THE SPINOR NORM AND HOMOMORPHISM ALGORITHMS FOR CLASSICAL GROUPS

SCOTT H. MURRAY AND COLVA M. RONEY-DOUGAL

ABSTRACT. We investigate the structure of the normaliser N in $\mathrm{GL}_d(q)$ of the orthogonal group $\Omega^\epsilon_d(q)$, for $\epsilon \in \{\circ, +, -\}$. We develop algorithms to compute the spinor norm, and hence to construct a homomorphism from N with kernel $\Omega^\epsilon_d(q)$. These algorithms run in low-degree polynomial time (with a discrete log oracle in some cases) and are implemented in MAGMA. We also present similar algorithms for the normalisers of the other quasisimple classical groups.

1. INTRODUCTION

1.1. **Motivation.** The spinor norm is an epimorphism from the general orthogonal group $\mathrm{GO}^\epsilon_d(q)$ to $\mathbb{F}_2^+$, originally given by decomposing elements into a product of reflections. The matrices of determinant one and spinor norm zero form the omega group $\Omega^\epsilon_d(q)$. In this paper, we investigate the structure of the conformal group $\mathrm{CO}^\epsilon_d(q)$, which is the normaliser in $\mathrm{GL}_d(q)$ of $\Omega^\epsilon_d(q)$. We develop an algorithm to compute the spinor norm of an element of a general orthogonal group.

Given an element g of a conformal orthogonal group, we solve two main algorithmic tasks. First we efficiently compute the image of g under the natural quotient by the omega group, as an element of a polycyclic group. Secondly we find a canonical coset representative of g modulo the omega group. We also find the image of g in an extension of $\mathbb{F}_q^\times$, since this avoids a discrete logarithm call. We then solve analogous problems for the other classical groups.

Almost all of our algorithms run in a number of finite field operations that is low-degree polynomial in d and $\log q$: the exception is the homomorphism to the polycyclically presented group, which may require at most one discrete logarithm call (or two in the unitary case).

We have two main motivations for this work. First, the matrix group recognition project, which seeks to efficiently compute composition series for finite-dimensional matrix groups over finite fields [13]. The first stage of this computation is to find a geometry preserved by the group, in the sense of Aschbacher's Theorem [1], and use it to compute a normal subgroup and its quotient. These decomposition algorithms terminate when they reach groups that lie between a classical group in its natural representation and its normaliser in $\mathrm{GL}_d(q)$ (Case $\mathcal{C}_8$), or are almost simple modulo scalars (Case $\mathcal{C}_9$).

Algorithms to constructively recognise the quasisimple classical groups (and $\Omega^+_4(q)$) in their natural representation are known [4, 5, 14]. This paper resolves the problem that the $\mathcal{C}_8$ group may properly contain the quasisimple classical group. We do not consider field or graph automorphisms, as they cannot be represented linearly in the natural representation.

In [17] an algorithm is presented to calculate a chief series for a $\mathcal{C}_8$ group containing an orthogonal group as a normal subgroup, using our spinor norm algorithm. It analyses the projective group and then the scalars, rather than the quotient by the quasisimple group, and hence

Date: May 2, 2008.

2000 *Mathematics Subject Classification.* Primary 20G40; 20H30, 20-04.

The second author would like to acknowledge the support of the Nuffield Foundation.

to determine the index of the quasisimple group in the $\mathcal{C}_8$ group it is necessary to constructively recognise the simple classical group.

Our other motivation is element conjugacy algorithms, which seek to provide low-degree polynomial time conjugacy tests, as well as returning a conjugating element (when appropriate) and a standard class representative. They start by considering conjugacy in the normaliser in the general linear group of each classical group, and then consider subgroups. This paper describes some of these subgroups, whilst canonical coset representatives are needed to find class representatives. Note that constructive recognition is not required for this application.

1.2. **Notation and forms.** Let p be a prime and let q be a power of p. Let $\mathbb{F}_q$ be the field of size q. Write $\mathbb{F}_q^\times$ for the multiplicative group of nonzero field elements, and $\mathbb{F}_q^{\times 2}$ for the nonzero squares. We assume that $\mathbb{F}_{q^2}$ is constructed as $\mathbb{F}_p(\zeta)$, where ζ is the root of the Conway polynomial [11]. See Section 8 for a brief discussion on avoiding this assumption for large fields. Thus ζ is a primitive element of $\mathbb{F}_{q^2}$ and $\xi = \zeta^{q+1}$ is a primitive element of $\mathbb{F}_q$.

Let $V = \mathbb{F}_q^d$ be the d-dimensional row space over $\mathbb{F}_q$, with standard basis $[v_1, \ldots, v_d]$. We assume that d is at least 3 and that d is even if q is even. By $\mathrm{diag}[a_1, a_2, \ldots, a_d]$ we mean the $d \times d$ matrix with entry a_i in position (i, i) and 0 elsewhere. By $\mathrm{antidiag}[a_1, a_2, \ldots, a_d]$ we mean the $d \times d$ matrix with entry a_i in position $(i, d-i+1)$ and 0 elsewhere.

A *symmetric bilinear form* is a map $\beta : V \times V \to \mathbb{F}_q$ such that $\beta(v, w) = \beta(w, v)$, $\beta(u+v, w) = \beta(u, w) + \beta(v, w)$, and $\beta(\lambda v, w) = \lambda\beta(v, w)$ for all $u, v, w \in V$ and $\lambda \in \mathbb{F}_q$. A *quadratic form* is a map $Q : V \to \mathbb{F}_q$ such that $Q(\lambda v) = \lambda^2 Q(v)$ and $\beta(u, v) = Q(u+v) - Q(u) - Q(v)$ is symmetric bilinear, for all $u, v \in V$ and $\lambda \in \mathbb{F}_q$. We call β the corresponding *orthogonal form*: if q is odd then we can recover Q from β via $Q(v) = \beta(v, v)/2$.

The form β is *nondegenerate* if $\beta(v, V) \neq 0$ for all $v \in V \setminus \{0\}$. The form Q is *nondegenerate* when $Q(v) \neq 0$ for all $v \neq 0$ such that $\beta(v, V) = 0$. When q is odd, Q is nondegenerate if and only if β is nondegenerate. We assume throughout that all quadratic forms are nondegenerate. A vector v is *singular* if $Q(v) = 0$.

We define an upper triangular $d \times d$ matrix M over $\mathbb{F}_q$ such that for $v = (a_1, \ldots, a_d)$,

$$Q(v) = \sum_{1 \leq i \leq j \leq d} m_{ij} a_i a_j.$$

Let $F = (\beta(v_i, v_j))_{d \times d}$, then $\beta(u, v) = uFv^{\mathrm{Tr}}$ and a short calculation shows that $F = M + M^{\mathrm{Tr}}$.

Two quadratic forms Q_1 and Q_2 on V are *isometric* if there exists $g \in \mathrm{GL}_d(q)$ such that $Q_1(vg) = Q_2(v)$ for all $v \in V$; they are *similar* if there exist $g \in \mathrm{GL}_d(q)$ and $\lambda \in \mathbb{F}_q^\times$ such that $Q_1(vg) = \lambda Q_2(v)$ for all $v \in V$. If two forms are similar then the groups preserving each form are conjugate in the general linear group.

2. Canonical forms and groups

In this section, we define a set of canonical forms, and the groups that preserve them.

Every element of $\mathbb{F}_{q^2}$ can be written as $a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1}$, where $p^m = q^2$ and $a_i \in \{0, \ldots, p-1\}$. This induces an ordering on $\mathbb{F}_{q^2}$ by lexicographically ordering the coefficients.

Theorem 2.1. [8, Theorem 8.12] *A root in $\mathbb{F}_{q^2}$ for a quadratic polynomial with coefficients in $\mathbb{F}_q$ can be found by a Las Vegas algorithm in $O(\log q)$ field operations.*

We can fix a canonical root of a quadratic by taking the smaller root with respect to our canonical ordering on $\mathbb{F}_{q^2}$. Similarly, we determine whether $a \in \mathbb{F}_q^{\times 2}$ and if so, define a canonical square root $\sqrt{a}$. If $a = \xi^{2i}$, then we write $a^{1/2}$ for ξ^i: this may differ by a sign from $\sqrt{a}$. For q even, the square root of a is unique and can be computed as $a^{q/2}$ in $O(\log q)$ field operations.

While discussing canonical field elements, we include a result which we will need in Section 6.

Proposition 2.2. *Let $a \in \mathbb{F}_q^\times$. A canonical solution of the norm equation $x^{q+1} = a$ over $\mathbb{F}_{q^2}$ can be found in Las Vegas $O(\log q + \log^2 p)$ field operations.*

Proof. We construct a solution to the norm equation in three cases. The first is $a \in \mathbb{F}_q^{\times 2}$ (which includes all even q). Let $\sqrt{a} = x$, then $x^{q+1} = x^2 = a$.

The second case is $a \notin \mathbb{F}_q^{\times 2}$ and $q \equiv 1 \pmod 4$. Now $-1 \in \mathbb{F}_q^{\times 2}$, so $-a \notin \mathbb{F}_q^{\times 2}$. Hence $x = \sqrt{-a} \in \mathbb{F}_{q^2}$ satisfies $x^{q+1} = (x^2)^{(q+1)/2} = (-a)(-a)^{(q-1)/2} = a$, as required.

The final case is $a \notin \mathbb{F}_q^{\times 2}$ and $q \equiv 3 \pmod 4$. Now $-a \in \mathbb{F}_q^{\times 2}$, so let $b = \sqrt{-a}$ and write $p + 1 = 2^m s$ for s odd. Calculate $c \in \mathbb{F}_p$ in $O(\log^2 p)$ field operations by

$$c_1 = 0; \qquad c_{i+1} = \left(\frac{c_i + 1}{2}\right)^{\frac{p+1}{4}} \ (i = 1, \ldots, m-2); \qquad c = \left(\frac{c_{m-1} - 1}{2}\right)^{\frac{p+1}{4}}.$$

By [2], the polynomial $g(X) = X^2 - 2cX - 1$ is irreducible over $\mathbb{F}_q$. Hence $-ag(X/b) = X^2 - 2bcX + a$ is also irreducible and its roots in $\mathbb{F}_{q^2}$ have norm a. □

Proposition 2.3. *Given $\zeta \in \mathbb{F}_{q^2}$, the following canonical elements can be constructed:*

1. *for q odd, a nonsquare $\delta \in \mathbb{F}_q$ in $O(\log q)$ operations;*
2. *for q odd, $\gamma \in \mathbb{F}_q$ such that γ and $1 - 4\gamma$ are nonsquares in $O(\log q)$ operations;*
3. *for q even, $\gamma \in \mathbb{F}_q$ such that $X^2 + X + \gamma$ is irreducible over $\mathbb{F}_q$ in $O(\log^2 q)$ operations;*
4. *for q odd, $\nu \in \mathbb{F}_q$ such that $1 + \nu^2$ is nonsquare, in $O(\log q)$ operations.*

Proof. For (1), take $\delta = \xi = \zeta^{q+1}$.

For (2), note that $\zeta + \zeta^q \neq 0$, as otherwise $\zeta^{q-1} = -1 = \zeta^{(q^2-1)/2}$. Set $\gamma = \xi/(\zeta + \zeta^q)^2$, then $\gamma \in \mathbb{F}_q$ because $\gamma^q = \gamma$. Also, $\gamma \notin \mathbb{F}_q^{\times 2}$ because $\xi \notin \mathbb{F}_q^{\times 2}$. Finally,

$$1 - 4\gamma = 1 - \frac{4\zeta\zeta^q}{(\zeta + \zeta^q)^2} = \left(\frac{\zeta - \zeta^q}{\zeta + \zeta^q}\right)^2 \notin \mathbb{F}_q^{\times 2},$$

since $\frac{\zeta - \zeta^q}{\zeta + \zeta^q}$ is taken to its negative under taking qth powers, and so is not in $\mathbb{F}_q$.

For (3), let $q = 2^m$. If m is odd, let $\delta = 1$. Otherwise, let $m = 2^r s$ for s odd. Define a_i recursively: $a_0 = 1$, and a_{i+1} is the canonical root of $X^2 + X + a_i$ in $\mathbb{F}_q$. Define δ to be the first a_j for which $X^2 + X + a_j$ is irreducible.

Define $T : \mathbb{F}_q \to \mathbb{F}_q$ by $T(x) = x^2 + x$, and note that $T(a_i) = a_i^2 + a_i = a_{i-1}$ for $i \geq 1$. It is easy to show that $T^{2^i}(x) = x^{2^{2^i}} + x$ for all i. Now suppose $a = a_{2^r+1} \in \mathbb{F}_q$ exists. Then $T^{2^r+1}(a) = 1$, so $T^{2^{r+1}}(a) = T^{2^{r+1}-2^r-1}(1) = 0$, and so $a^{2^{2^{r+1}}} = a$. Hence $a \in \mathbb{F}_{2^{2^{r+1}}}$, which intersects $\mathbb{F}_q$ in $\mathbb{F}_{2^{2^r}}$. This implies that $a^{2^{2^r}} = a$, so $T^{2^r}(a) = 0$, which contradicts $T^{2^r+1}(a) = 1$. Therefore $j \leq 2^r \leq \log q$.

For (4), note that $4\zeta^{q+1}/(\zeta - \zeta^q)^2 \in \mathbb{F}_q^{\times 2}$. Let $\nu \in \mathbb{F}_q$ be its square root, then $1 + \nu^2 \notin \mathbb{F}_q^{\times 2}$. □

Definition 2.4 (Standard quadratic forms)**.** *We denote these forms by Q^ϵ, $\epsilon \in \{\circ, +, -\}$.*

- $\circ$ **type:** *$d = 2m + 1$ and V has basis $(e_1, \ldots, e_m, x, f_m, \ldots, f_1)$ with $Q^\circ(e_i) = Q^\circ(f_j) = 0$, $\beta^\circ(e_i, f_j) = \delta_{ij}$, $\beta^\circ(e_i, x) = \beta^\circ(f_i, x) = 0$ and $Q^\circ(x) = \delta$.*
- $+$ **type:** *$d = 2m$ and V has basis $(e_1, \ldots, e_m, f_m, \ldots, f_1)$ with $Q^+(e_i) = Q^+(f_j) = 0$ and $\beta^+(e_i, f_j) = \delta_{ij}$.*
- $-$ **type:** *$d = 2m + 2$ and V has basis $(e_1, \ldots, e_m, x, y, f_m, \ldots, f_1)$ with $Q^-(e_i) = Q^-(f_j) = 0$, $\beta^-(e_i, f_j) = \delta_{ij}$, $\beta^-(a, b) = 0$ for $a \in \{e_i, f_j\}$, $b \in \{x, y\}$, $(Q^-(x), Q^-(y), \beta^-(x, y)) = (1, \gamma, 1)$.*

Proposition 2.5. *Every nondegenerate quadratic form is similar to one of the forms given in Definition 2.4. When the dimension is even, the + type form is not similar to the − type form.*

Proof. This is well-known: see for instance [19, Chapter 11]. □

For odd dimension and characteristic, there are two nonisometric classes of forms, which are similar. In all other cases, forms are similar if and only if they are isometric.

Define the *conformal orthogonal*, *(general) orthogonal*, and *special orthogonal* groups by

$$\mathrm{CO}_d(q,Q) = \{g \in \mathrm{GL}_d(q) \mid \text{there exists } \lambda \in \mathbb{F}_q^\times \text{ such that } Q(vg) = \lambda Q(v) \text{ for all } v \in \mathbb{F}_q^d\},$$
$$\mathrm{GO}_d(q,Q) = \{g \in \mathrm{GL}_d(q) \mid Q(vg) = Q(v) \text{ for all } v \in \mathbb{F}_q^d\},$$
$$\mathrm{SO}_d(q,Q) = \mathrm{GO}_d(q,Q) \cap \mathrm{SL}_d(q).$$

If $Q = Q^\epsilon$, we denote these groups by $\mathrm{CO}_d^\epsilon(q)$, and so on. If q is odd, these groups can also be defined in terms of β. Some authors denote $\mathrm{GO}_d^\epsilon(q)$ by $\mathrm{O}_d^\epsilon(q)$.

3. Discriminants, the τ map, the spinor norm, and reflections

Define $\iota : \mathbb{F}_q^\times \to \mathbb{F}_2^+$ by $\iota(x) = 0$ when $x \in \mathbb{F}_q^{\times 2}$, and $\iota(x) = 1$ otherwise. The *discriminant* of Q is $\iota(\det(F))$: this is constant on isometry types of forms. Define $\tau : \mathrm{CO}_d(q,Q) \to \mathbb{F}_q$ by $Q(vx) = \tau(x)Q(v)$ for all $v \in V$. It is well-known (see for example [12, 2.1.2]) that τ is a homomorphism with kernel $\mathrm{GO}_d(q,Q)$.

We give the most computationally useful of the equivalent definitions of the spinor norm:

Definition 3.1 (Spinor norm)**.**

(1) *Let q be odd and let F be the matrix of the orthogonal form corresponding to Q. Let*
$$A(g) = \{v \in V \ : \ \exists\ n \text{ s.t. } v(1+g)^n = 0\}, \quad B(g) = \textstyle\bigcap_{n=1}^{\infty} V(1+g)^n, \quad \text{and}$$
$$\alpha(g) = \det\left(F|_{A(g)}\right) \det\left(\left.\tfrac{1+g}{2}\right|_{B(g)}\right).$$
The spinor norm *of g is $\mathrm{sp}(g) = \iota(\alpha(g))$.*

(2) *For q even, the* spinor norm *of g is $\mathrm{sp}(g) = \mathrm{rank}(1+g) \bmod 2$.*

Lemma 3.2. [7, 20]

(1) sp *is a homomorphism from $\mathrm{GO}_d(q,Q)$ onto $\mathbb{F}_2^+$.*
(2) $\mathrm{sp}(-1) = 0$ *if and only if the discriminant of Q is zero.*

Definition 3.3. $\Omega_d(q,Q) = \mathrm{SO}_d(q,Q) \cap \ker(\mathrm{sp})$.

We define the omega group as in [12], however it is common in the literature to define it as the derived group of $\mathrm{SO}_d(q,Q)$. These definitions agree provided that $d \geq 3$ and $(d,q,\epsilon) \neq (4,2,+)$. It is well-known (see for instance [12, Cor 2.10.4] that $N_{\mathrm{GL}_d(q)}(\Omega_d(q,Q)) = \mathrm{CO}_d(q,Q)$.

Let $v \in V$ be nonsingular, so that $Q(v) \neq 0$. The *reflection* in v is

$$\mathrm{refl}_v : V \to V, \quad u \mapsto u - \beta(u,v)v/Q(v).$$

Lemma 3.4. *Let Q be a nondegenerate quadratic form on V.*

(1) *All reflections are elements of $\mathrm{GO}_d(q,Q)$.*
(2) *All reflections have determinant -1 and order 2.*
(3) *For q odd and $v \in V$ nonsingular, $\mathrm{sp}(\mathrm{refl}_v) = 0$ if and only if $Q(v) \in \mathbb{F}_q^{\times 2}$.*
(4) *For q even and $v \in V$ nonsingular, $\mathrm{sp}(\mathrm{refl}_v) = 1$.*
(5) *For q odd and $u, v \in V$ nonsingular, $\Omega_d(q,Q)\,\mathrm{refl}_u = \Omega_d(q,Q)\,\mathrm{refl}_v$ if and only if*
$$\iota(Q(u)) = \iota(Q(v)).$$

Proof. (1) is an easy calculation. (2) is true since refl_v negates elements of $\langle v\rangle$ and fixes elements of $U = \{u \in V \mid (u,v) = 0\}$. For (3) and (4), let $g = \mathrm{refl}_v$. For q odd, $A(g) = \langle v\rangle$ and $B(g) = U$, so $\alpha(g) = Q(v)$. For q even, $\mathrm{rank}(1+g) = 1$. (5) follows from (3) and Lemma 3.2. □

4. Presentations

We now give an explicit presentation for the quotient of $\mathrm{CO}^\epsilon_d(q)$ by $\Omega^\epsilon_d(q)$. For the projective groups, see [12, §§2.5–2.8]. Recall $d \geq 3$ throughout and if q is even then d is even.

Define $v_0 = e_1 + f_1$ so that $Q^\epsilon(v_0) = 1$. For q odd, let δ be as in Proposition 2.3 and define $v_1 = e_1 + \delta f_1$, so that $Q^\epsilon(v_1) = \delta$. We can now define our canonical reflections

$$R_0 = \mathrm{refl}_{v_0} \quad \text{and} \quad R_1 = \mathrm{refl}_{v_1}.$$

For q odd, $\mathrm{sp}(R_i) = i$ for $i \in \mathbb{F}_2^+$. For q even, we only define R_0. Define the coset $r_i = \Omega^\epsilon_d(q)R_i$.

Theorem 4.1.

(1) *If q is odd, then $\mathrm{GO}^\epsilon_d(q) = \langle R_0, R_1, \Omega^\epsilon_d(q)\rangle$ and $\mathrm{SO}^\epsilon_d(q) = \langle R_0R_1, \Omega^\epsilon_d(q)\rangle$. Furthermore, $\mathrm{GO}^\epsilon_d(q)/\Omega^\epsilon_d(q)$ has presentation*

$$\langle r_0, r_1 \mid r_0^2 = r_1^2 = (r_0r_1)^2 = 1\rangle.$$

(2) *If q and d are even, then $\mathrm{GO}^\pm_d(q) = \langle R_0, \Omega^\pm_d(q)\rangle$, and $\mathrm{GO}^\pm_d(q)/\Omega^\pm_d(q)$ has presentation*

$$\langle r_0 \mid r_0^2 = 1\rangle.$$

Proof. (1) The group defined by the given presentation has order 4. By [12, §2.1], the index $[\mathrm{GO}^\epsilon_d(q) : \Omega^\epsilon_d(q)] = 4$, so it suffices to show that r_0 and r_1 satisfy the given relations, and that they are distinct and nontrivial. The relations $r_0^2 = r_1^2 = 1$ hold by Lemma 3.4.2, which also shows that $r_0 \neq 1 \neq r_1$. If $g = (R_0R_1)^2$ then $\det(g) = 1$, and $\mathrm{sp}(g) = 2\,\mathrm{sp}(R_0R_1) = 0$, so $(r_0r_1)^2 = 1$. Finally, $\mathrm{sp}(R_0) \neq \mathrm{sp}(R_1)$ so $r_0 \neq r_1$ by Lemma 3.4.5.
(2) This is similar, since $[\mathrm{GO}^\epsilon_d(q) : \Omega^\epsilon_d(q)] = 2$ for q even [12, §2.1]. □

Let $\lambda \in \mathbb{F}_q^\times$. For even q, define $C^\pm(\lambda) = \lambda^{q/2}I_d$. For odd q, define

$$\begin{aligned}
C^\circ(\lambda) &= \lambda^2 I_m \oplus (\lambda) \oplus I_m, && \text{for } d = 2m+1 \text{ odd};\\
C^+(\lambda) &= \lambda I_m \oplus I_m, && \text{for } d = 2m \text{ even};\\
C^-(\lambda) &= \lambda^2 I_m \oplus \lambda I_2 \oplus I_m, && \text{for } d = 2m+2 \text{ even};\\
C_0^- &= \gamma I_m \oplus \mathrm{antidiag}[1,\gamma] \oplus I_m && \text{for } d = 2m+2 \text{ even}.
\end{aligned}$$

It is easy to check that $C^\epsilon(\lambda) \in \mathrm{CO}^\epsilon_d(q)$ and $C_0^- \in \mathrm{CO}^-_d(q)$. Note that $\tau(C^\epsilon(\lambda)) = \lambda^2$ when q is odd and ϵ is $\circ$ or $-$; whilst $\tau(C^\epsilon(\lambda)) = \lambda$ in all other cases. Also, we check that

$$\begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 2\gamma \end{pmatrix}\begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix} = \gamma\begin{pmatrix} 2 & 1 \\ 1 & 2\gamma \end{pmatrix},$$

and so $\tau(C_0^-) = \gamma$. Let $c(\lambda)$ be the coset $\Omega^\epsilon_d(q)C^\epsilon(\lambda)$, and let c_0 be $\Omega^-_d(q)C_0^-$.

Theorem 4.2.

(1) *If q is even, then $\mathrm{CO}^\pm_d(q) = \langle R_0, C^\pm(\xi), \Omega^\pm_d(q)\rangle$. Furthermore, $\mathrm{CO}^\pm_d(q)/\Omega^\pm_d(q)$ has presentation $G^\pm(q)$ with generators r_0, $c(\lambda)$ for all $\lambda \in \mathbb{F}_q^\times$ and relations*

$$c(\lambda)c(\mu) = c(\lambda\mu),\ r_0^2 = 1,\ r_0c(\lambda) = c(\lambda)r_0.$$

(2) *The group* $\mathrm{CO}_d^\circ(q) = \langle R_0, R_1, C^\circ(\xi), \Omega_d^\circ(q)\rangle$. *Furthermore,* $\mathrm{CO}_d^\circ(q)/\Omega_d^\circ(q)$ *has presentation* $G^\circ(q)$ *with generators* r_0, r_1, $c(\lambda)$ *for all* $\lambda \in \mathbb{F}_q^\times$ *and relations*

$$c(\lambda)c(\mu) = c(\lambda\mu),\ r_0^2 = r_1^2 = (r_0r_1)^2 = 1,\ r_ic(\lambda) = c(\lambda)r_i,\ c(-1) = r_1.$$

(3) *If* q *is odd then* $\mathrm{CO}_d^+(q) = \langle R_0, R_1, C^+(\xi), \Omega_d^+(q)\rangle$. *Furthermore,* $\mathrm{CO}_d^+(q)/\Omega_d^+(q)$ *has presentation* $G^+(q)$ *with generators* r_0, r_1, $c(\lambda)$ *for all* $\lambda \in \mathbb{F}_q^\times$ *and relations*

$$c(\lambda)c(\mu) = c(\lambda\mu),\ r_0^2 = 1,\ r_1^2 = (r_0r_1)^2 = 1,\ r_i^{c(\lambda)} = r_{(i+\iota(\lambda)) \bmod 2}.$$

(4) *If* q *is odd then* $\mathrm{CO}_d^-(q) = \langle R_0, R_1, C^-(\xi), C_0^-, \Omega_d^-(q)\rangle$. *Furthermore,* $\mathrm{CO}_d^-(q)/\Omega_d^-(q)$ *has presentation* $G^-(q)$ *with generators* r_0, r_1, c_0, $c(\lambda)$ *for all* $\lambda \in \mathbb{F}_q^\times$ *and relations*

$$c(\lambda)c(\mu) = c(\lambda\mu),\ r_0^2 = r_1^2 = (r_0r_1)^2 = 1,\ r_ic(\lambda) = c(\lambda)r_i,$$
$$r_i^{c_0} = r_{(i+1) \bmod 2},\ c_0c(\lambda) = c(\lambda)c_0,\ c_0^2 = c(\gamma),\ c(-1) = r_0r_1.$$

Proof. The kernel of τ on $\mathrm{CO}_d^\epsilon(q)$ is $\mathrm{GO}_d^\epsilon(q)$, and its image is $\mathbb{F}_q^\times$ if d is even, and $\mathbb{F}_q^{\times 2}$ otherwise [12, §2.1]. For d odd, $\tau(C^\circ(\xi)) = \xi^2$ generates $\mathbb{F}_q^{\times 2}$. If ϵ is $+$ or q is even, then $\tau(C^\epsilon(\xi)) = \xi$ generates $\mathbb{F}_q^\times$. Finally, if ϵ is $-$ and q is odd, then $\tau(C^-(\xi)) = \xi^2$ and $\tau(C_1^-) = \gamma$ generate $\mathbb{F}_q^\times$, since γ is nonsquare. Hence by Theorem 4.1, $\mathrm{CO}_d^\epsilon(q)$ is generated by the given elements.

For q even, $G^\pm(q) = \langle c(\xi)\rangle \times \langle r_0\rangle \cong \mathbb{F}_q^\times \times \mathbb{F}_2^+$. The group $G^\circ(q)$ is a direct product of $\langle r_0\rangle \cong \mathbb{F}_2^+$ and $\langle c(\xi)\rangle \cong \mathbb{F}_q^\times$. For q odd, $G^+(q)$ is an extension of $\langle r_0, r_1\rangle \cong (\mathbb{F}_2^+)^2$ by $\langle c(\xi)\rangle \cong \mathbb{F}_q^\times$, whilst $G^-(q)$ is an extension of $\langle r_0, r_1\rangle \cong (\mathbb{F}_2^+)^2$ by $\langle c(\xi), c_1\rangle \cong \mathbb{F}_q^\times$. Hence $G^\epsilon(q)$ has the same order as $\mathrm{CO}_d^\epsilon(q)/\Omega_d^\epsilon(q)$ [12, § 2.1]. It therefore suffices to show that the relations hold.

All relations involving only r_0 and r_1 hold by Theorem 4.1. For the relations involving r_0 or r_1 conjugated by $c(\lambda)$ or c_0, note that $\mathrm{refl}_v^g = \mathrm{refl}_{vg}$ for $v \in V$ and $g \in \mathrm{CO}_d^\epsilon(q)$. For q even, all reflections are in the same coset of $\Omega_d^\pm(q)$, and so $r_0^{c(\lambda)} = r_0$. For q odd, $\iota(Q(vg)) = \iota(Q(v)) + \iota(\tau(g))$. For the relations involving products and powers of $c(\lambda)$ and c_0, one checks that $C^\epsilon(\lambda)C^\epsilon(\mu) = C^\epsilon(\lambda\mu)$ and so $c(\lambda)c(\mu) = c(\lambda\mu)$. Now, $C_{2m+1}^\circ(-1) = I_m \oplus (-1) \oplus I_m = \mathrm{refl}_x$, and since $Q^\circ(x) = \delta$ we deduce $c(-1) = r_1$. Finally, $C^-(\lambda)$ commutes with C_0^-; $(C_0^-)^2 = C^-(\gamma)$; and $C^-(-1) = I_m \oplus -I_2 \oplus I_m = \mathrm{refl}_x \mathrm{refl}_y$, so $c(-1) = r_0r_1$. □

By setting $c = c(\xi)$, or $c = c(\sqrt{\xi\gamma^{-1}})c_0$, we get equivalent PC presentations:

Corollary 4.3. *The group* $\mathrm{CO}_d^\circ(q)/\Omega_d^\circ(q)$ *has presentation*

$$H^\circ(q) = \langle r_0, r_1, c \mid r_0^2 = r_1^2 = (r_0r_1)^2 = 1, r_0^c = r_0, r_1^c = r_1, c^{(q-1)/2} = r_1\rangle.$$

If q *is odd then* $\mathrm{CO}_d^\pm(q)/\Omega_d^\pm(q)$ *has presentation*

$$H^\pm(q) = \langle r_0, r_1, c \mid r_0^2 = r_1^2 = (r_0r_1)^2 = 1, r_0^c = r_1, r_1^c = r_0, c^{q-1} = 1\rangle.$$

If q *is even then* $\mathrm{CO}_d^\pm(q)/\Omega_d^\pm(q)$ *has presentation*

$$H^\pm(q) = \langle r_0, c \mid r_0^2 = 1, r_0^c = r_0, c^{q-1} = 1\rangle.$$

From the theory of PC presentations [9], an element of $H^\epsilon(q)$ can be written uniquely as:

qd **odd:** $r_0^i r_1^j c^k$ with $i, j \in \{0, 1\}$ and $k \in \{0, \ldots, (q-3)/2\}$;
q **odd,** d **even:** $r_0^i r_1^j c^k$ with $i, j \in \{0, 1\}$ and $k \in \{0, \ldots, q-2\}$;
q **even:** $r_0^i c^k$ with $i \in \{0, 1\}$ and $k \in \{0, \ldots, q-2\}$.

5. Algorithms for orthogonal groups

We start this section by introducing various basic algorithms for later use. Recall the results about finite fields in Section 2. We do not assume the availability of discrete logarithms or primitive field elements, unless explicitly stated.

We define ω to be the exponent of matrix multiplication, so that multiplication of two $d \times d$ matrices is $O(d^\omega)$ field operations. The current best known bounds for ω are $2 \leq \omega \leq 2.236$. The following results on complexity of matrix operations are standard and can be found in [6].

Theorem 5.1. *Computing the rank, the nullspace, the characteristic polynomial and the determinant of a $d \times d$ matrix over $\mathbb{F}_q$ requires $O(d^\omega)$ field operations.*

A quadratic form Q is given by its matrix M (or equivalently F for odd q). Given vectors $u, v \in V$, we can compute $Q(v)$ or $\beta(u, v)$ in $O(d^2)$ field operations.

There is an algorithm in [10] to construct an isometry between symmetric bilinear forms in Las Vegas $O(d^3 + d \log q)$ field operations for q odd. However, it returns different isometries if called more than once. Since we require an isometry to construct coset representatives, we now present a canonical isometry algorithm. For odd d, if two forms are similar rather than isometric, then replacing one form matrix by a nonsquare scalar multiple will produce two isometric forms without changing the groups concerned.

Theorem 5.2. *For odd q, let $\zeta \in \mathbb{F}_{q^2}$ and isometric forms F and F_1 be given. We construct a canonical isometry between F and F_1 in Las Vegas $O(d^3 + d \log q)$ field operations.*

Proof. We show how to convert F into a diagonal matrix that for d odd is either I_d or ξI_d, and for d even is either I_d or $\mathrm{Diag}[1, \ldots, 1, \xi]$, depending on the discriminant of F.

By replacing v_1 by v_j or $v_1 + v_j$ for some j if necessary (an $O(d)$ operation) we may assume without loss of generality that $f_{11} \neq 0$. For $2 \leq i \leq d$ we replace v_i by $f_{1i}^{-1} v_i - f_{11}^{-1} v_1$. For each i this requires $O(d)$ field operations, so $O(d^2)$ in total. After this, if $i \neq 1$ then $f_{1i} = f_{i1} = 0$. Repeating for $2 \leq i \leq d$ we transform F into a diagonal matrix in $O(d^3)$ field operations.

In Las Vegas $O(d \log q)$ field operations we transform F to a diagonal matrix whose diagonal entries are equal to 1 if $f_{ii} \in \mathbb{F}_q^{\times 2}$, or ξ if $f_{ii} \notin \mathbb{F}_q^{\times 2}$.

We finish by transforming the diagonal entries in pairs from ξ to 1, unless d is odd in which case if there are an even number of 1s we transform the diagonal entries in pairs from 1 to ξ. To do this we select two equal entries, say f_{ii} and f_{jj}. We replace v_i by $v_i + \nu v_j$ and v_j by $\nu v_j - v_i$, where ν is from Proposition 2.3.4. Since $\nu^2 \neq -1$, these two vectors are linearly independent, and a short calculation shows that this has the effect of multiplying f_{ii} and f_{jj} by $(1 + \nu^2)$, a nonsquare. To finish, we transform the new entries to either 1 or ξ as before. □

Proposition 5.3. *Given Q, a canonical nonsingular vector v can be constructed in $O(d)$ field operations. For odd q, given F and ζ, canonical vectors w_0, w_1 with $Q(w_0) = 1$ and $Q(w_1) = \delta$ can be constructed in $O(d^2 + \log q)$ field operations. Reflections in these vectors can then be constructed in $O(d^2)$ field operations.*

Proof. If we require only v we look for the smallest i such that $m_{ii} \neq 0$, and let $v = v_i$. If none exists, let j be minimal subject to $m_{1j} \neq 0$, and let $v = v_1 + v_j$.

To find w_0, w_1 we first check the diagonal entries of M to see if one is square and the other nonsquare. If so, we are done. Failing this we follow a similar procedure to Theorem 5.2 to find an isometry such that the top 3×3 block of F is diagonal: this requires $O(d)$ operations. If at this stage at least one entry is square and another is nonsquare, we are done. So assume without loss of generality that all are squares. We follow Theorem 5.2 to make an isometry mapping

all three entries to 1 in Las Vegas $O(\log q)$. Let X be the resulting sequence of isometries. Construct ν from Proposition 2.3 in $O(\log q)$ operations. Then v_1X and $(v_1+\nu v_2)X$ are vectors of square and nonsquare norm.

To calculate $\mathrm{refl}\, w$, we first compute $Q(w)$ in $O(d^2)$ operations. Next we note that wFv_i^{Tr} can be computed in $O(d)$, as Fv_i is the ith row of F. Then row i of $\mathrm{refl}\, w$ is $v_i-(wFv_i^{\mathrm{Tr}})Q(w)^{-1}v$. □

Corollary 5.4. *Let Q be a nondegenerate quadratic form of dimension d over the field of size q. Let g be an element of $\mathrm{GO}_d(q,Q)$. Then $\tau(g)$ can be computed in $O(d^2)$ field operations.*

Proof. Let v be a nonsingular vector, as in Proposition 5.3. Then $\tau(g)=Q(vg)/Q(v)$ can be computed in $O(d^2)$ field operations. □

Recall $A(g)$ and $B(g)$ from Section 3. The following lemma is elementary linear algebra:

Lemma 5.5. *Let $g\in \mathrm{GL}_d(q)$, and write the characteristic polynomial of $g+1$ in the form $x^ef(x)$ with $f(0)\neq 0$. Then $A(g)=\ker((g+1)^e)$ and $B(g)=\ker(f(g+1))$.*

Here is the main result on computing the spinor norm.

Theorem 5.6. *Let $g\in \mathrm{GO}_d(q,Q)$, then $\mathrm{sp}(g)$ can be found in $O(d^\omega)$ field operations if q is even, and Las Vegas $O(d^3+\log q)$ field operations if q is odd.*

Proof. If q is even we calculate $\mathrm{sp}(g)=\mathrm{rank}(g-I_d)$ in $O(d^\omega)$ operations by Theorem 5.1.

If q is odd, we compute $a:=g+I_d$ in $O(d)$. We then compute the characteristic polynomial $C(a)$ in $\mathbb{F}_q[x]$ of a in $O(d^\omega)$ field operations by Theorem 5.1. We factorise $C(a)=x^ep(a)$, where $p(1)\neq 0$, in $O(d)$ operations.

Computing a^e, where $e\leq d$, requires $O(d^\omega\log d)$ field operations. We compute $A(g)$ in $O(d^\omega)$ operations as the nullspace of a^e by Lemma 5.5. We find $d_A:=\det(F\mid_{A(g)})$ in $O(d^\omega)$.

If $e<d$ then following [14] we conjugate a to Frobenius normal form in $O(d^3)$ operations [18]. After this, matrix multiplication is $O(d^2)$, so we evaluate $p(a)$ in $O(d^3)$ field operations. We then compute $B(g)$, namely the nullspace of $p(a)$, in $O(d^\omega)$. Calculating $d_B:=\det(a/2\mid_{B(g)})$ requires $O(d^\omega)$ field operations.

Finally we test whether d_Ad_B is a square in Las Vegas $O(\log q)$ field operations. □

Next we consider the natural homomorphism from $\mathrm{GO}_d(q,Q)$ to $\mathbb{F}_2^+$ or $(\mathbb{F}_2^+)^2$.

Proposition 5.7. *Let Q be a nondegenerate quadratic form, and let $g\in\mathrm{GO}_d(q,Q)$. Then the image of g under the natural homomorphism to $\mathbb{F}_2^+$ (q even) or $(\mathbb{F}_2^+)^2$ (q odd) can be found in $O(d^\omega)$ (q even) or Las Vegas $O(d^3+\log q)$ (q odd) field operations.*

A canonical coset representative for g can then be constructed in $O(d^2)$ field operations if q is even and, given ζ, in Las Vegas $O(d^2+\log q)$ field operations otherwise.

Proof. If q is even then we calculate the homomorphism to $\mathbb{F}_2^+$ as $\mathrm{sp}(g)$ in $O(d^\omega)$ field operations. For the coset representative we return $\mathrm{refl}_v^{\mathrm{sp}(g)}$ as in Proposition 5.3.

Next let q be odd. We compute $\det(g)$ in $O(d^\omega)$ and $\mathrm{sp}(g)$ in $O(d^3+\log q)$ operations. The image of g is $(a,\mathrm{sp}(g))$, where $a=\mathrm{sp}(g)$ if $\det(g)=1$ and $a=\mathrm{sp}(g)+1 \bmod 2$ otherwise. We find R_1 and R_2 in $O(d^2+\log q)$ as in Proposition 5.3. If the image of g is (a,b) then a representative is $R_1^aR_2^b$. □

Recall $G^\epsilon(q)$ and $H^\epsilon(q)$ from Theorem 4.2 and Corollary 4.3. Discrete logs can be computed in subexponential time [16], but we view them as an oracle. We can now give our main result.

Theorem 5.8. *Let g be an element of $\mathrm{CO}_d(q,Q)$, and if q is odd and d is even let ζ be given.*

(1) *The image of g under the natural homomorphism to $G^\epsilon(q)$ can be computed in $O(d^\omega)$ field operations if q is even, by a Las Vegas algorithm in $O(d^3 + \log q)$ field operations if qd is odd, and by a Las Vegas algorithm in $O(d^3 + d \log q)$ field operations otherwise.*
(2) *The image of g as a standard word in $H^\epsilon(q)$ can be calculated in the same number of field operations as (1), plus one discrete logarithm call. If q is odd and Q is of $-$ type, we assume that the discrete log of γ has been precomputed.*
(3) *A canonical representative of the coset $\Omega_d(q, Q)g$ can be computed in the same number of field operations as (1).*

Proof for q even. By Theorem 4.2, $G^\epsilon(q) = \langle r_0 \rangle \times \langle c(\xi) \rangle \cong \mathbb{F}_2^+ \times \mathbb{F}_q^\times$. If $g \mapsto r_0^i c(\lambda)$, then $\lambda = \tau(g)$, hence $i = \mathrm{sp}(gC^\epsilon(\lambda)^{-1})$. We find $\tau(g)$ in $O(d^2)$ operations by Corollary 5.4, and then compute $c(\lambda) = \lambda^{q/2} I_d$ in $O(d^2 + \log q)$ operations. We find i in $O(d^\omega)$ by Theorem 5.6. The image of g in $H^\epsilon(q)$ is $r_0^i c^j$ where $j = \log_\xi \lambda$. We use Proposition 5.3 to find a canonical reflection R_0, then a canonical coset representative of g is $R_0^i C^\epsilon(\lambda)$. □

Proof for q odd, d odd. By Theorem 4.2, $G^\circ(q) = \langle r_1 \rangle \times \langle c(\xi) \rangle \cong \mathbb{F}_2^+ \times \mathbb{F}_q^\times$. Let $\alpha = \sqrt{\tau(g)}$, and define the map $\psi : g \mapsto r_0^i c(\lambda)$ where

$$\lambda = \lambda(g) = \alpha \det(g\alpha^{-1}) \quad \text{and} \quad i = i(g) = \mathrm{sp}(g\lambda(g)^{-1}).$$

We first show that this is the natural homomorphism to $G^\circ(q)$. Let $\alpha_1 = \sqrt{\tau(g_1)}$, $\alpha_2 = \sqrt{\tau(g_2)}$ and $\alpha_3 = \sqrt{\tau(g_1 g_2)}$. Then $\alpha_3 = t\alpha_1\alpha_2$ for $t = \pm 1$, so

$$\begin{aligned}\lambda(g_1 g_2) &= \alpha_3 \det(g_1 g_2 \alpha_3^{-1}) \\ &= t\alpha_1\alpha_2 \det(g_1 g_2)\det(t^{-1}) \det(\alpha_1^{-1}\alpha_2^{-1}) \\ &= t^{1-d}\alpha_1 \det(g_1\alpha_1^{-1})\alpha_2 \det(g_2\alpha_2^{-1}) = \lambda(g_1)\lambda(g_2)\end{aligned}$$

since $1 - d$ is even, and λ is a homomorphism. Then $g \mapsto i(g)$ is a homomorphism since $\tau(\det(g\alpha^{-1})) = (\pm 1)^2 = 1$, so λ has kernel $\mathrm{SO}_d(q, Q)$ and sp is a homomorphism on $\mathrm{SO}_d(q, Q)$.

We find α in Las Vegas $O(\log q)$ operations, then set $\lambda = \alpha \det(g\alpha^{-1})$ and $i = \mathrm{sp}(g\lambda(g)^{-1})$ in $O(d^3 + \log q)$ operations, so (1) follows.

For (2) we let $k = \log_\xi \lambda$. If $k < (q-1)/2$ we map g to $r_0^i r_1^i c^k$, whereas if $k \geq (q-1)/2$ we map g to $r_0^{1+i} r_1^i c^{k-(q-1)/2}$. For (3), we calculate R_0, R_1 in Las Vegas $O(d^2 + \log q)$ field operations by Proposition 5.3. We represent g by $\alpha R_0^a R_1^b$, where $b = \mathrm{sp}(\alpha^{-1} g)$ and $a = b$ if $\det(\alpha^{-1} g) = 1$ and $b + 1$ otherwise. □

Proof for q odd, d even, $+$ type. For (1), we first find a canonical isometry X from the standard form to F, in $O(d^3 + d \log q)$ operations, by Theorem 5.2. We compute $\lambda = \tau(g)$ in $O(d^2)$, by Proposition 5.3. We calculate $h = g^{x^{-1}} C^+(\lambda)^{-1}$ in $O(d^\omega)$, and find $a = \det(h)$ and $b = \mathrm{sp}(h)$ in $O(d^3 + \log q)$ field operations. If $a = 1$, let $b' = b$, otherwise $b' = b + 1$. Map g to $r_0^{b'} r_1^b c(\lambda)$.

For (2), we find $k = \log_\xi \lambda$ and map g to $r_0^{b'} r_1^b c^k$. For (3) we write down the canonical elements R_0, R_1 from §4 in $O(d^2 + \log q)$, then represent g by $(R_0^{b'} R_1^b C^+(\lambda))^X$. □

Proof for q odd, d even, $-$ type. For (1), we first find a canonical isometry X from the standard form to F in $O(d^3 + d \log q)$ field operations. We compute $\tau(g)$ in $O(d^2)$ field operations. If $\tau(g)$ is a square, we take $\lambda = \sqrt{\tau(g)}$, $z = c(\lambda)$ and $C = C^-(\lambda)$. Otherwise we take $\lambda = \sqrt{\tau(g)\gamma^{-1}}$, $z = c_0 c(\lambda)$, and $C = C_0^- C^-(\lambda)$. We then let $h = g^{x^{-1}} C^{-1}$, find $a = \det(h)$ and $b = \mathrm{sp}(h)$ in $O(d^3 + \log q)$ field operations. We map g to $r_0^{b'} r_1^b z$, where $b' = b$ if $a = 1$ and $b' = b + 1$ otherwise.

For (2) we find $k = \log_{\xi^\gamma} \lambda = \frac{\log \lambda}{\log \gamma + 1}$ with a discrete log call, and map g to $r_0^{b'} r_1^b c^k$. For (3) we write down R_0 and R_1 from §4 in $O(d^2 + \log q)$, then the representative is $(R_0^{b'} R_1^b C)^X$. □

Note that similar, but faster, algorithms can be given for $\mathrm{CO}_d(q, Q)/\mathrm{GO}_d(q, Q)$.

6. Algorithms for other classical groups

In this section, we briefly present similar algorithms for other classical groups.

Proposition 6.1. *The image of $g \in \mathrm{GL}_d(q)$ under the natural map to $\mathrm{GL}_d(q)/\mathrm{SL}_d(q) \cong \mathbb{F}_q^\times$ can be computed in $O(d^\omega)$ field operations. The image of g in the polycyclically presented group $\langle c \mid c^{q-1} \rangle$ can be then computed in one discrete log call, given a primitive field element. A canonical coset representative can also be constructed in $O(d^\omega)$ field operations.*

Proof. The image of g in $\mathbb{F}_q^\times$ is $\det(g)$. To represent $\det(g)$ as an element of the polycyclic group we calculate its discrete logarithm. A canonical coset representative is $\mathrm{diag}[\det(g), 1, \ldots, 1]$. □

For the symplectic and unitary groups, let $S_d(q, F)$ denote $\mathrm{Sp}_d(q, F)$ or $\mathrm{SU}_d(q, F)$ respectively. All groups of the same type are isometric. We let $u = 1$ for the symplectic groups and $u = 2$ otherwise. We define $N_d(q, F) := N_{\mathrm{GL}_d(q^u)}(S_d(q, F))$, and define $\tau : N_d(q, F) \to \mathbb{F}_{q^u}^\times$ by $F(ug, vg) = \tau(g) F(u, v)$, for all $u, v \in V$.

Lemma 6.2. *The map τ is a homomorphism from $N_d(q, F)$ to $\mathbb{F}_{q^u}^\times$ with kernel $\mathrm{Sp}_d(q, F)$ or $\mathrm{GU}_d(q, F)$, respectively. Given $g \in N_d(q, F)$ and F we calculate $\tau(g)$ in $O(d^2)$ field operations.*

Proof. The first claim is proved in [12, 2.1.2(ii)]. We compute $\tau(g)$ by first calculating $v_1 F$ in $O(d)$ field operations, as it is the first row of F. Let the first nonzero entry of $v_1 F$ be α in position i. Then $F(v_1, v_i) = \alpha \neq 0$. We compute $v_1 g, v_i g$ in $O(d)$ since they each consist of a row of g. We calculate $\beta := (v_1 g) F (v_i g)^{\mathrm{Tr}}$ in $O(d^2)$ field operations, then $\tau(g) = \alpha/\beta$. □

The standard symplectic form is $F_d := \mathrm{antidiag}[1, 1, \ldots, 1, -1, \ldots, -1]$, with $d/2$ entries 1.

Proposition 6.3. *Let F be a symplectic form over $\mathbb{F}_q^d$ with $d \geq 3$, then $N_d(q, F)/\mathrm{Sp}_d(q, F) \cong \mathbb{F}_q^\times$. The image of $g \in N_d(q, F)$ in $\mathbb{F}_q^\times$ can be computed in $O(d^2)$ field operations. The image of g in $\langle c \mid c^{q-1} \rangle$ then requires a single discrete logarithm call, given ξ. A coset representative can be constructed in $O(d^3)$ field operations if q is odd and $O(d^2 + \log q)$ field operations if q is even.*

Proof. Note that $\tau(\xi I_d) = \xi^2$, which gives the first claim for even q. For q odd, with respect to F_d the element $h = \mathrm{diag}[\xi, \ldots, \xi, 1, \ldots, 1]$ satisfies $\tau(h) = \xi$, so the first claim follows.

The image of g in $\mathbb{F}_q^\times$ is $\tau(g)$, which is calculated in $O(d^2)$ field operations by Lemma 6.2. We represent $\tau(g)$ as an element of a polycyclic group with one discrete log call.

If q is even then a canonical coset representative is $\tau(g)^{q/2} I_d$. If q is odd then we use [10] to find a canonical isometry X from F to F_d in $O(d^3)$ field operations. A coset representative is $\mathrm{diag}[\tau(g), \ldots, \tau(g), 1, \ldots, 1]^X$. □

Now we consider the unitary groups. We take the standard unitary form to be I_d. Recall that ζ is a primitive element of $\mathbb{F}_{q^2}$. First we describe the structure of $N_d(q, F)$.

Proposition 6.4. *Let F be a unitary form over $\mathbb{F}_{q^2}^d$, with $d \geq 3$, then $N_d(q, F) = \langle \mathrm{GU}_d(q, F), \mathbb{F}_{q^2}^\times \rangle$. The quotient $U_{d,q} = N_d(q, F)/\mathrm{SU}_d(q, F)$ has presentation $\langle a, b | a^{q-1} = b^d, b^{q+1} = 1, b^a = b \rangle$.*

Let $g \in N_d(q, F)$, then a canonical coset representative for g can be computed in $O(d^3 + d(\log q + \log^2 p))$ operations. Given a discrete log oracle and ζ, the image of g in $U_{d,q}$ can be computed in Las Vegas $O(d^\omega + \log q + \log^2 p)$ field operations, plus two uses of the oracle.

Proof. The first claim follows from the fact that all linear outer automorphisms $\mathrm{PSU}_d(q,F)$ lie in $\mathrm{PGU}_d(q,F)$, so $N_d(q,F)$ only contains $\mathrm{GU}_d(F)$ and scalars. For the second claim, first note that $\tau(\mathbb{F}_{q^2}^\times) = \mathbb{F}_q^\times$, and $\zeta^{q-1} I_d \in \mathrm{GU}_d(q,F)$. Since $\det(\zeta^{q-1} I_d) = \zeta^{d(q-1)}$ and $\mathrm{GU}_d(q,F)/\mathrm{SU}_d(q,F) \cong \langle \zeta^{q-1} \rangle$, the structure of $U_{d,q}$ is as stated.

We compute $\tau(g)$ in $O(d^2)$ field operations, by Lemma 6.2. Next we find a canonical μ such that $\mu^{q+1} = \tau(g)$ in $O(\log q + \log^2 p)$ by Proposition 2.2, and then calculate $\delta = \mu^{-d} \det(g)$.

To compute the coset representative we use the algorithms from [10], upgraded to use the canonical solution to the norm equation, to find a canonical siometry X from F to I_d in Las Vegas $O(d^3 + d(\log q + \log^2 p))$. Since $\langle \mathrm{SU}_d(q), \mathrm{diag}[\zeta^{q-1}, 1, \ldots, 1] \rangle = \mathrm{GU}_d(q)$, a canonical coset representative is $\mathrm{diag}[\mu\delta, \mu, \ldots, \mu]^X$.

To find the image of g in $U_{d,q}$, we use the oracle to find $x = (\log_\zeta \tau(g))/(q+1)$: note $x \in \mathbb{N}$ since $\tau(g) \in \mathbb{F}_q$. We find $y = \log_\zeta(\det(g)\zeta^{-xd})/(q-1)$. Finally, we map g to $a^x b^y \in U_{d,q}$. □

7. Timings

In this section we present various tables of timings data for a Magma v2.14-9 [3] implementation of our algorithms. We tested our spinor norm algorithm on $\mathrm{GO}_d(q,Q)$ on all five cases: odd dimension and odd characteristic, and both types of form in even dimensions in both even and odd characteristic. In each case we computed the spinor norm of a random element of a random conjugate of the general orthogonal group.

Next we tested the canonical coset representative algorithms on all five cases. We took a random conjugate of the conformal orthogonal group, and then selected a random element. The time required to find coset representatives for elements of the general orthogonal group will be between these two times.

The experiments were carried out on a 1.5 GHz PowerPC G4 processor. The machine has 1.25GB of RAM, but memory was not a factor. All times are given in milliseconds, and are the average of 50 trials; the symbol – indicates that the average time was less than 1 millisecond.

As we would expect, the time required grows extremely slowly with q, and somewhat more quickly with d. Far less time is required for even q than odd q, and much less time is required to calculate the spinor norm of an element than to decompose the element. Notice however that the representation of the field is more significant than its size, as 3^{16} is only about four times larger than 10000019, yet the tests always take far longer. Notice also that for q odd there is not much difference between the time required to calculate $\mathrm{sp}(g)$ and the time to find a canonical coset representative, whilst for even q the latter task takes almost twice as long.

8. Large fields

In this section, we briefly discuss how to deal with large fields, in particular fields of size $q = p^a$ for which the Conway polynomial of degree $2a$ and characteristic p is not known. A list of all known Conway polynomials is at [15], and these polynomials are also available in Magma. The main problem in this case is that the primitive element ζ in $\mathbb{F}_{q^2}$ is not known, so the canonical elements δ and γ cannot be computed as in Proposition 2.3. Needless to say, discrete logarithms are also completely infeasible when the primitive element is unknown.

The easiest fix for this problem is to find random elements for δ and γ. For q odd, the field $\mathbb{F}_q$ contains $(q-1)/2$ nonsquares, and it is not hard to prove that roughly a quarter of the elements have the property required for γ. Once the elements are found, they can be fixed for the remainder of that computation. This means that our canonical coset representatives from different runs would not be comparable.

TABLE 1. Spinor norm on $\mathrm{GO}^\epsilon_d(q, Q)$, q odd

		p					3^i		
Type	d	5	17	47	73	10000019	3^6	3^{11}	3^{16}
$\circ$	15	1	1	2	2	1	2	5	21
	35	4	11	11	10	9	29	103	553
	55	10	38	37	37	40	157	646	3686
	75	26	97	97	97	101	529	2143	15408
	95	47	181	182	182	281	1343	5728	46955
$+$	20	2	2	3	2	3	4	12	58
	40	6	16	14	15	12	47	180	913
	60	14	48	49	49	47	220	894	5384
	80	30	114	117	115	125	679	2902	20779
	100	63	215	214	213	329	1645	7339	88168
$-$	20	1	3	2	3	1	4	15	62
	40	5	15	16	13	12	46	211	943
	60	12	49	48	50	50	222	1021	5175
	80	30	119	117	118	134	687	3254	19366
	100	63	225	236	239	384	1647	7341	81668

TABLE 2. Spinor norm on $\mathrm{GO}^\epsilon_d(q, Q)$, q even

Type	$+$					$-$				
q	2^5	2^{10}	2^{20}	2^{40}	2^{80}	2^5	2^{10}	2^{20}	2^{40}	2^{80}
d 20	$-$	$-$	$-$	4	4	$-$	$-$	$-$	4	3
40	1	1	4	19	24	$-$	$-$	2	18	25
60	$-$	1	12	60	78	$-$	1	12	60	82
80	2	4	27	143	193	1	3	29	146	197
100	2	7	57	311	413	4	7	56	289	390

An alternative would be to find canonical elements without the use of a primitive element. For example, we can find a canonical δ by an argument similar to Proposition 2.3. We do not know how to do this for odd q however. Canonical isometries can be found without the use of primitive elements, using a more complicated algorithm than the one in Theorem 5.2.

REFERENCES

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[2] I.F. Blake, S. Gao, and R.C. Mullin. Explicit factorization of $x^{2^k} + 1$ over $\mathbf{F}_p$ with prime $p \equiv 3 \bmod 4$. *Appl. Algebra Engrg. Comm. Comput.*, 4(2):89–94, 1993.

[3] W. Bosma and J.J. Cannon. *Handbook of Magma functions*. School of Mathematics and Statistics, University of Sydney, Sydney, 2.14 edition, 2007.

[4] P.A. Brooksbank. A constructive recognition algorithm for the matrix group $\Omega(d, q)$. In *Groups and computation, III*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 79–93. de Gruyter, Berlin, 2001.

[5] P.A. Brooksbank. Constructive recognition of classical groups in their natural representation. *J. Symbolic Comput.*, 35(2):195–239, 2003.

[6] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997.

TABLE 3. Coset decomposition on $\mathrm{CO}^\epsilon_d(q, Q)$, q odd

		p					3^i		
Type	d	5	17	47	73	10000019	3^6	3^{11}	3^{16}
$\circ$	15	4	6	6	6	5	5	10	29
	35	18	30	25	28	29	44	137	628
	55	47	80	79	80	93	198	712	3922
	75	92	180	199	188	259	622	2477	16303
	95	177	347	354	376	520	1534	6495	46340
$+$	20	7	10	10	10	11	11	24	93
	40	23	42	39	39	43	74	253	1211
	60	57	104	107	103	119	285	1097	6589
	80	112	230	223	223	282	830	3357	24526
	100	218	430	442	441	592	1920	8985	94569
$-$	20	7	9	12	9	12	145	27	104
	40	24	43	40	42	42	222	263	1315
	60	63	122	110	119	130	434	1163	7301
	80	119	239	243	252	305	1028	3586	25659
	100	223	450	455	414	654	2089	8610	97101

TABLE 4. Coset decomposition on $\mathrm{CO}^\epsilon_d(q, Q)$, q even

Type	$+$					$-$				
q	2^5	2^{10}	2^{20}	2^{40}	2^{80}	2^5	2^{10}	2^{20}	2^{40}	2^{80}
d 20	1	2	4	8	14	1	1	3	7	11
40	5	6	9	39	50	7	8	11	46	55
60	17	18	26	124	170	14	12	25	131	154
80	35	31	67	284	369	17	32	56	304	353
100	49	67	127	553	629	71	60	119	553	736

[7] R.H. Dye. A geometric characterization of the special orthogonal groups and the Dickson invariant. *J. London Math. Soc. (2)*, 15(3):472–476, 1977.

[8] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992.

[9] D.F. Holt, B. Eick, and E.A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[10] D.F. Holt and C.M. Roney-Dougal. Constructing maximal subgroups of classical groups. *LMS J. Comput. Math.*, 8:46–79, 2005.

[11] C. Jansen, K. Lux, R. Parker, and R. Wilson. *An Atlas of Brauer Characters*. Oxford University Press, Oxford, UK, 1995.

[12] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*. Cambridge University Press, Cambridge, 1990.

[13] C.R. Leedham-Green. The computational matrix group project. In *Groups and computation, III*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 229–247. de Gruyter, Berlin, 2001.

[14] C.R. Leedham-Green and E.A. O'Brien. Constructive recognition of classical groups in odd characteristic. In preparation.

[15] F. Lübeck. `http://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol`.

[16] I.E. Shparlinski. *Finite fields: theory and computation*, volume 477 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, 1999.
[17] M.J. Stather. *Algorithms for Computing with Finite Matrix Groups*. PhD thesis, University of Warwick, 2006.
[18] A. Storjohann. An $O(n^3)$ algorithm for the Frobenius normal form. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Rostock)*, pages 101–104, New York, 1998. ACM.
[19] D.E. Taylor. *The geometry of the classical groups*. Heldermann Verlag, Berlin, 1992.
[20] H. Zassenhaus. On the spinor norm. *Arch. Math.*, 13:434–451, 1962.

Department of Mathematics and Statistics F07, University of Sydney, NSW, 2006 Australia
E-mail address: murray@maths.usyd.edu.au

School of Mathematics and Statistics, St Andrews, Fife KY16 9SS, UK.
E-mail address: colva@mcs.st-and.ac.uk