field operations. Adjoin $-{}^*S_m^\circ \oplus -I_m$ and $-I_m \oplus -{}^*S_m^\circ$, which both have spinor norm 1 with respect to F_1. Finally, convert F_1 to F_d^ϵ in $O(d^2 + \log q)$ field operations, by Proposition 3.8(3). □

REMARK. Let P be the block permutation matrix of $(1, 2)$ that interchanges the two fixed subspaces of H, and let $P_1 = (I_{d/2} \oplus \zeta I_{d/2})P$. Then P_1 normalises H and $P_1(I_{d/2} \oplus \zeta I_{d/2})P_1^{\mathrm{T}} = \zeta(I_{d/2} \oplus \zeta I_{d/2})$, so $\langle H, P_1\rangle$ is an imprimitive subgroup of $\mathrm{CO}(d, q, F_1)$.

Proposition 5.1 is now immediate from Lemmas 5.2, 5.3, 5.4 and 5.5.

6. *Semilinear groups*

A group $H \leqslant \mathrm{GL}(d, q)$ is *semilinear* if there is a vector space isomorphism $\tau : \mathrm{GF}(q^s)^{d/s} \to \mathrm{GF}(q)^d$ for some divisor s of d, a subgroup $H^\Gamma \leqslant \Gamma\mathrm{L}(d/s, q^s)$ and an induced embedding (also denoted τ) of $\Gamma\mathrm{L}(d/s, q^s)$ in $\mathrm{GL}(d, q)$, such that $H = \tau(H^\Gamma)$.

In this section we shall prove the following proposition.

PROPOSITION 6.1. *Let $\mathrm{P}\Omega^\epsilon(d, q) \trianglelefteq G \leqslant \mathrm{PC}\Gamma\mathrm{O}^\epsilon(d, q)$. Canonical representatives of the semilinear subgroups of G that arise in Theorem 1.1 can be constructed in $O(d^3 + d^2 \log q)$ field operations.*

The semilinear subgroups H of $\Omega^\epsilon(d, q)$ occurring in Theorem 1.1 are of the types listed in Table 3, based on [**14**, Table 4.3.A], where κ denotes the form preserved by the linear subgroup of $\tau^{-1}(H)$. Here the trace map Tr maps $\alpha \in \mathrm{GF}(q^s)$ to $\alpha + \alpha^q + \ldots + \alpha^{q^{s-1}} \in \mathrm{GF}(q)$.

We denote the canonical primitive element of $\mathrm{GF}(q^s)$ by ν. The matrix operation $(a_{ij}) \mapsto (a_{ij}^q)$ is denoted σ_q, as is the induced automorphism of $\mathrm{GL}(d/s, q^s)$.

LEMMA 6.2 [**10**]. *A canonical subgroup $\langle \Gamma_A, \Gamma_B\rangle \leqslant \mathrm{GL}(s, q)$ that is the image of $\Gamma\mathrm{L}(1, q^s)$, with $|\Gamma_A| = q^s - 1$ and $|\Gamma_B| = s$, may be constructed in $O(s^2 + \log q)$ field operations.*

TABLE 3. *Types of semilinear group.*

ϵ	Type	Description of κ	Conditions
$\circ, +, -$	$\mathrm{GO}^\epsilon(d/s, q^s, \kappa)$	$Q(v) = \mathrm{Tr}(\kappa(v))$	s prime, $d/s \geqslant 3$
$+, -$	$\mathrm{GO}^\circ(d/2, q^2, \kappa)$	$Q(v) = \mathrm{Tr}(\kappa(v))$	$qd/2$ odd
$+, -$	$\mathrm{GU}(d/2, q, \kappa)$	κ unitary, $Q(v) = \kappa(v, v)$	$\epsilon = (-1)^{d/2}$

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

Furthermore, the multiplicative order of $\det(\Gamma_A)$ *is* $q-1$, *and* $\det(\Gamma_B)=1$ *if* s *is odd or* q *is even, or* -1 *if* s *is even and* q *is odd. The first* $s-1$ *rows of* Γ_A *each have a single non-zero entry.*

Note that the construction given in [**10**] is deterministic and hence produces canonical Γ_A and Γ_B. We can calculate $\Gamma_A, \Gamma_A^2, \ldots, \Gamma_A^{s-1}$ in $O(s^3)$ field operations, as each power requires the calculation of only one new row. Define a canonical monomorphism $\tau : \mathrm{GL}(d/s, q^s) \to \mathrm{GL}(d, q)$ as follows. First express the entries of a matrix in $\mathrm{GL}(d/s, q^s)$ as linear combinations $\alpha_0 + \alpha_1\nu + \alpha_2\nu^2 + \ldots + \alpha_{s-1}\nu^{s-1}$, with each $\alpha_i \in \mathrm{GF}(q)$ in $O(s^2 \log q)$ field operations, using Lemma 2.1(2). Then replace each power ν^i $(0 \leqslant i < s)$ in this expression by the $s \times s$ matrix Γ_A^i, and sum in $O(s^3)$ field operations.

We first consider line 1 of Table 3, but only for $s > 2$.

Lemma 6.3. *A canonical set of subgroups of* $\Omega^\epsilon(d, q)$ *of type* $\mathrm{GO}^\epsilon(d/s, q^s)$, *as in Table 3 with* s *an odd prime, can be constructed in* $O(d^3 + d^2 \log q)$ *field operations.*

Proof. For each such s, we construct a subgroup H of $\Omega^\epsilon(d, q)$, with

$$H \cong \Omega^\epsilon(d/s, q^s).s,$$

by [**14**, Propositions 4.3.14, 4.3.16, 4.3.17], where the extension is induced by $\langle\sigma_q\rangle$, the only subgroup of $\mathrm{N}_{\mathrm{GO}^\epsilon(d,q)}(\Omega^\epsilon(d/s, q^s))/\Omega^\epsilon(d/s, q^s)$ of order s.

Use Lemma 6.2 to construct $\Gamma_A, \Gamma_B \in \mathrm{GL}(s, q)$ and then the powers Γ_A^i for $1 < i < s$ in $O(s^3 + \log q)$ field operations. Define the monomorphism $\tau : \mathrm{GL}(d/s, q^s) \to \mathrm{GL}(d, q)$ as above.

If $\epsilon = -$, the central 2×2 block of $Q^-_{d/s}(q^s)$ is not equal to the central 2×2 block of $Q^-_{d/s}(q)$. Construct $A^\epsilon_{d/s}(q^s)$ and $B^\epsilon_{d/s}(q^s)$, and then convert them to matrices A_1 and B_1 preserving $Q^\epsilon_{d/s}(q)$ in $O(d/s + s\log q)$ field operations by Proposition 3.8(1). The point of this is that $\Omega(d/s, q^s, Q^\epsilon_{d/s}(q))$ is normalised by σ_q. If $\epsilon = +$ or $\circ$, then let $A_1 = A^\epsilon_{d/s}(q^s)$ and $B_1 = B^\epsilon_{d/s}(q^s)$.

In all cases, the set of entries of A_1 and B_1 has size not depending on d, q or s, so we can construct $A := \tau(A_1), B := \tau(B_1)$ generating a group isomorphic to $\Omega^\epsilon(d/s, q^s)$ in $O(d^2 + s^2 \log q)$ field operations, as explained above. Let $C := \Gamma_B \oplus \ldots \oplus \Gamma_B \in \mathrm{GL}(d, q)$. Since conjugation by C induces the automorphism σ_q of $\tau(\mathrm{GL}(d/s, q^s))$, the matrix C normalises $\langle A, B\rangle$, and $\langle A, B, C\rangle \cong H$.

Now H fixes the form $\mathrm{Tr}(Q^\epsilon_{d/s}(q))$. The matrix of this form consists of $s \times s$ blocks corresponding to the entries of the matrix of $Q^\epsilon_{d/s}(q)$, where a zero block represents a zero entry of $Q^\epsilon_{d/s}(q)$. Since $Q^\epsilon_{d/s}(q)$, A_1 and B_1 each have $O(d/s)$ non-zero entries, the matrices $\mathrm{Tr}(Q^\epsilon_{d/s}(q))$, A, B and C each have $O(d/s)$ non-zero blocks. If $\epsilon = +$, then all non-zero blocks of $\mathrm{Tr}(Q^\epsilon_{d/s}(q))$ are identical, and we find a $2s \times 2s$ matrix converting a pair of blocks to Q^+_{2s} in $O(s^3 + s\log q)$ field operations by Proposition 3.7. A similar argument holds in type $\circ$. In type $-$, we also find elements of $\mathrm{GL}(4s, q)$ that transform the central $4s \times 4s$ block to the central $4s$ rows and columns of $Q^\epsilon_d(q)$. Since A, B, C have $O(d)$ non-zero blocks, with a constant size set of blocks occurring, we convert them to preserve Q^ϵ_d in $O(s^3 + s\log q + d^2)$ field operations by Proposition 3.7.

Thus, for fixed s, we require $O(s^3 + s^2 \log q + d^2)$ field operations. Let $\mathcal{S}$ be the set of all odd primes dividing d. Then $|\mathcal{S}| = O(\log d)$, and summing gives

$$\begin{aligned} O\left(\sum_{s\in\mathcal{S}} s^3 + s^2\log q + d^2\right) &= O\left(\sum_{t=d/s,\, s\in\mathcal{S}} (d^3/t^3 + d^2/t^2 \log q + d^2)\right) \\ &= O\left(d^3 \sum_{t\geqslant 1} t^{-3} + d^2 \log q \sum_{t\geqslant 1} t^{-2} + d^2 \log d\right) \\ &= O(d^3 + d^2 \log q). \end{aligned}$$

□

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

LEMMA 6.4. *A canonical subgroup H of $\Omega^\epsilon(d,q)$ of type $\mathrm{GO}^{\epsilon_1}(d/2,q^2)$ (the second type in Table 3 and the first type with $s=2$) can be constructed in $O(d^\omega+\log q)$ field operations.*

Proof. We construct $H^* := \langle \tau(A^{\epsilon_1}_{d/2}(q^2)), \tau(B^{\epsilon_1}_{d/2}(q^2))\rangle$, preserving $\mathrm{Tr}(Q^{\epsilon_1}_{d/2}(q^2))$, and $C := \Gamma_B \oplus \ldots \oplus \Gamma_B$, in $O(d^2+\log q)$ field operations (as in the previous lemma, with $s=2$). In each case, with respect to an appropriate form Q, the corresponding subgroup of $\mathrm{GO}^\epsilon(d,q)$ is $M := \langle \tau(\mathrm{GO}^{\epsilon_1}(d/2,q^2,Q)), C\rangle$ by [**14**, Equation (4.3.11)].

There are three cases to consider. If $\epsilon=+$ and $d\equiv 0 \bmod 4$, then

$$H \cong \Omega^+(d/2,q^2).[4],$$

by [**14**, Proposition 4.3.14]. Since the matrices of $Q^+_{d/2}(q^2)$ and $Q^+_{d/2}(q)$ are the same, σ_q fixes $\Omega^+(d/2,q^2)$, so C normalises H^*. If q is even, then adjoin C and $\tau(S^+_{d/2}(q^2))$ to H^* to produce the extension of degree four: since $H=M$ in this case, both of these elements lie in $\Omega^+(d,q)$. If q is odd, then [**14**, Lemma 2.7.2, Equations (4.3.19)–(4.3.21)] state that $\tau(S^+_{d/2}(q^2))$ has determinant $+1$ and spinor norm -1, and that the determinant of all elements of M is 1. Therefore, to create the extension of degree four, let Y be an element of $\{\tau(G^+_{d/2}(q^2)), \tau(G^+_{d/2}(q^2)S^+_{d/2}(q^2))\}$ that has spinor norm 1. We find Y in $O(d^\omega+\log q)$ field operations by Proposition 3.6. The determinant of C is 1, so adjoin Y and either C or $CS^+_{d/2}(q^2)$, depending on $\mathrm{sp}(C)$.

If $\epsilon=-$ and $d\equiv 0 \bmod 4$, then

$$H\cong \Omega^-(d/2,q^2).2,$$

by [**14**, Proposition 4.3.16]. If q is even, then $2\mathrm{Rank}(g+I_{d/2}) = \mathrm{Rank}(\tau(g)+I_d)$ for all $g\in \mathrm{GL}(d/2,q^2)$, so $\det(\tau(S^-_{d/2}(q^2))) = \mathrm{sp}(\tau(S^-_{d/2}(q^2)))=1$. Thus, adjoin $\tau(S^-_{d/2}(q^2))$ to H^*. If q is odd, then [**14**, Lemma 4.1.21] shows that $\mathrm{sp}(\tau(\mathrm{SO}^-(d/2,q^2)))=\langle -1\rangle$, since it contains an element that acts as ζI_2 on a totally singular 2-space $W=\tau(\langle e_1\rangle)$ and centralises $W^\perp/W$. A short calculation shows that $\det(\tau(G^-_{d/2}(q^2)))=1$, so either $\tau(G^-_{d/2}(q^2))$ or $\tau(S^-_{d/2}(q^2)G^-_{d/2}(q^2))$ lies in $\Omega^-(d,q,\mathrm{Tr}(Q^-_{d/2}(q^2)))$. This can be tested in $O(d^\omega+\log q)$ field operations by Proposition 3.6.

If $d\equiv 2 \bmod 4$, then q is odd and

$$H\cong (Z\times \Omega^\circ(d/2,q^2)).2,$$

by [**14**, Proposition 4.3.20], where $Z=Z(\Omega^\epsilon(d,q))$. If $D(Q^\epsilon_d(q))=\mathsf{N}$, then adjoin to H^* whichever of $\pm\tau(S^\circ_{d/2}(q^2))$ has spinor norm 1 (recalling that $-I\notin \Omega^\epsilon(d,q)$ for a non-square discriminant), testing for this condition in $O(d^\omega+\log q)$ field operations by Proposition 3.6.

If $D(Q^\epsilon_d(q))=\mathsf{S}$, note that $\det(C)=-1$ by Lemma 6.2, and define $S=\tau(\nu^{(q-1)/2}I_{d/2})$. Since $\nu^{(q-1)/2}I_{d/2}$ transforms the form $Q^\circ_{d/2}(q)$ to $\nu^{q-1}Q^\circ_{d/2}(q)$, the matrix S transforms $\mathrm{Tr}(Q^\circ_{d/2}(q))$ to $\nu^{q^2-1}\mathrm{Tr}(Q^\circ_{d/2}(q))$; that is, it fixes $\mathrm{Tr}(Q^\circ_{d/2}(q))$. Also, since $\det(\tau(g))=\det(g)^{q+1}$ for all $g\in \mathrm{GL}(d/2,q^2)$ and $d/2$ is odd, $\det(S)=-1$. So, $\det(CS)=1$ and CS induces σ_q on H, since S centralises H^*. A short calculation shows that $(CS)^2=-I_d$. Now $\mathrm{sp}(\tau(S^\circ_{d/2}(q^2)))=-1$ by [**14**, Equation (4.3.26)], so adjoin CS or $CS\tau(S^\circ_{d/2}(q^2))$ to H^*, depending on $\mathrm{sp}(CS)$. This is calculated in $O(d^\omega+\log q)$ field operations by Proposition 3.6.

In all cases, finish by converting the form $\mathrm{Tr}(Q^{\epsilon_1}_{d/2}(q^2))$ to $Q^\epsilon_d(q)$ in $O(d^2+\log q)$ field operations by a similar method to the previous lemma, noting that each row and column requires at most eight row and column operations. □

REMARK. In the second and third cases in the theorem above, the group H is not absolutely irreducible, and it is useful to be able to construct an element in $\mathrm{GO}^\epsilon(d,q)$ inducing the field

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

automorphism, which has determinant -1. When $d/2$ is odd and $D(Q^{\epsilon}_d(q)) = \mathsf{N}$, use the matrix C in the proof above.

When $d/2$ is even and $\epsilon = -$, the entries of the matrix of $Q^{-}_{d/2}(q^2)$ cannot be chosen to lie in $\mathrm{GF}(q)$, so the automorphism of $\mathrm{GL}(d/2, q^2)$ induced by σ_q does not normalise $\Omega^{-}(d/2, q^2)$, and hence C does not normalise $\tau(\Omega^{-}(d/2, q^2))$. Let $S \in \mathrm{GL}(d/2, q^2)$ transform $Q^{-}_{d/2}(q^2)^{\sigma_q}$ to $Q^{-}_{d/2}(q^2)$. Then the automorphism of $\mathrm{GL}(d/2, q^2)$ induced by σ_q followed by conjugation by S normalises $\Omega^{-}(d/2, q^2)$, and $C\tau(S) \in \mathrm{GO}^{-}(d, q, \mathrm{Tr}(Q^{-}_d(q^2)))$ normalises and induces the field automorphism of $\tau(\mathrm{GO}^{-}(d/2, q^2))$. However, $(C\tau(S))^2$ lies in $\tau(\mathrm{GO}^{-}(d/2, q^2) \setminus \mathrm{SO}^{-}(d/2, q^2))$.

Whenever q is odd in the theorem above, the element $\tau(\nu^{(q+1)/2} I_{d/2})$ normalises H and lies in $\mathrm{CO}^{\epsilon}(d, q, \mathrm{Tr}(Q^{\epsilon}_{d/2}(q^2)))$ but does not fix the form.

Lemma 6.5. *A canonical subgroup H of $\Omega^{\epsilon}(d, q)$ of type $\mathrm{GU}(d/2, q)$, as in Table 3, can be constructed in $O(d^{\omega} + \log q)$ field operations.*

Proof. Here $\epsilon = +$ if and only if $d \equiv 0 \bmod 4$. Define τ and C as in the earlier lemmas of this section.

If q is odd and $\epsilon = +$, then

$$H \cong (\tfrac{1}{2}\mathrm{GU}(d/2, q)).2,$$

where the outer 2 is induced by σ_q and $\frac{1}{2}\mathrm{GU}(d/2, q)$ is the unique subgroup of $\mathrm{GU}(d/2, q)$ of index two [**14**, Proposition 4.3.18]. Construct a conjugate of $\frac{1}{2}\mathrm{GU}(d/2, q)$ by first applying τ to the standard generators of $\mathrm{SU}(d/2, q)$ to produce matrices A and B in $O(d^2 + \log q)$ field operations. Then let $B_1 := \tau(\mathrm{Diag}[\xi^{2(q-1)}, 1, \ldots, 1])$, which is constructed in $O(d^2 + \log q)$ field operations. Finally, let X be either C or $C\tau(\mathrm{Diag}[\xi^{(q-1)}, 1, \ldots, 1])$, whichever has spinor norm 1 (tested in $O(d^{\omega} + \log q)$ field operations by Proposition 3.6). Then X is constructed in $O(d^{\omega} + \log q)$ field operations. The form Q_1 fixed by $\langle A, B, X\rangle$ is $Q_1(v) = v(v^{\sigma_q})^{\mathrm{T}}$, with a basis $1, \xi$ for $\mathrm{GF}(q^2)$ over $\mathrm{GF}(q)$. The matrix M_{Q_1} consists of identical 2×2 blocks along the antidiagonal, so Q_1 is converted to Q^{ϵ}_d in $O(d^2 + \log q)$ field operations, by Proposition 3.8(3).

If q is odd and $\epsilon = -$, then $H \cong \frac{1}{2}\mathrm{GU}(d/2, q)$ and the construction is similar to, but easier than, that for $\epsilon = +$. If q is even and $\epsilon = +$, then $H \cong \mathrm{GU}(d/2, q).2$; the construction is similar to that for q odd. Similarly, if q is even and $\epsilon = -$, then $H \cong \mathrm{GU}(d/2, q)$. □

Proposition 6.1 is now immediate from Lemmas 6.3, 6.4 and 6.5.

7. *Tensor product groups*

A group is *tensor product* if it preserves a decomposition $V = V_1 \otimes V_2$. In this section, we shall prove the following proposition.

Proposition 7.1. *Let $\mathrm{P}\Omega^{\epsilon}(d, q) \trianglelefteq G \leqslant \mathrm{PC\Gamma O}^{\epsilon}(d, q)$. Canonical representatives of the tensor product subgroups of G that arise in Theorem 1.1 can be constructed in $O(d^{\omega+\varepsilon} + d^{1+\varepsilon}\log q)$ field operations for every $\varepsilon > 0$.*

Recall the definition of the Kronecker product of matrices, $A \otimes B$, from § 2. For groups $G \leqslant \mathrm{GL}(d_1, q)$ and $H \leqslant \mathrm{GL}(d_2, q)$, we define

$$G \otimes H = (G \times H)/\{(\alpha I_{d_1}, \alpha^{-1} I_{d_2}) : \alpha I_{d_1} \in G, \alpha^{-1} I_{d_2} \in H\}.$$

Table 4, taken from [**14**, Table 4.4.A], lists the types of tensor product group.

The determinant of $A \otimes B \in \mathrm{GL}(d_1, q) \otimes \mathrm{GL}(d_2, q)$ is $\det(A)^{d_2}\det(B)^{d_1}$. If q is odd, and G and H preserve bilinear forms F_G and F_H, respectively, then $G \otimes H$ preserves a bilinear form

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

with matrix $F_G \otimes F_H$. If both F_G and F_H are symmetric or both are symplectic, then $F_G \otimes F_H$ is symmetric. If q is even, and F_G and F_H are both symplectic or both symmetric, then $G \otimes H$ preserves a quadratic form $\overline{Q}$ defined by $\overline{Q}(w_1 \otimes w_2) = 0$ for all $w_i \in V_i$ and $\overline{F} = F_G \otimes F_H$.

Recall that ζ and ξ are the (fixed) primitive elements of $\mathrm{GF}(q)$ and $\mathrm{GF}(q^2)$, respectively. For q odd, let $\alpha = \xi^{(q+1)/2}(\xi - \xi^q)(\xi + \xi^q)^{-1} \in \mathrm{GF}(q)$ and $\beta = 2\zeta(\xi + \xi^q)^{-1}$. Then $\alpha^2 + \beta^2 = \zeta$, and a short calculation shows that

$$A = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$$

converts F_2^{S} to ζF_2^{S}. Similarly, $B = \mathrm{AntiDiag}[\zeta, 1]$ converts F_2^{N} to ζF_2^{N}. Let $E_d^{\mathsf{S}} := A \oplus \ldots \oplus A \in \mathrm{GL}(d, q)$ and $E_d^{\mathsf{N}} := B \oplus A \oplus A \oplus \ldots \oplus A \in \mathrm{GL}(d, q)$. Then E_d^k converts F_d^k to ζF_d^k.

We start with a technical lemma [**14**, Lemma 4.4.13]. Recall that for a non-singular vector v, we write r_v for the reflection in v.

LEMMA 7.2. *Let q be odd, let $V = V_1 \otimes V_2$ with corresponding quadratic form $Q_1 \otimes Q_2$ and let the vector $v \in V_1$ be non-singular.*

(1) *Let $v_1, \ldots, v_d$ be the standard basis for (V_2, F_d^k), where $k \in \{\mathsf{S}, \mathsf{N}\}$. Then*

$$r_v \otimes 1 = r_{v\otimes v_1} r_{v\otimes v_2} \ldots r_{v\otimes v_{d_2}}.$$

(2) *If both V_1 and V_2 have even dimension, then $r_v \otimes 1 \in \mathrm{SO}(V) \setminus \Omega(V)$ if $D(Q_2) = \mathsf{N}$, and $r_v \otimes 1 \in \Omega(V)$ otherwise.*

LEMMA 7.3. *A canonical subgroup H of $\Omega^\epsilon(d, q)$ of type $\Omega^{\epsilon_1}(d_1, q) \otimes \Omega^{\epsilon_2}(d_2, q)$, as in Table 4, can be constructed in $O(d^\omega + d \log q)$ field operations.*

Proof. We consider various possibilities for d_1, d_2, ϵ_1 and ϵ_2. In each case we will construct a conjugate of H that preserves a diagonal or antidiagonal form F_1 with at most four distinct entries, so F_1 may be converted to $F_d^\epsilon(q)$ in $O(d^2 + \log q)$ field operations by Proposition 3.8(3).

For d odd, $H \cong (\Omega^\circ(d_1, q) \otimes \Omega^\circ(d_2, q)).2$ [**14**, Proposition 4.4.18]. Construct $\Omega^\circ(d_1, q) \otimes \Omega^\circ(d_2, q)$ as a Kronecker product. By Lemma 7.2(1), $\mathrm{sp}(S_{d_1}^\circ \otimes S_{d_2}^\circ) = 1$. The form $F_{d_1}^\circ \otimes F_{d_2}^\circ$ is antidiagonal with three distinct non-zero entries.

Next assume that d_2 is odd but d_1 is even, so that $\epsilon = \epsilon_1$. Then $H \cong \Omega^\epsilon(d_1, q) \otimes \mathrm{SO}^\circ(d_2, q)$ [**14**, Proposition 4.4.17]. First construct ${}^*X_l^\alpha(q)$, where $X \in \{A, B, S\}$, $\alpha \in \{\circ, \epsilon\}$, and $l \in \{d_1, d_2\}$, and then construct a conjugate of H preserving the diagonal form $F_{d_1}^{D(F_{d_1}^{\epsilon_1})} \otimes I_{d_2}$ as a Kronecker product.

Finally, assume that both d_1 and d_2 are even, so that $\epsilon = +$. For $i = 1, 2$, let $k_i = D(F_{d_i}^{\epsilon_i})$, and let $F_1 = F_{d_1}^{k_1} \otimes F_{d_2}^{k_2}$. Define s to be 4 if any of the following hold:

(1) $\epsilon_1 = \epsilon_2 = -$;
(2) $\epsilon_1 = \epsilon_2 = +$ and exactly one of k_1, k_2 equals S;
(3) $\epsilon_1 = \epsilon_2 = +$, $k_1 = k_2$ and $d \equiv 4 \bmod 8$; or
(4) $\epsilon_1 = +$, $\epsilon_2 = -$ and at least one of k_1, k_2 equals N;

TABLE 4. *Types of tensor product group.*

ϵ	Type	Conditions
$\circ, +, -$	$\Omega^{\epsilon_1}(d_1, q) \otimes \Omega^{\epsilon_2}(d_2, q)$	$d = d_1 d_2$, $(d_1, \epsilon_1) \neq (d_2, \epsilon_2)$ $d_1, d_2 > 2$, q odd $(\epsilon = \circ) \Leftrightarrow (\epsilon_1 = \epsilon_2 = \circ)$ $(\epsilon = -) \Leftrightarrow (\epsilon_1 = -, \epsilon_2 = \circ)$
$+$	$\mathrm{Sp}(d_1, q) \otimes \mathrm{Sp}(d_2, q)$	$d \equiv 0 \bmod 4$, $d = d_1 d_2$, $d_1 < d_2$

and $s = 8$ otherwise. Then $H \cong (\mathrm{SO}^{\epsilon_1}(d_1, q) \otimes \mathrm{SO}^{\epsilon_2}(d_2, q)).[s]$ [**14**, Propositions 4.4.14, 4.4.15, 4.4.16]. Construct $H_1 = \mathrm{SO}(d_1, q, F_{d_1}^{k_1}) \otimes \mathrm{SO}(d_2, q, F_{d_2}^{k_2})$ in $O(d^2 + \log q)$ field operations, preserving F_1. Let $G_1 = {}^*G_{d_1}^{\epsilon_1} \otimes 1$ and $G_2 = 1 \otimes {}^*G_{d_2}^{\epsilon_2}$. It is immediate from Lemma 7.2(2) that $\mathrm{sp}(G_i) = 1$ if and only if $k_{3-i} = \mathsf{S}$. Let $D = E_{d_1}^{k_1} \otimes (E_{d_2}^{k_2})^{-1} \in \mathrm{SO}^+(d, q, F_1)$, and note that $(E_d^k)^{-1}$ can be computed in $O(d^2)$ field operations.

If $s = 8$, then adjoin G_1, G_2 and D to H_1. If $s = 4$, then compute the spinor norms of G_1, G_2 and D in $O(d^\omega + \log q)$ field operations, and adjoin appropriate products to H_1. □

Remark. It is possible to write down conditions on d_1, d_2, q, ϵ_1 and ϵ_2 that determine when each of G_1, G_2 and D have spinor norm 1, and thus improve the complexity of the above result to $O(d^2 + \log q)$ field operations, but we omit the lengthy calculations.

Lemma 7.4. *A canonical subgroup H of $\Omega^+(d, q)$ of type $\mathrm{Sp}(d_1, q) \otimes \mathrm{Sp}(d_2, q)$, as in Table 4, can be constructed in $O(d^2)$ field operations.*

Proof. If $d \equiv 4 \bmod 8$ or q is even, then $H \cong \mathrm{Sp}(d_1, q) \circ \mathrm{Sp}(d_2, q)$, otherwise $H \cong (\mathrm{Sp}(d_1, q) \circ \mathrm{Sp}(d_2, q)).2$ [**14**, Proposition 4.4.12].

Generate $\mathrm{Sp}(d_1, q) \circ \mathrm{Sp}(d_2, q)$ as a Kronecker product in $O(d^2)$ field operations, by Theorem 3.11. If $d \equiv 0 \bmod 8$ and q is odd, then adjoin $(\zeta I_{d_1/2} \oplus I_{d_1/2}) \otimes (\zeta^{-1} I_{d_2/2} \oplus I_{d_2/2})$. Since the standard symplectic form is antidiagonal with all non-zero entries ± 1, if q is even these matrices all naturally preserve Q_d^ϵ, whilst if q is odd these matrices may be converted to preserve Q_d^ϵ in $O(d^2 + \log q)$ field operations by Proposition 3.8(3). □

Proposition 7.1 follows from the preceding two lemmas and the fact that there are $O(d^\varepsilon)$ classes of tensor product groups of each type, for every real $\varepsilon > 0$, by Lemma 2.2(2).

8. *Subfield groups*

A group is *subfield* if, modulo scalars, it can be written over a proper subfield of $\mathrm{GF}(q) = \mathrm{GF}(p^e)$. Throughout this section, f will denote a divisor of e such that $r = e/f$ is prime. In [**14**, Table 4.5.A], we find that for each such f there are at most two types of subfield subgroups H. If either d or r is odd, then there is exactly one. If d is even and $r = 2$, then there are none if $\epsilon = -$ and two if $\epsilon = +$.

Proposition 8.1. *Let $\mathrm{P}\Omega^\epsilon(d, q) \trianglelefteq G \leqslant \mathrm{PC\Gamma O}^\epsilon(d, q)$. Canonical representatives of the set of subfield subgroups of G that arise in Theorem 1.1 can be constructed in $O(d^2 \log \log q + \log q \log \log q)$ field operations.*

Proof. There are $O(\log \log q)$ prime divisors of e by Lemma 2.2(1). Let H denote one of the subgroups to be constructed. The structure of H is given in [**14**, Propositions 4.5.8, 4.5.9].

If d is odd, then $H \cong \Omega^\circ(d, q^{1/r})$ if r is odd, and $H \cong \mathrm{SO}^\circ(d, q^{1/2})$ if $r = 2$. The group $\mathrm{SO}^\circ(d, q^{1/r})$ naturally preserves $F_d^\circ(q)$, and generators for H are constructed in $O(d^2 + \log q)$ field operations.

So, assume for the remainder of the proof that d is even. If q is even, then $H \cong \Omega^{\epsilon_1}(d, q^{1/r})$ for all r. If $\epsilon_1 = +$, then $Q_d^+(q^{1/r}) = Q_d^+(q)$. If $\epsilon_1 = -$, then convert $Q_d^-(q^{1/r})$ to $Q_d^\epsilon(q)$ in $O(d + \log q)$ field operations by Proposition 3.8(1).

Suppose from now on that q is odd. The first case is when r is odd. Then $\epsilon_1 = \epsilon$ and $H \cong \Omega^{\epsilon_1}(d, q^{1/r})$. The group $\Omega^+(d, q^{1/r})$ preserves $F_d^+(q^{1/r}) = F_d^+(q)$. The forms $F_d^-(q^{1/r})$ and $F_d^-(q)$ differ on $\langle x, y \rangle$, which is corrected in $O(d + \log q)$ field operations by Proposition 3.8(1), so this case requires $O(d^2 + \log q)$ field operations.

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

Suppose from now on that $r=2$, so d is even and $\epsilon=+$. Then q is square so $q\equiv 1 \bmod 4$. Let $k=D(F_d^{\epsilon_1}(q^{1/2}))$ over $\mathrm{GF}(q^{1/2})$, and let

$$s=\begin{cases}1 & \text{if either } d\equiv 0 \bmod 4 \text{ and } k=\mathsf{N},\\ & \text{or } d\equiv 2 \bmod 4 \text{ and } k=\mathsf{S},\\ 2 & \text{otherwise.}\end{cases}$$

Then $H\cong \mathrm{SO}^{\epsilon_1}(d,q^{1/2}).[s]$ by [**14**, Proposition 4.5.10].

For $s=1$ and $\epsilon_1=+$, set

$$H=\mathrm{SO}^+(d,q^{1/2})=\mathrm{SO}(d,q^{1/2},F_d^+(q)).$$

For $s=1$ and $\epsilon_1=-$, convert $F_d^-(q^{1/2})$ to $F_d^+(q)$ in $O(d+\log q)$ field operations by Proposition 3.8(1).

Now suppose $s=2$, and let $\lambda=\zeta^{(q^{1/2}+1)/2}$, so that λ^2 is the primitive element of $\mathrm{GF}(q^{1/2})$. If $\epsilon_1=+$, then let $A=\lambda I_{d/2}\oplus\lambda^{-1}I_{d/2}$. Then A fixes $F_d^+(q)=F_d^+(q^{1/2})$ and $\det(A)=1$, so $A\in\mathrm{SO}^+(d,q)$. To see that $\mathrm{sp}(A)=1$, use Lemma 3.5(3), and note that either $d=0 \bmod 4$ or $q^{1/2}\equiv 3 \bmod 4$, so in both cases the determinant of A restricted to $\langle e_1,\ldots,e_m\rangle$ is square. We construct H as $\langle \mathrm{SO}^+(d,q^{1/2}),A\rangle$.

If $\epsilon_1=-$, then $q^{1/2}\equiv 1 \bmod 4$ and $d\equiv 2 \bmod 4$ by Lemma 3.3(1). Let

$$F_1=\mathrm{AntiDiag}[1,1]\oplus\ldots\oplus\mathrm{AntiDiag}[1,1]\oplus\mathrm{Diag}[1,\lambda^2].$$

Note that F_1 is of $-$ type over $\mathrm{GF}(q^{1/2})$ but of $+$ type over $\mathrm{GF}(q)$. Set

$$A=\mathrm{Diag}[\lambda,\lambda^{-1}]\oplus\ldots\oplus\mathrm{Diag}[\lambda,\lambda^{-1}]\oplus\mathrm{AntiDiag}[-\lambda^{-1},\lambda].$$

Then $\det(A)=1$ and A preserves F_1. A short calculation shows that the final block of A has spinor norm 1 with respect to $\mathrm{Diag}[1,\lambda^2]$. Since there are an even number of copies of the first block of A, it follows that $A\in\Omega^+(d,q,F_1)$. The form F_1 can be converted to $F_d^+(q)$ in $O(d^2+\log q)$ field operations by Proposition 3.8(3), whilst $F_d^-(q^{1/2})$ is converted to $F_d^+(q)$ in $O(d+\log q)$ field operations by Proposition 3.8(1). Finally, H is generated by these conjugates of $\mathrm{SO}^-(d,q^{1/2})$ and A. □

9. *Groups of extraspecial normaliser type*

Assume $\epsilon=+$, $q=p$ is odd and $d=2^m$, otherwise there are no extraspecial normaliser groups. Then, by [**14**, Proposition 4.6.8], $\Omega^+(d,q)$ has a subgroup isomorphic to $2_+^{1+2m}.\Omega^+(2m,2)$ if $p\equiv\pm 3 \bmod 8$, and to $2_+^{1+2m}.\mathrm{GO}^+(2m,2)$ if $p\equiv\pm 1 \bmod 8$. The group $E\cong 2_+^{1+2m}$ is a central product of dihedral groups of order eight.

In this section we shall prove the following proposition.

PROPOSITION 9.1. *Let $\mathrm{P}\Omega^\epsilon(d,q)\trianglelefteq G\leqslant \mathrm{PC\Gamma O}^\epsilon(d,q)$. A canonical representative of the extraspecial normaliser type subgroups of G that arise in Theorem 1.1 can be constructed in $O(d^2\log d+\log q)$ field operations.*

We write down generators of $\mathrm{N}_{\mathrm{GL}(d,q)}(E)\cong\langle Z(\mathrm{GL}(d,q)),E.\mathrm{GO}^+(2m,2)\rangle$, and then modify them to produce a subgroup of $\Omega^+(d,q)$.

LEMMA 9.2. *A canonical group $\mathrm{N}_{\mathrm{GL}(d,q)}(E)$ can be constructed in $O(d^2\log d)$ field operations.*

Proof. We first construct E. Let $X=\mathrm{Diag}[1,-1]$ and $Y=\mathrm{AntiDiag}[1,1]$. Then $[Y,X]=-I_2$, and so $\langle X,Y\rangle\cong D_8\cong 2_+^{1+2}$. For $1\leqslant i\leqslant m$, define $X_i:=I_{2^{m-i}}\otimes X\otimes I_{2^{i-1}}$ and $Y_i:=$

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

$I_{2^{m-i}} \otimes Y \otimes I_{2^{i-1}}$. The group $\langle X_i, Y_i \mid 1 \leqslant i \leqslant m\rangle$ is a central product of m copies of $\langle X, Y\rangle$, so let E be this group. It can be checked that E fixes the form $I_d = F_d^{\mathsf{S}}$.

Now we construct $\mathrm{N}_{\mathrm{GL}(d,q)}(E)$. Let $E_k := 2_+^{1+2k} \leqslant \mathrm{GL}(2^k, q)$, so that $E = E_m$. For $G \leqslant \mathrm{GL}(d, q)$, we write $\overline{G}$ for $G/(G \cap Z(\mathrm{GL}(d, q)))$. Let

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

Then $\langle X, Y, U\rangle$ induces $\mathrm{GO}^+(2, 2) \cong 2$ on $\overline{E_1}$. For $1 \leqslant i \leqslant m$, define $U_i := I_{2^{m-i}} \otimes U \otimes I_{2^{i-1}}$. Then the U_i all normalise E and $\langle X_i, Y_i, U_i : 1 \leqslant i \leqslant m\rangle$ induces a direct product of m copies of $\mathrm{GO}^+(2, 2)$ on E.

Let $W \in \mathrm{GL}(4, q)$ be the permutation matrix defined by $(1, 3) \in \mathrm{Sym}(4)$. Then $I_2 \otimes X$ is centralised by W, whereas $(X \otimes I_2)^W = -(I_2 \otimes X)(X \otimes I_2)$. Similarly, $Y \otimes I_2$ is centralised by W, whilst $(I_2 \otimes Y)^W = (I_2 \otimes Y)(Y \otimes I_2)$. For $1 \leqslant i \leqslant m-1$, define $W_i := I_{2^{m-1-i}} \otimes W \otimes I_{2^{i-1}}$. Then $X_j^{W_i} = X_j$ for $j \neq i+1$ and $X_{i+1}^{W_i} = -X_i X_{i+1}$, whereas $Y_j^{W_i} = Y_j$ for $j \neq i$ and $Y_i^{W_i} = Y_i Y_{i+1}$.

We now prove by induction on k that for $2 \leqslant k \leqslant m$ the group

$$N_k := \langle X_i, Y_i, U_i, W_j : 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant k-1\rangle$$

induces $\mathrm{GO}^+(2k, 2)$ on $\overline{E_k}$. We check this by direct computation for $k \leqslant 4$ and then, for the inductive step, we may assume that N_{k+1}, in its action on $\overline{E_{k+1}}$, properly contains $\mathrm{GO}^+(2(k-1), 2) \times \mathrm{GO}^+(4, 2)$. But, since $k-1 \geqslant 3$, this is a maximal subgroup of $\mathrm{GO}^+(2k+2, 2)$ by [**14**, Table 3.5.E]. So, N_{k+1} induces $\mathrm{GO}^+(2k+1, 2)$ on $\overline{E_{k+1}}$, which completes the induction. Thus,

$$\langle X_i, Y_i, U_i, W_j, Z(\mathrm{GL}(d, q)) : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant m-1\rangle$$

is the normaliser in $\mathrm{GL}(d, q)$ of E. □

Proof of Proposition 9.1. We consider each non-scalar generator of $\mathrm{N}_{\mathrm{GL}(d,q)}(E)$. The determinant of X is -1, so $\det(X_i) = (-1)^{d/2} = 1$ for all i, since $d = 2^m \geqslant 8$. Furthermore, $\mathrm{sp}(X) = 1$ with respect to F_2^{S}. Thus, $\mathrm{sp}(X_i) = 1$ with respect to F_d^{S} for all i, by Lemma 7.2(2). Similarly, Y_i and W_i are in $\Omega(d, q, F_d^{\mathsf{S}})$ for all i.

The determinant of U is -2, and $UF_2^{\mathsf{S}}U^{\mathrm{T}} = 2F_2^{\mathsf{S}}$. If $q \equiv \pm 1 \bmod 8$, then there exists a canonical $\rho \in \mathrm{GF}(q)$ such that $\rho^2 = 2$, which can be constructed in $O(\log q)$ field operations. Then, as before, $\mathrm{sp}(\rho^{-1}U_i) = \det(\rho^{-1}U_i) = 1$.

Assume now that $q \equiv \pm 3 \bmod 8$. The determinant of U_i is $2^{d/2}$ for $1 \leqslant i \leqslant m$, so $\det(U_i U_{i+1}^{-1}) = 1$. Let $S = (I_2 \otimes U)(U^{-1} \otimes I_2)$, then $S \in \mathrm{GO}(4, q, F_4^{\mathsf{S}})$. Therefore, $\mathrm{sp}(U_i U_{i+1}^{-1}) = 1$ for $1 \leqslant i \leqslant m-1$ by Lemma 7.2(2). Since $U_i U_j = U_j U_i$ for all i, j, it follows that $\langle X_i, Y_i, W_i, U_i U_{i+1}^{-1}\rangle \cong 2_+^{1+2m}.\Omega^+(2m, 2)$, as required. Note that $U_i U_{i+1}^{-1}$ can be calculated in $O(d^2)$ field operations as a Kronecker product.

For all q, the form F_d^{S} fixed by E can be converted to the standard form in $O(d^2 \log d + \log q)$ field operations by Proposition 3.8(3), so discarding the scalar generators produces the required subgroup of $\Omega^+(d, q)$. □

10. *Tensor induced groups*

A group is *tensor induced* if it preserves a decomposition $V = V_1 \otimes \ldots \otimes V_t$, with $\dim(V_i) = m$ for $1 \leqslant i \leqslant t$. In this section we shall prove the following proposition.

Proposition 10.1. *Let* $\mathrm{P}\Omega^{\epsilon}(d, q) \trianglelefteq G \leqslant \mathrm{P}\mathrm{C}\Gamma\mathrm{O}^{\epsilon}(d, q)$. *Canonical representatives of the tensor induced subgroups of* G *that arise in Theorem* 1.1 *can be constructed in* $O(d^{\omega} \log\log d + \log d \log\log d \log q)$ *field operations.*

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

Let $H \leqslant \mathrm{GL}(m, q)$ and let $K \leqslant \mathrm{Sym}(t)$ be transitive. Then

$$H \operatorname{TWr} K = (H \otimes \ldots \otimes H){:}K$$

is the *tensor wreath product* of H and K. It is like a standard wreath product except that we take a *central* product of t copies of H with amalgamated subgroup $H \cap Z(\mathrm{GL}(m, q))$. If each V_i admits a bilinear form F_i, then there is a bilinear form F on V given by setting

$$F(v_1 \otimes \ldots \otimes v_t, w_1 \otimes \ldots \otimes w_t) := \prod_{i=1}^{t} F_i(v_i, w_i),$$

and extending linearly. If qt is even and the F_i are symplectic, then F is symmetric. If the F_i are symmetric, then F is symmetric. Table 5 gives the types of tensor induced group, based on [**14**, Table 4.7.A].

LEMMA 10.2 [**10**]. *Let $H = \langle h_1, \ldots, h_a \rangle \leqslant \mathrm{GL}(m, q)$, and let $K = \langle k_1, \ldots, k_b \rangle$ be a transitive subgroup of* $\mathrm{Sym}(t)$. *Then $H \operatorname{TWr} K$ can be constructed in $O((a + b)m^{2t})$ field operations.*

LEMMA 10.3. *A canonical subgroup of $\Omega^+(d, q)$ of type* $\mathrm{Sp}(m, q) \operatorname{TWr} \mathrm{Sym}(t)$*, as in Table* 5*, can be constructed in $O(d^2 + \log q)$ field operations.*

Proof. If $m \equiv 2 \bmod 4$ and $t = 2$, then $H \cong \mathrm{Sp}(m, q) \times \mathrm{Sp}(m, q)$ by [**14**, Proposition 4.7.5]. Construct canonical generators for $\mathrm{Sp}(m, q)$ in $O(m^2)$ field operations by Theorem 3.11, then construct a canonical copy of H as a central product with four generators in $O(d^2)$ field operations. The resulting form F_1 is antidiagonal with all entries ± 1, so can be converted to Q_d^+ in $O(d^2 + \log q)$ field operations by Propositions 3.8(2) and 3.8(3).

Otherwise, by [**14**, Proposition 4.7.5],

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

and (comparing with [**14**, Equation (4.7.6)]) H is the stabiliser in $\mathrm{GO}^+(d, q)$ of the tensor decomposition. Thus, all elements of $\mathrm{GO}^+(d, q)$ that stabilise the tensor decomposition lie in (a fixed conjugate of) H. First construct a copy of $\mathrm{Sp}(m, q) \operatorname{TWr} \mathrm{Sym}(t)$ in $O(d^2)$ field operations, by Lemma 10.2. If q is odd, then let

$$D = \mathrm{Diag}[\zeta, \ldots, \zeta, 1, \ldots, 1] \otimes \mathrm{Diag}[\zeta^{-1}, \ldots, \zeta^{-1}, 1, \ldots, 1] \otimes I_m \otimes \ldots \otimes I_m,$$

with t factors, and $m/2$ entries 1 in the first two matrices. We adjoin D, which can be constructed in $O(d^2)$ field operations, as a new generator. A short calculation shows that $D \in \mathrm{GO}^+(d, q, F_1)$ and D normalises $\mathrm{Sp}(m, q) \operatorname{TWr} \mathrm{Sym}(t)$. We let $H^* = \langle \mathrm{Sp}(m, q) \operatorname{TWr} \mathrm{Sym}(t), D \rangle$. Then $H^* \cong H$. Finally, F_1 is antidiagonal with all entries ± 1, so can be converted to Q_d^+ in $O(d^2 + \log q)$ field operations by Proposition 3.8(3). □

LEMMA 10.4. *A canonical subgroup of $\Omega^\circ(d, q)$ of type* $\mathrm{GO}^\circ(m, q) \operatorname{TWr} \mathrm{Sym}(t)$*, as in Table* 5*, can be constructed in $O(d^\omega + \log q)$ field operations.*

TABLE 5. *Types of tensor induced group.*

Case	Type	Conditions
$+$	$\mathrm{GO}^\pm(m, q) \operatorname{TWr} \mathrm{Sym}(t)$	$d = m^t$ and q odd
$+$	$\mathrm{Sp}(m, q) \operatorname{TWr} \mathrm{Sym}(t)$	$d = m^t$ and qt even, $(m, q) \notin \{(2, 2), (2, 3)\}$
$\circ$	$\mathrm{GO}^\circ(m, q) \operatorname{TWr} \mathrm{Sym}(t)$	$d = m^t$ and qm odd

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

Proof. By [14, Proposition 4.7.8], $H \cong \Omega^\circ(m,q)^t.2^{t-1}.\mathrm{Sym}(t)$ and, by [14, Equation (4.7.6)],

$$\mathrm{N}_{\mathrm{GO}^\circ(d,q)}(H) = \mathrm{GO}^\circ(m,q)\,\mathrm{TWr}\,\mathrm{Sym}(t) \cong \langle -I\rangle \times \mathrm{SO}^\circ(m,q)\,\mathrm{TWr}\,\mathrm{Sym}(t).$$

First construct generators A, B, C, D for $\Omega^\circ(m,q,I_d)\,\mathrm{TWr}\,\mathrm{Sym}(t)$, where D corresponds to $(1,2) \in \mathrm{Sym}(t)$. This can be done in $O(d^2 + \log q)$ field operations by Theorem 3.9 and Lemma 10.2. The group $H_1 = \Omega(m,q,I_d)\,\mathrm{TWr}\,\mathrm{Alt}(t)$ preserves I_d and is a subgroup of $\Omega(m,q,I_d)\,\mathrm{TWr}\,\mathrm{Sym}(t) \leqslant \mathrm{GO}(d,q,I_d)$, so $H_1 \leqslant \Omega(d,q,I_d)$. By [14, Equation (4.7.8)], odd permutations of $\mathrm{Sym}(t)$ have determinant -1 if $m \equiv 3 \bmod 4$ and determinant 1 otherwise. In the former case, replace D by $-D$.

The element ${}^*S_m^\circ$ is the product of a reflection in a vector of square norm and one of non-square norm, so $S := {}^*S_m^\circ \otimes I_m \otimes \ldots \otimes I_m$ is the product of m^{t-1} reflections in vectors of square norm and m^{t-1} reflections in vectors of non-square norm. Let $T = {}^*S_m^\circ \otimes ({}^*S_m^\circ)^{-1} \otimes I_m \otimes \ldots \otimes I_m$. Then $\mathrm{sp}(S) = -1$, so $\mathrm{sp}(T) = 1$. Compute $\mathrm{sp}(D)$ in $O(d^\omega + \log q)$ field operations, then let E be whichever of $\pm S^i D$ has determinant and spinor norm 1, for $i \in \{0,1\}$. Then $H^* = \langle A, B, C, T, E\rangle$ is isomorphic to H. The group H^* preserves the form I_d, so H^* can be converted to preserve F_d° in $O(d^2 + \log q)$ field operations by Proposition 3.8(3). □

LEMMA 10.5. *A canonical subgroup of $\Omega^+(d,q)$ of type $\mathrm{GO}^{\epsilon_1}(m,q)\,\mathrm{TWr}\,\mathrm{Sym}(t)$, as in Table 5, can be constructed in $O(d^2 + \log d \log q)$ field operations.*

Proof. The tensor induced subgroups G of $\mathrm{GO}^+(m^t,q)$ of this type have shape

$$(2,q-1).\mathrm{PGO}^{\epsilon_1}(m,q)^t.[2^{t-1}].\mathrm{Sym}(t),$$

for $\epsilon_1 \in \{+,-\}$. The structure of H depends on m, q, t and ϵ_1, but a short calculation shows that it always contains a group K, which is either $\mathrm{SO}^{\epsilon_1}(m,q)\,\mathrm{TWr}\,\mathrm{Alt}(t)$ or (if $t=2$ and $m \equiv 2 \bmod 4$) is $\mathrm{SO}^{\epsilon_1}(m,q) \otimes \mathrm{SO}^{\epsilon_1}(m,q)$. Let $k = D(Q_m^{\epsilon_1})$. Make a conjugate of K from groups preserving F_m^k in $O(d^2 + \log q)$ field operations, using Corollary 3.10 and Lemma 10.2. The group K preserves a diagonal form F_1 with $O(t)$ distinct entries.

Next we analyse which other elements of G lie in $\Omega^+(d,q)$. It is immediate that $G_1 := G_m^{\epsilon_1} \otimes I_m \otimes \ldots \otimes I_m$ has determinant 1, and it follows from Lemma 7.2 that $\mathrm{sp}(G_1) = 1$ unless $t = 2$ and $k = \mathsf{N}$.

Recall the definition of E_d^k from just before Lemma 7.2. The element $E_m^k \otimes (E_m^k)^{-1} \otimes I_m \otimes \ldots \otimes I_m$ always has determinant 1, and it can be shown (see [14, Propositions 4.4.14, 4.4.16] and use Lemma 7.2) that it has spinor norm -1 if and only if $t = 2$ and $m \equiv 2 \bmod 4$.

Finally, let P induce the permutation $(1,2)$ on the tensor factors. Then P is a product of $m^{t-2}\binom{m}{2}$ reflections, so $P \notin \mathrm{SO}^+(d,q)$ if and only if $t = 2$ and $m \equiv 2 \bmod 4$. It follows from Lemma 7.2 that if $t \geqslant 3$ then $P \in \Omega^+(d,q,F_1)$ unless $t = 3$, $m \equiv 2 \bmod 4$ and $k = \mathsf{N}$.

Now we work through the possible cases for m, q, t and ϵ_1.

If $t = 2$ and $m \equiv 2 \bmod 4$, then a simple generalisation of [14, Propositions 4.7.6, 4.7.7] shows that

$$H \cong (\mathrm{SO}^{\epsilon_1}(m,q) \otimes \mathrm{SO}^{\epsilon_1}(m,q)).[4].$$

If $k = \mathsf{S}$ then let $H^* = \langle K, {}^*G_m^{\epsilon_1} \otimes I_m, I_m \otimes {}^*G_m^{\epsilon_1}\rangle$, and if $k = \mathsf{N}$ then let

$$H^* = \langle K, {}^*G_m^{\epsilon_1} \otimes ({}^*G_m^{\epsilon_1})^{-1}, {}^*G_m^{\epsilon_1}E_m^k \otimes (E_m^k)^{-1}\rangle.$$

If $t = 2$, $m \equiv 0 \bmod 4$ and $\epsilon_1 = -$ then we calculate that

$$H \cong (\mathrm{SO}^-(m,q) \otimes \mathrm{SO}^-(m,q)).[8].$$

Let P_1 be whichever of P or $P({}^*G_m^- \otimes I_m)$ has spinor norm 1, and let

$$H^* = \langle K, {}^*G_m^- \otimes ({}^*G_m^-)^{-1}, E_m^k \otimes (E_m^k)^{-1}, P_1\rangle.$$

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

If $t = 3$, $m \equiv 2 \bmod 4$ and $k = \mathsf{N}$, then

$$H \cong \left(\bigotimes_{i=1}^{3} \mathrm{SO}^{\epsilon_1}(m, q)\right).[2^5].3.$$

Let

$$H^* = \langle K, {}^*G_m^{\epsilon_1} \otimes I_m \otimes I_m, E_m^{\mathsf{N}} \otimes (E_m^{\mathsf{N}})^{-1} \otimes I_m\rangle.$$

In all other cases,

$$H \cong \left(\bigotimes_{i=1}^{t} \mathrm{SO}^{\epsilon_1}(m, q)\right).[2^{2t-1}].\mathrm{Sym}(t)$$

and we let

$$H^* = \langle K, {}^*G_m^{\epsilon_1} \otimes I_m \otimes \ldots \otimes I_m, E_m^k \otimes (E_m^k)^{-1} \otimes I_m \otimes \ldots \otimes I_m, P\rangle.$$

In each case, F_1 is diagonal with $O(t) = O(\log d)$ distinct entries, which can be converted to $Q_d^+(q)$ in $O(d^2 + \log d \log q)$ field operations. □

For each of the preceding three lemmas there are $O(\log\log d)$ groups to construct, so Proposition 10.1 follows.

11. *The plus type groups in dimension eight*

The maximal subgroups of the almost simple groups with socle $\mathrm{P}\Omega^+(8, q)$ are described in detail in [**13**], and listed in Table I of that paper. Many of these subgroups, including all of the geometric maximal subgroups of $\mathrm{P}\Omega^+(8, q)$ itself, belong to families that occur in other dimensions and, in these cases, we have already described how to construct the pre-images of their intefrsections with $\mathrm{P}\Omega^+(8, q)$.

In this section, we describe how to write down generators for the pre-images in $\Omega^+(8, q)$ of the intersections with $\mathrm{P}\Omega^+(8, q)$ of those geometric maximal subgroups that arise only in dimension eight; that is, those which arise *only* as maximal subgroups of extensions of $\mathrm{P}\Omega^+(8, q)$ that involve the triality automorphism. It turns out that these pre-images are all maximal subgroups H of other subgroups K of $\Omega^+(8, q)$, whose constructions we have already described.

In particular, we shall prove the following proposition.

Proposition 11.1. *Let $\mathrm{P}\Omega^+(8, q) \trianglelefteq G \leqslant \mathrm{Aut}(\mathrm{P}\Omega^+(8, q))$. A set of canonical representatives of the subgroups of G that arise in Theorem 1.1 can be constructed in $O(\log q \log\log q)$ field operations.*

We shall proceed down the list in [**13**, Table I], so we are assuming that the reader has this table to hand. The assertions that we shall make concerning certain subgroups in the list being contained in other subgroups in the list can all be easily justified by consulting the references provided in the final column of that table.

To avoid confusion between, for example, the subgroup named P_2 in line 4 of [**13**, Table I] and the notation P_k that we used in § 4 to denote the stabiliser of a totally singular k-space, we shall continue to use P_k as in § 4, but use P_k' to denote the subgroups named P_k in [**13**]. All other group names are distinct from symbols used elsewhere in this paper. We write $^\wedge H$ to mean the pre-image in $\Omega^+(8, q)$ of a subgroup of $\mathrm{P}\Omega(8, q)$.

Lines 1 to 3 of [**13**, Table I] consist of groups that are constructed in § 4, namely $^\wedge R_{s1} = P_1$ and $^\wedge R_{34}^1 \cong {}^\wedge R_{34}^2 = P_4$.

Lemma 11.2. *A canonical pre-image of the group $^\wedge P_2'$ in line 4 of [**13**, Table I] can be constructed in $O(\log q)$ field operations.*

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

Proof. Roughly speaking, we construct ${}^{\wedge}P_2' \leqslant P_3$ by replacing the factor $\mathrm{GL}(3,q)$ in P_3 (constructed in Lemma 4.2) by its maximal parabolic subgroup K with structure $q^2{:}(\mathrm{GL}(1,q)\times\mathrm{GL}(2,q))$. We described how to construct the intersection of K with $\mathrm{SL}(3,q)$ in [**10**, Proposition 4.1]. By the construction in Lemma 4.2, we need generators for $q^2{:}(\mathrm{GL}(1,q)\times\mathrm{GL}(2,q))$ when q is even, and of $q^2{:}\frac{1}{2}(\mathrm{GL}(1,q)\times\mathrm{GL}(2,q))$ together with an element of $\mathrm{GL}(1,q)\times\mathrm{GL}(2,q)$ with non-square determinant when q is odd. These are easily obtained in a similar way to the generators constructed in [**10**, Proposition 4.1], and we omit the details. The group P_3 is constructed in $O(\log q)$ field operations, and so ${}^{\wedge}P_2'$ is, too. □

The groups R_{s2} and R_{s3} in lines 5 and 6 of [**13**, Table I] are P_2 and P_3, respectively, which are constructed in Lemma 4.2. The group P_3 is not maximal in $\Omega^+(8,q)$ since, for all even $n\geqslant 3$, the group of type P_{n-1} is contained in groups in the two classes of type P_n in $\Omega^+(2n,q)$; see [**14**, Table 3.5.H]. (It is however the intersection of $\Omega^+(2n,q)$ with maximal subgroups of various extensions of $\Omega^+(2n,q)$.)

LEMMA 11.3. *A canonical copy of the groups $P_{2,3}'$ and $P_{2,4}'$ in lines 7 and 8 of [**13**, Table I] can be constructed in $O(\log q)$ field operations.*

Proof. These groups are images of $R_{s3}=P_3$ under the triality automorphism, but this does not enable us to construct them. However, $P_{2,3}'$ and $P_{2,4}'$ are conjugate in $\mathrm{GO}^+(8,q)$, so we only need to construct $P_{2,3}'$. This is a subgroup of $R_{s1}=P_1$ in line 1. Construct $P_{2,3}'$ by replacing the factor $\Omega^+(6,q)$ in P_1 by its maximal parabolic subgroup with structure $q^3{:}\mathrm{GL}(3,q)$ (q even) or $q^3{:}\frac{1}{2}\mathrm{GL}(3,q)$ (q odd). However, from the construction in Lemma 4.2, generating P_1 when q is odd requires S_6^+. To make $P_{2,3}'$, replace S_6^+ by an element of $\mathrm{GL}(3,q)$ with non-square determinant. The group P_1 can be constructed in $O(\log q)$ field operations by Proposition 4.2, and the modifications require $O(1)$ field operations. □

The groups in lines 9–14 of [**13**, Table I] are constructed in § 4 or are not geometric.

LEMMA 11.4. *A canonical copy of the groups $G_2(q)$ in lines 15–18 of [**13**, Table I] can be constructed in $O(\log q)$ field operations.*

Proof. These groups are subgroups of the conjugate of $\Omega(7,q)$ in line 9, whose construction is described in Lemma 4.3. Suppose first that q is odd. The four classes of groups are all conjugate in $\mathrm{CO}^+(8,q)$, so we need only construct one of them. When q is odd, $G_2(q)$ is generated by A and B below, each of which is a product of at most three matrices given in [**11**], and can be constructed in $O(1)$ field operations.

$$A=\begin{pmatrix}\zeta&0&0&0&0&0&0\\0&\zeta^{-1}&0&0&0&0&0\\0&0&\zeta^2&0&0&1&0\\0&0&0&1&0&0&0\\0&0&0&0&\zeta^{-2}&0&0\\0&0&0&0&0&\zeta&0\\0&0&0&0&0&0&\zeta^{-1}\end{pmatrix},\quad B=\begin{pmatrix}-1&0&1&0&0&0&0\\-1&0&0&0&0&0&0\\0&-1&0&-1&0&1&0\\0&-2&0&-1&0&0&0\\0&-1&0&0&0&0&0\\0&0&0&0&1&0&1\\0&0&0&0&1&0&0\end{pmatrix}.$$

Conjugate A and B in $O(\log q)$ field operations so that they preserve I_7 and use these in place of the generators of $\Omega(7,q)$ to get the group in line 15. The element $G_1^{\circ}(q)\oplus G_7^{\circ}(q)$ adjoined as an extra generator in Lemma 4.3 can be taken to be $-I_8$. So, the group we construct is actually $2\times G_2(q)$. This is then converted to preserve F_8^+ in $O(\log q)$ field operations.

For q even, there is only one class of groups of type $G_2(q)$. Generate $G_2(q)$ as a subgroup of $\mathrm{Sp}(6,q)$ by deleting the fourth rows and columns in the matrices A and B above to get

https://doi.org/10.1112/S1461157009000035 Published online by Cambridge University Press

A^* and B^*. Then use the method of Lemma 4.4, but replace the generators of $\mathrm{Sp}(6, q)$ by A^* and B^*. □

The groups in lines 19–21 of [**13**, Table I] are constructed in § 4.

LEMMA 11.5. *A canonical copy of the group N_2 in line* 22 *of* [**13**, *Table* I] *can be constructed in $O(\log q)$ field operations.*

Proof. This group is a subgroup of that in line 19, which arises roughly by replacing the factor $\Omega^+(6, q)$ by its maximal imprimitive subgroup of type $\mathrm{GL}(3, q).2$, as in Lemma 5.4. The construction in Lemma 4.3 of the group in line 19 requires the elements $S_6^+(q)$ and (when q is odd) $G_6^+(q)$. To construct N_2, we need corresponding elements of $\mathrm{SO}^+(6, q)$ and (for q odd) $\mathrm{GO}^+(6, q)$ that normalise the subgroup $\frac{1}{2}\mathrm{GL}(3, q)$. When q is odd, an element of $\mathrm{GL}(3, q)$ lying outside of $\frac{1}{2}\mathrm{GL}(3, q)$ has determinant 1 as an element of $\mathrm{GO}^+(6, q)$ and so replaces $S_6^+(q)$. The element J_6, which interchanges the two blocks of imprimitivity, replaces $S_6^+(q)$ when q is even and $G_6^+(q)$ when q is odd. □

The groups in lines 23–25 of [**13**, Table I] are constructed in § 4.

LEMMA 11.6. *A canonical copy of the group N_1 in line* 26 *of* [**13**, *Table* I] *can be constructed in $O(\log q)$ field operations.*

Proof. This is a subgroup of the group R_{-2} in line 23, whose construction is described in Lemma 4.3. The group N_1 arises roughly by replacing the factor $\Omega^-(6, q)$ by its maximal semilinear subgroup of type $\mathrm{GU}(3, q)$, by an identical approach to that described in Lemma 6.5. The construction of R_{-2} requires the elements $S_6^-(q)$ and (when q is odd) $G_6^-(q)$, and to construct N_1 we need corresponding elements of $\mathrm{SO}^-(6, q)$ and (for q odd) $\mathrm{GO}^-(6, q)$ that normalise the subgroup $\frac{1}{2}\mathrm{GU}(3, q)$. When q is odd, an element of $\mathrm{GU}(3, q)$ lying outside of $\frac{1}{2}\mathrm{GU}(3, q)$ has determinant 1 as an element of $\mathrm{GO}^-(6, q)$, and so can be used in place of $S_6^-(q)$. The element C in the proof of Lemma 6.5, which induces the field automorphism, replaces $S_6^-(q)$ when q is even and $G_6^-(q)$ when q is odd. □

The groups in lines 27–32 of [**13**, Table I] are constructed in §§ 4 and 7, whilst the groups in lines 33–50 are constructed in §§ 5 and 9.

LEMMA 11.7. *A canonical copy of the groups $N_4^1, \ldots, N_4^4$ in lines* 51–54 *of* [**13**, *Table* I] *can be constructed in $O(1)$ field operations.*

Proof. These groups are conjugate in $\mathrm{CO}^+(8, q)$, so we only need one of them. They have projective structure $[2^9]{:}\mathrm{PSL}(3, 2)$, and are subgroups of the groups in lines 33–50. Since they arise as subgroups of $2^8{:}\mathrm{Alt}(8)$, they are constructed by writing down generators of the subgroup $2^3{:}\mathrm{PSL}(3, 2) = \mathrm{AGL}(3, 2)$ of $\mathrm{Alt}(8)$, in its natural representation, and then using the construction of Lemma 5.3. □

The groups in lines 55–58 are constructed in § 5, and the groups in lines 59–60 are constructed in § 6.

LEMMA 11.8. *A canonical copy of the group N_3 in line* 61 *of* [**13**, *Table* I] *can be constructed in $O(\log q)$ field operations.*

Proof. This is a subgroup of the imprimitive group in line 58, for which a non-projective construction is given in Lemma 5.2. The generators of the linear group K are constructed from A_4^-, B_4^-, S_4^- and (when q odd) G_4^-. The group N_3 arises from the semilinear subgroup $\mathrm{P}\Omega^-(2, q^2).2 \cong D_{(q^2+1)/2}$ of $\mathrm{P}\Omega^-(4, q)$. We therefore first describe how to construct the appropriate subgroup of $\Omega^-(4, q)$, and then how to add the normalising elements.

Apply the homomorphism $\tau : \Omega^-(2, q^2) \to \Omega^-(4, q)$ to the two generators of $\Omega^-(2, q^2)$ as in § 6. If q is even, then $\tau(S_2^-(q^2))$ lies in $\Omega^-(4, q)$, as in the proof of Lemma 6.3. This suffices to generate $D_{(q^2+1)/2} \cong \mathrm{GO}_2^-(q^2)$. If q is odd, then $G_2^-(q^2)$ is a reflection, and $\mathrm{Det}(\tau(G_2^-(q^2))) = 1$. Since $-I \notin \Omega^-(4, q)$, one of $\pm\tau(G_2^-(q^2))$ has spinor norm 1, and can be chosen as the second generator for the subgroup of $\Omega^-(4, q)$.

To construct N_3, we need elements of $\mathrm{SO}^-(4, q)$ and (for q odd) $\mathrm{GO}^-(4, q)$ that normalise the subgroup $\Omega^-(2, q^2)$. For the former, when q is odd, choose $-I_4$. For the former, when q is even, and the latter, when q is odd, we need an element normalising and inducing the field automorphism of $\Omega^-(2, q^2)$, to produce an absolutely irreducible group. The element $C := \Gamma_B \oplus \Gamma_B$ does not normalise $\Omega^-(2, q^2)$. In $O(\log q)$ field operations, compute $X \in \mathrm{GL}(2, q^2)$, which conjugates $\Omega^-(2, q^2, (Q_2^-)^{\sigma_q})$ to $\Omega^-(2, q^2, Q_2^-)$. Then an appropriate replacement for $S_4^-(q)$ (q even) or $G_4^-(q)$ (q odd) is $C\tau(X)$, computed in $O(\log q)$ field operations. □

The groups in lines 62–64 and 67 are constructed in § 8. The remaining groups are not geometric.

References

1. M. Aschbacher, 'On the maximal subgroups of the finite classical groups', *Invent. Math.* 76 (1984) 469–514.
2. W. Bosma and J. J. Cannon (eds), *Handbook of Magma functions*, version 2.14 (2007) http://magma.maths.usyd.edu.au/magma/.
3. P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic complexity theory* (Springer, Berlin, 1997).
4. J. J. Cannon and D. F. Holt, 'Computing maximal subgroups of finite groups', *J. Symbol. Comput.* 37 (2004) 589–609.
5. D. Coppersmith and S. Winograd, 'Matrix multiplication via arithmetic progressions', *J. Symbol. Comput.* 9 (1990) 251–280.
6. R. H. Dye, 'A geometric characterization of the special orthogonal groups and the Dickson invariant', *J. London Math. Soc.* 15 (1977) 472–476.
7. B. Eick and A. Hulpke, 'Computing the maximal subgroups of a permutation group I', *Groups and computation III*, Ohio State University Research Institute Publications 8 (eds W. M. Kantor and À. Seress; de Gruyter, Berlin, 2001) 155–168.
8. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edn (Oxford University Press, Oxford, 1979).
9. G. Hiss and G. Malle, 'Low dimensional representations of quasi-simple groups', *LMS J. Comput. Math.* 4 (2001) 22–63 [Corrigenda: *LMS J. Comput. Math.* 5 (2002) 95–126].
10. D. F. Holt and C. M. Roney-Dougal, 'Constructing maximal subgroups of classical groups', *LMS J. Comput. Math.* 8 (2005) 46–79.
11. R. B. Howlett, L. J. Rylands and D. E. Taylor, 'Matrix generators for exceptional groups of Lie type', *J. Symbol. Comput.* 31 (2001) 429–445.
12. W. M. Kantor and Á. Seress, 'Black box classical groups', *Mem. Amer. Math. Soc.* 149 (2001).
13. P. B. Kleidman, 'The maximal subgroups of the finite 8-dimensional orthogonal groups $\mathrm{P}\Omega_8^+(q)$ and of their automorphism groups', *J. Algebra* 110 (1987) 173–242.
14. P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups* (Cambridge University Press, Cambridge, 1990).
15. F. Lübeck, 'Small degree representations of finite Chevalley groups in defining characteristic', *LMS J. Comput. Math.* 4 (2001) 135–169.
16. S. H. Murray and C. M. Roney-Dougal, 'Constructive homomorphisms for classical groups', CIRCA Preprint 2009/16, http://www-circa.mcs.st-and.ac.uk/pre-prints.php, *J. Symbol. Comput.*, to appear.
17. C. M. Roney-Dougal, 'Conjugacy of subgroups of the general linear group', *Experiment. Math.* 13 (2004) 151–163.
18. L. J. Rylands and D. E. Taylor, 'Matrix generators for the orthogonal groups', *J. Symbol. Comput.* 25 (1998) 351–360.
19. V. Strassen, 'Gaussian elimination is not optimal', *Numer. Math.* 13 (1969) 354–356.

20. D. E. TAYLOR, *The geometry of the classical groups* (Heldermann, Berlin, 1992).
21. H. ZASSENHAUS, 'On the spinor norm', *Arch. Math.* 13 (1962) 434–451.

Derek F. Holt
Mathematics Institute
University of Warwick
Coventry CV4 7AL
United Kingdom

d.f.holt@warwick.ac.uk

Colva M. Roney-Dougal
School of Mathematics and Statistics
University of St Andrews
St Andrews, Fife KY16 9SS
United Kingdom

colva@mcs.st-and.ac.uk