

CONSTRUCTIVE HOMOMORPHISMS FOR CLASSICAL GROUPS

SCOTT H. MURRAY AND COLVA M. RONEY-DOUGAL

ABSTRACT. Let $\Omega \leq \mathrm{GL}_d(q)$ be a quasisimple classical group in its natural representation and let $\Delta = \mathrm{N}_{\mathrm{GL}_d(q)}(\Omega)$. We construct the projection from Δ to Δ/Ω and provide fast, polynomial-time algorithms for computing the image of an element. Given a discrete logarithm oracle, we also represent Δ/Ω as a group with at most 3 generators and 6 relations. We then compute canonical representatives for the cosets of Ω . We describe applications of these methods to the matrix group recognition project and conjugacy problems. A key ingredient of our algorithms is a new, asymptotically fast method for constructing isometries between spaces with bilinear or unitary forms.

1. INTRODUCTION

In this paper, we provide a variety of algorithms for classical groups. Fix a prime power q , and let $u = 2$ for unitary groups and 1 otherwise. We consider $H \leq \mathrm{GL}_d(q^u)$ such that $\Omega \leq H \leq \Delta$, where Ω is a quasisimple classical group and $\Delta = \mathrm{N}_{\mathrm{GL}_d(q^u)}(\Omega)$ is the corresponding conformal group [KL90]. Most of our algorithms are randomised Las Vegas in the sense of [Bab97]. We often need Las Vegas algorithms whose output is independent of the random choices made. In this case we call the output *canonical*.

The matrix group recognition project [LG01] seeks to efficiently compute composition series for matrix groups over finite fields. By finding a geometry preserved by the group, in the sense of Aschbacher's theorem [Asc84], a normal subgroup and its quotient can often be computed. This decomposition terminates when we reach groups that are almost simple, modulo their subgroup of scalar matrices. These groups are either classical groups in their natural representation (Aschbacher's class 8) or other almost simple groups (class 9). This paper provides algorithms for dealing with a group known to be in class 8. Algorithms to constructively recognise the quasisimple classical groups in their natural representation are known [Bro01, Bro03]. This paper presents efficient, practical reduction algorithms for the other class 8 groups.

Another motivation is constructing efficient algorithms for element conjugacy in classical groups H where the dimension d is large. The fundamental problem is to determine if two elements are conjugate and, if so, provide a conjugating element. For the sake of memory efficiency, it makes sense to conjugate a single element to a canonical representative of its conjugacy class. Given a solution to the conjugacy problem for Δ [HM07, Bri06], we construct an algorithm for any H between Ω and Δ , provided we have *canonical* coset representatives for H/Ω . This is the primary motivation for the requirement that our algorithms give canonical solutions. See Subsection 4 for more details.

Stather [Sta06] presented an algorithm to calculate a chief series for a class 8 orthogonal group, using our spinor norm algorithm, as presented in this current article. Stather's algorithm works in the projective group, whereas we give a version for matrix groups.

Date: September 21, 2009.

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

The second author would like to acknowledge the support of the Nuffield Foundation. The authors also thank the Magma project at the University of Sydney, where some of the work was carried out.

We give our timings in terms of finite field operations (addition, multiplication, etc). Our algorithms are polynomial in d and $\log q$, except for some which require one or two calls to a discrete logarithm oracle: we specify when this is the case. We define ω to be the exponent of matrix multiplication: for example, the standard method gives $\omega = 3$. For sufficiently large d (depending on the field size) MAGMA [BC07] uses the algorithm of [Str69] with $\omega = \log_2 7 + \epsilon$ for any $\epsilon > 0$: this gives a noticeable practical, as well as a theoretical, improvement.

The most fundamental algorithmic problem for classical groups is the construction of isometries between classical forms. We give a new method that is asymptotically faster than existing ones (except for quadratic forms with q even).

Theorem 1.1. *Suppose we have two symplectic, unitary, or quadratic forms on the space $V = \mathbb{F}_{q^u}^d$. We can determine if they are isometric, and find a canonical isometry matrix in: deterministic $O(d^\omega)$ field operations if the forms are symplectic; Las Vegas $O(d^\omega + d^2 \log q + d \log^2 p)$ field operations if the forms are unitary; Las Vegas $O(d^\omega + d \log q)$ field operations if q is odd and the forms are quadratic; and deterministic $O(d^3 + d \log q)$ field operations if q is even and the forms are quadratic.*

We now state our main theorem:

Theorem 1.2. *Let $\Omega \leq \mathrm{GL}_d(q^u)$ be a quasisimple classical group fixing a known classical form, and let $\Delta = \mathrm{N}_{\mathrm{GL}_d(q^u)}(\Omega)$.*

- (1) *A finitely presented group G isomorphic to Δ/Ω can be constructed in $O(\log^2 q)$ field operations. A presentation P for G with at most 3 generators and 6 relations can be found in the same time.*
- (2) *The image of $g \in \Delta$ under the natural projection $\Delta \rightarrow G$ can be computed in Las Vegas $O(d^\omega + d(\log q + \log^2 p))$ field operations. This image can be written as a canonical word in the generators of P at the additional cost of at most two calls to the discrete logarithm oracle.*
- (3) *A canonical representative of the coset Ωg can be computed in Las Vegas $O(d^\omega + d(\log q + \log^2 p))$ field operations.*

In Section 2 we define our canonical forms, and present algorithms for forms and classical groups, including proving Theorem 1.1. In Section 3 we prove Theorem 1.2. In Section 4 we present some applications, before concluding in Sections 5 and 6 with some data on our implementations: our spinor norm algorithm is now part of the standard release of Magma.

2. GROUPS AND FORMS

In this section, we introduce some algorithms for classical forms and classical groups. We require that the output of our algorithms be *canonical*: the algorithm always gives the same output with a given input.

2.1. Fields. Let p be a prime and let q be a power of p . As is standard, we assume that \mathbb{F}_q is constructed by adjoining a canonical root ξ of the Conway polynomial [JLPW95] to the prime field \mathbb{F}_p , so that ξ is the canonical primitive element of \mathbb{F}_q . See [Lüb] for a current list of the fields for which this assumption is valid. We let ζ be the primitive element of \mathbb{F}_{q^2} , and note that $\xi = \zeta^{q+1}$. Given $\alpha \in \mathbb{F}_q$, the *discrete logarithm* $\log_\xi(\alpha)$ is the unique $i = 0, 1, \dots, q-1$ such that $\alpha = \xi^i$.

We now show how to find canonical solutions to various equations over \mathbb{F}_q or \mathbb{F}_{q^2} . Note that this result is the main source of randomisation in our algorithms.

Theorem 2.1 ([GCL92, 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.*

Let \mathbb{F}_q^\times denote the multiplicative group of \mathbb{F}_q , and let $\mathbb{F}_q^{\times 2}$ denotes the set of squares in \mathbb{F}_q^\times . Every element of \mathbb{F}_{q^2} can be written as $a_0 + a_1\zeta + \dots + a_{m-1}\zeta^{m-1}$, where $p^m = q^2$ and $a_i \in \{0, \dots, p-1\}$. This induces an ordering on \mathbb{F}_{q^2} by lexicographically ordering the coefficients. We can fix a canonical root of a polynomial equation by taking the smallest root with respect to our ordering on \mathbb{F}_{q^2} . Hence for $\alpha \in \mathbb{F}_q$ we can find a *canonical* square root $\sqrt{\alpha} \in \mathbb{F}_{q^2}$. For q even, the square root of α is unique and can be computed as $\alpha^{q/2}$ in $O(\log q)$ field operations. For $\alpha \in \mathbb{F}_q$, we define $\iota(\alpha) = 0$ if $\alpha \in \mathbb{F}_q^{\times 2}$ and $\iota(\alpha) = 1$ otherwise, tested in deterministic $O(\log q)$ by powering.

Canonical solutions for trace and norm equations are needed for the unitary groups.

Proposition 2.2. *Let $\alpha \in \mathbb{F}_q^\times$. A canonical solution $\eta \in \mathbb{F}_{q^2}$ to the trace equation $\eta + \eta^q = \alpha$ can be found in $O(1)$ field operations if q is odd, or $O(\log q)$ otherwise. A canonical solution $\eta \in \mathbb{F}_{q^2}$ of the norm equation $\eta^{q+1} = \alpha$ can be found in Las Vegas $O(\log q + \log^2 p)$ field operations.*

Proof. For the trace equation with q odd, $\eta = \alpha/2$. Otherwise, we can determine $\alpha \mapsto \alpha^q$ as an \mathbb{F}_q -linear map in $O(\log q)$ field operations. Then η exists by [Lan93, Theorem 6.3] and can be found by linear algebra, considering \mathbb{F}_{q^2} as an \mathbb{F}_q -space.

We construct a solution to the norm equation in three cases. If $\alpha \in \mathbb{F}_q^{\times 2}$, let $\eta := \sqrt{\alpha}$, then $\eta^{q+1} = \eta^2 = \alpha$. If $\alpha \notin \mathbb{F}_q^{\times 2}$ and $q \equiv 1 \pmod{4}$, then $-\alpha \in \mathbb{F}_q^{\times 2}$, so $-\alpha \notin \mathbb{F}_q^{\times 2}$. Hence the polynomial $X^2 + \alpha$ is irreducible over \mathbb{F}_q , and its roots in \mathbb{F}_{q^2} have norm α . If $\alpha \notin \mathbb{F}_q^{\times 2}$ and $q \equiv 3 \pmod{4}$, then $-\alpha \in \mathbb{F}_q^{\times 2}$. Let $\beta = \sqrt{-\alpha}$ and write $p+1 = 2^m s$ for s odd. Calculate $c \in \mathbb{F}_p$ in $O(\log^2 p)$ field operations by

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

By [BGM93], the polynomial $g(X) = X^2 - 2cX - 1$ is irreducible over \mathbb{F}_q . Hence $-\alpha g(X/\beta) = X^2 - 2\beta cX + \alpha$ is also irreducible and its roots in \mathbb{F}_{q^2} have norm α . \square

The following elements are all used to compute with orthogonal groups.

Proposition 2.3. *The following canonical elements can be constructed in \mathbb{F}_q :*

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

Proof. For (1), note that $\zeta + \zeta^q \neq 0$ (where ζ is primitive in \mathbb{F}_{q^2}) 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, $1 - 4\gamma = (\zeta - \zeta^q)^2(\zeta + \zeta^q)^{-2} \notin \mathbb{F}_q^{\times 2}$, since $(\zeta - \zeta^q)(\zeta + \zeta^q)^{-1} \notin \mathbb{F}_q$.

For (2), let $q = 2^m$. If m is odd, let $\gamma = 1$. 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 γ to be the first a_j for which $X^2 + X + a_j$ is irreducible, if any. Define $T : \mathbb{F}_q \rightarrow \mathbb{F}_q$ 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 (3), 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 $1 + \nu^2 \notin \mathbb{F}_q^{\times 2}$. \square

2.2. Forms and Isometries. In this subsection we define our standard forms, and present an algorithm to construct canonical isometries between forms.

Let $V = \mathbb{F}_q^d$ have standard basis v_1, \dots, v_d . By $\text{diag}(a_1, a_2, \dots, a_d)$ we mean the $d \times d$ matrix with entry a_i in position (i, i) and 0 elsewhere. By $\text{antidiag}(a_1, a_2, \dots, a_d)$ we mean the $d \times d$ matrix with entry a_i in position $(i, d - i + 1)$ and 0 elsewhere. By $A \oplus B$ we mean a block diagonal matrix, with blocks A and B along the main diagonal and 0 elsewhere.

The following results are standard and can be found in [BCS97, Chapter 16].

Theorem 2.4. *Computing the row echelon form, the rank, the nullspace, or the determinant of a $d \times d$ matrix over \mathbb{F}_q requires $O(d^\omega)$ field operations.*

We refer to [Tay92] or [Gro02] for basic terminology on classical forms. We fix the following notation: either β is a nondegenerate symplectic or unitary form over V ; or Q is a nondegenerate quadratic form over V and β is its polar form, so that $2Q(v) = \beta(v, v)$. A vector v is *isotropic* if $\beta(v, v) = 0$ and *singular* if $Q(v) = 0$. A subspace $W \leq V$ is *anisotropic* if $Q(v) = 0$ for $v \in W$ implies that $v = 0$. The matrix of β is $F = (\beta(v_i, v_j))_{d \times d}$, and satisfies $\beta(u, v) = uFv^{\text{Tr}}$. The matrix of Q is the upper triangular matrix $M = (m_{ij})_{d \times d}$ such that $Q(v) = \sum_{1 \leq i \leq j \leq d} m_{ij} a_i a_j$, for $v = (a_1, \dots, a_d)$. If β is the polar form of Q , then $F = M + M^{\text{Tr}}$ and F determines M if and only if q is odd.

Definition 2.5 (Standard forms). *We define the following standard forms:*

Symplectic or even dimension unitary: $d = 2m$ and V has basis $(e_1, \dots, e_m, f_m, \dots, f_1)$ with $\beta(e_i, e_j) = \beta(f_i, f_j) = 0$, $\beta(e_i, f_j) = \delta_{ij}$.

Unitary, odd dimension: $d = 2m + 1$ and V has basis $(e_1, \dots, e_m, x, f_m, \dots, f_1)$ with $\beta(e_i, e_i) = \beta(f_i, f_i) = \beta(e_i, x) = \beta(f_i, x) = 0$, $\beta(e_i, f_j) = \delta_{ij}$, $\beta(x, x) = 1$.

Orthogonal, \circ type: $d = 2m + 1$ and V has basis $(e_1, \dots, e_m, x, f_m, \dots, f_1)$ with $Q^\circ(e_i) = Q^\circ(f_i) = \beta^\circ(e_i, x) = \beta^\circ(f_i, x) = 0$, $\beta^\circ(e_i, f_j) = \delta_{ij}$, $Q(x) = 1$.

Orthogonal, $+$ type: $d = 2m$ and V has basis $(e_1, \dots, e_m, f_m, \dots, f_1)$ with $Q^+(e_i) = Q^+(f_j) = 0$ and $\beta^+(e_i, f_j) = \delta_{ij}$.

Orthogonal, $-$ type: $d = 2m + 2$ and V has basis $(e_1, \dots, e_m, x, y, f_m, \dots, f_1)$ with $Q^-(e_i) = Q^-(f_j) = 0$, $\beta^-(e_i, f_j) = \delta_{ij}$, $\beta^-(a, b) = 0$ for $a \in \{e_i, f_j\}$, $b \in \{x, y\}$, $Q^-(x) = \beta^-(x, y) = 1$, $Q^-(y) = \gamma$, as in Proposition 2.3.

It is well known (see for instance [Tay92]) that every nondegenerate quadratic, symplectic or unitary form over a finite field is similar to exactly one of the forms given in Definition 2.5. For odd dimension and characteristic, there are two isometry classes of quadratic forms, which are similar. Otherwise, forms are similar if and only if they are isometric. The *discriminant* of Q is $\iota(\det(F))$. Two quadratic forms are isometric if and only if they have the same discriminant.

The following will be needed for constructing isometries and coset representatives.

Lemma 2.6. *Given a quadratic or unitary form, we can find a canonical nonsingular or anisotropic vector in $O(d)$ field operations. Furthermore, if q is odd then given a quadratic form Q we can find canonical vectors u_1, u_2 such that $\iota(Q(u_1)) = 0$ and $\iota(Q(u_2)) = 1$ in Las Vegas $O(d^2 + \log q)$ field operations.*

Proof. For the first claim, let $M = (m_{ij})$ be the form matrix, so M is quadratic, symmetric or unitary. 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 $m_{1j} \neq 0$. If M is quadratic, let $v = v_1 + v_j$, otherwise take $v = v_1 + \xi v_j$.

For the second claim, first choose v_1 anisotropic as above. Compute v_1^\perp as the nullspace of Fv_1^{Tr} in $O(d^2)$, then recursively choose anisotropic $v_2 \in v_1^\perp$. If possible, take $u_1 = v_i$ for square $Q(v_i)$ and $u_2 = v_j$ for nonsquare $Q(v_j)$. If this is not possible, then either both $Q(v_i)$ are square

or both nonsquare. Let $w = v_1 + \nu\sqrt{Q(v_1)/Q(v_2)}v_2$, where ν is as in Proposition 2.3. Then $Q(w) = (1 + \nu^2)Q(v_1)$ and hence $\iota(Q(w)) = 1$ if and only if $\iota(Q(v_1)) = 0$. \square

Next we present the main technical ingredient of our isometry construction algorithm. We deal uniformly with symplectic, unitary and orthogonal forms, and refer to the symplectic case as *case S*. We define the *initial k -block* of a matrix X to be the matrix consisting of the first k columns of the first k rows of X . For a matrix over \mathbb{F}_{q^2} , the map σ is the q th power map on matrix entries: each application of σ is $O(\log q)$. For a matrix X we write X^* for $-X^{\text{Tr}}$ in case S, for $X^{\sigma^{\text{Tr}}}$ in the unitary case, and for X^{Tr} in the orthogonal case. Furthermore we write X^\dagger for X^{Tr} in case S and for X^* otherwise. Let $a = \log q$ in the unitary case and 0 otherwise.

Theorem 2.7 (Diagonalise forms). *Let A be the matrix of a (possibly degenerate) symmetric, unitary or symplectic form over \mathbb{F}_{q^u} , with q odd if A is symmetric. Then in deterministic $O(d^\omega + ad^2)$ field operations, a canonical $S \in \text{GL}_d(q^u)$ can be constructed such that SAS^\dagger is the diagonal sum of antidiagonal 2×2 matrices in case S, and is diagonal otherwise.*

Proof. We prove the result via a sequence of claims.

CLAIM 1: If A is of the form

$$\begin{pmatrix} A_1 & 0 & A_2 \\ 0 & 0 & A_3 \\ A_2^* & A_3^* & A_4 \end{pmatrix},$$

where $A_1 \in \text{GL}_k(q^u)$ for $1 \leq k \leq d-1$ (with k even in case S) and A_3 has $0 \leq s < d-k$ rows, then a canonical $S \in \text{GL}_d(q^u)$ can be constructed in $O(d^\omega + ad^2)$ field operations such that

$$SAS^\dagger = A_1 \oplus \begin{pmatrix} 0 & A_3 \\ A_3^* & A_5 \end{pmatrix}.$$

To verify this, let $S \in \text{GL}_d(q^u)$ have $-A_2^*A_1^{-1}$ in the bottom left, and the identity elsewhere.

CLAIM 2: If $A \neq 0$ then a canonical $S \in \text{GL}_d(q^u)$ may be constructed in $O(d^\omega)$ such that $SAS^\dagger = A_1 \oplus 0$ with $A_1 \in \text{GL}_k(q^u)$ for some $1 \leq k \leq d$ (with k even in case S).

To verify the claim, let $S \in \text{GL}_d(q^u)$ be such that SA is in row echelon form, constructed in $O(d^\omega)$ field operations by Theorem 2.4. Then

$$SAS^\dagger = \begin{pmatrix} X \\ 0 \end{pmatrix} S^\dagger = Y$$

for some matrix $X_{k \times d}$ with full row rank. Now, Y has its final $d-k$ rows all zero, and $Y = Y^*$. Thus the final $d-k$ columns of Y are all zero, and the initial k -block of Y is in $\text{GL}_k(q^u)$.

CLAIM 3: Let $d \equiv 0 \pmod{4}$ in case S, and let d be even otherwise. If

$$A = \begin{pmatrix} 0 & A_1 \\ A_1^* & A_2 \end{pmatrix}$$

with $A_1 \in \text{GL}_{d/2}(q^u)$ then in $O(d^\omega + ad^2)$ a canonical $S \in \text{GL}_d(q^u)$ can be constructed such that the initial $(d/2)$ -block of SAS^\dagger is invertible.

To verify the claim, first use Claim 2 to construct $U \in \text{GL}_{d/2}(q^u)$ in $O(d^\omega)$ such that $UA_2U^\dagger = A_3 \oplus 0$, with $A_3 \in \text{GL}_k(q^u)$ for some $k \leq d/2$ (and k even in case S). Let $S_1 = (A_1U^\dagger)^{-1} \oplus U$ in $O(d^\omega + ad^2)$, then

$$B := S_1AS_1^\dagger = \begin{pmatrix} 0 & I_{d/2} \\ I_{d/2}^* & A_3 \oplus 0 \end{pmatrix}.$$

It is now routine to construct a canonical S_2 such that $S_2BS_2^\dagger$ has invertible initial $(d/2)$ -block.

CLAIM 4: Let l with $1 \leq l \leq d-1$ be given, with l even in case S. If A is invertible, a canonical $S \in \text{GL}_d(q^u)$ can be constructed in $O(d^\omega + ad^2)$ such that the initial l -block of SAS^\dagger is invertible.

If $l > 1$ then first construct a canonical permutation matrix S_1 mapping A to a matrix B whose initial l -block is not identically zero. If $l = 1$ and $a_{11} = 0$ then construct a canonical anisotropic vector v in $O(d)$ by Lemma 2.6 and let B be the form resulting from swapping v this with v_1 . Let

$$B = \begin{pmatrix} B_1 & B_2 \\ B_2^* & B_3 \end{pmatrix},$$

where B_1 is $l \times l$. If B_1 is invertible, we are done. Otherwise, construct a matrix S_2 such that

$$C := S_2BS_2^\dagger = \begin{pmatrix} C_1 \oplus 0 & C_2 \\ C_2^* & B_3 \end{pmatrix},$$

where $C_1 = C_1^* \in \text{GL}_k(q^u)$ for some $k < l$ (with k even in case S). The matrix C can be computed in $O(d^\omega + ad^2)$ operations by Claim 2. Since C_1 is invertible, by Claim 1 in $O(d^\omega + ad^2)$ we construct a matrix S_3 such that

$$D := S_3CS_3^\dagger = C_1 \oplus \begin{pmatrix} 0 & D_1 \\ D_1^* & D_2 \end{pmatrix},$$

where D_1 is $(l-k) \times (d-l)$. The fact that A and C_1 are both invertible implies that D_1 has full row rank, so construct a matrix $P \in \text{GL}_{d-l}(q^u)$ in $O(d^\omega)$ such that $D_1P = (E_1 \ E_2)$ with $E_1 \in \text{GL}_{l-k}(q^u)$. Let $S_4 := I_l \oplus P^\dagger$. Then

$$E := S_4DS_4^\dagger = C_1 \oplus \begin{pmatrix} 0 & E_1 & E_2 \\ E_1^* & E_3 & E_4 \\ E_2^* & E_4^* & E_5 \end{pmatrix},$$

where E_3 is $(l-k) \times (l-k)$. By Claim 3 in $O(d^\omega + ad^2)$ we can construct a $2(l-k) \times 2(l-k)$ matrix M such that

$$M \begin{pmatrix} 0 & E_1 \\ E_1^* & E_3 \end{pmatrix} M^\dagger$$

has initial $(l-k)$ -block invertible. Let $S_5 = I_k \oplus M \oplus I_{d-2l+k}$, then $S_5ES_5^\dagger$ has invertible initial l -block.

MAIN THEOREM: By Claim 2, in $O(d^\omega + da^2)$ we can map $S_1AS_1^\dagger = A_1 \oplus 0$ with $A_1 \in \text{GL}_r(q^u)$ for some $r \leq d$, with r even in case S. Then by Claim 4, in $O(d^\omega + da^2)$ we can construct a matrix S_2 mapping A_1 to a matrix A_2 whose initial k -block B_1 is invertible, where $k = 2\lfloor r/4 \rfloor$ in case S and $k = \lfloor r/2 \rfloor$ otherwise. Now by Claim 1, in $O(d^\omega + da^2)$ we can construct a matrix S_3 mapping A_2 to $B_1 \oplus C_1$, where $C_1 = C_1^* \in \text{GL}_{d-k}(q^u)$. We now recurse on B_1 and C_1 , stopping when we reach (2×2) matrices in case S or 1×1 matrices otherwise. The whole process completes in $O(d^\omega + ad^2)$ and produces canonical matrices at each step. \square

We remark that the symmetric case of the above theorem is proved in [BCS97, Thm 16.25], although we correct several minor errors in the proof. Note that Theorem 1.1 applies unchanged to computing similarities rather than isometries.

Proof of Theorem 1.1. A canonical deterministic $O(d^3 + d \log q)$ algorithm for quadratic forms in even characteristic is given in [HRD05]. For quadratic forms in odd characteristic we work with the polar form. Note that it is enough to find an isometry or similarity from any given form to some fixed form.

First diagonalise the form to $\text{diag}(a_1, \dots, a_d)$, or map it to a direct sum of 2×2 matrices in case S. Each symplectic matrix $\text{antidiag}(a, -a)_{2 \times 2}$ is mapped to $\text{antidiag}(1, -1)$ by $\text{diag}(a^{-1}, 1)$. In the unitary case, the form is mapped to I_d by $\text{diag}(\alpha_1, \dots, \alpha_d)$, where α_i is a canonical solution to $\alpha_i^{q+1} = a_i^{-1}$, using Proposition 2.2.

In the orthogonal case, if d is odd and the discriminant is nonsquare then let α be the first nonsquare entry, and multiply all entries by α^{-1} (we produce a similarity if $\alpha \neq 1$). In all orthogonal cases now map all the square entries a_i to 1 by $\sqrt{a_i}^{-1}$ and the nonsquare entries a_i to the first nonsquare entry, μ , by $\sqrt{\mu/a_i}$. The entries μ are then changed in pairs to $\mu(1 + \nu^2)$ using the fact that $\begin{pmatrix} 1 & \nu \\ -\nu & 1 \end{pmatrix} \begin{pmatrix} 1 & \nu \\ -\nu & 1 \end{pmatrix}^{\text{Tr}} = (1 + \nu^2)I_2$ where ν is as in Proposition 2.3. These entries can now be changed to 1s, since $\mu(1 + \nu^2) \in \mathbb{F}^{\times 2}$. If there is a single nonsquare entry remaining (so that d is even) then this is moved to the first row and mapped to ξ . \square

2.3. Groups. Suppose β (or Q) is a nondegenerate form, as in the previous subsection. Then $\Delta := \text{N}_{\text{GL}_d(q^u)}(\Omega)$ consists of all similarities of the form with itself. The invariant group I consists of all isometries. We use notation from [KL90] for classical groups.

Define $\tau : \Delta \rightarrow \mathbb{F}_{q^u}$ by $\beta(ux, vx) = \tau(x)\beta(u, v)$ for all $u, v \in V$. It is well-known (see for example [KL90, Lemma 2.1.2]) that τ is a homomorphism with kernel I .

Lemma 2.8. *Given $g \in \Delta$, the value of $\tau(g)$ can be computed in $O(d^2)$ field operations.*

Proof. Find w such that $wFv_1^{\text{Tr}} \neq 0$ in $O(d)$. Then $\tau(g)$ is $\beta(wg, v_1g)/\beta(w, v_1)$. \square

For quadratic forms, the spinor norm is an epimorphism from the general orthogonal group $\text{GO}_d(q, Q)$ to \mathbb{F}_2^+ , originally defined by decomposing elements into a product of reflections.

Definition 2.9 (Spinor norm). *Let g preserve the form Q .*

- (1) *For q odd, let $U \leq V$ be the image of $1 - g$ and define the bilinear form χ on U by $\chi(u, v) = 2\beta(w, v)$ where $w(1 - g) = u$. The spinor norm of g is $\text{sp}(g) = \iota(\det(\chi))$.*
- (2) *For q even, the spinor norm of g is $\text{sp}(g) = \text{rank}(1 + g) \bmod 2$.*

Our definition for odd q is due to [Tay92], except for the factor of two which we include so the values of the spinor norm agree with [KL90, p. 29]. We follow [KL90, Proposition 2.5.7] and define $\Omega_d(q, Q) := \text{SO}_d(q, Q) \cap \ker(\text{sp})$. Note that some authors define $\text{SO}_d(q, Q) = \Omega_d(q, Q)$ when q is even, but once again we follow [KL90]. What we call the spinor norm for even q is called the Dickson invariant by some authors.

Theorem 2.10. *Let $g \in \text{GO}_d(q, Q)$, then $\text{sp}(g)$ can be found in $O(d^\omega)$ field operations if q is even, and $O(d^\omega + \log q)$ field operations if q is odd.*

Proof. If q is even, apply Theorem 2.4. If q is odd, compute the nullspace N of $a := I_d - g$ and find a matrix M whose rows are a basis to a complement of N in $O(d^\omega)$. Then the rows of Ma are a basis for the image of a . Calculate the form χ_g on Ma as $S = 2MF(Ma)^{\text{Tr}}$ in $O(d^\omega)$. Finally, find $\iota(\det S)$, by raising $\det(S)$ to the power $(q - 1)/2$. \square

We finish this section with a discussion of reflections. Let $v \in V$ be nonsingular, so that $Q(v) \neq 0$. The reflection in v is denoted refl_v , and maps $\text{refl}_v : u \mapsto u - \beta(u, v)v/Q(v)$.

Lemma 2.11. *Let Q be nondegenerate with polar form F , and let $u, v \in V$ be nonsingular.*

- (1) *All reflections are elements of $\text{GO}_d(q, Q)$, and have determinant -1 and order 2.*
- (2) *For q even, $\text{sp}(\text{refl}_v) = 1$.*
- (3) *For q odd, $\text{sp}(\text{refl}_v) = \iota(\beta(v, v))$.*
- (4) *For q odd the cosets $\Omega_d(q, Q) \text{refl}_u = \Omega_d(q, Q) \text{refl}_v$ if and only if $\iota(\beta(u, u)) = \iota(\beta(v, v))$.*

Proof. Parts (1) and (2) are well-known, and are easy exercises. For part (3), let $g = \text{refl}_v$. Then $(1 - g)$ has image $\langle v \rangle$, and maps $v \mapsto 2v$, so the matrix of χ_g is $(\beta(v, v))_{1 \times 1}$. Part (4) follows from part (3) and the fact that sp is a homomorphism. \square

Proposition 2.12. *For odd q , canonical reflections R_0, R_1 with $\text{sp}(R_i) = i$ can be constructed in Las Vegas $O(d^2 + \log q)$ field operations. For even q , a canonical reflection R_0 can be constructed in $O(d^2)$.*

Proof. For q odd, by Lemma 2.6.2 we can find canonical vectors u_0, u_1 with $\iota(Q(u_i)) = i$. Note that $u_i F v_j^{\text{Tr}}$ can be computed in $O(d)$ field operations for each j , as $F v_j$ is the j th row of F . Then row j of refl_{u_i} is $v_j - (u_i F v_j^{\text{Tr}}) Q(u_i)^{-1} u_i$. The other case is similar. \square

3. CONSTRUCTIVE HOMOMORPHISMS

In this section, for each type of classical group we construct the image of elements of the conformal group Δ under the natural quotient by the (normally quasisimple) group Ω in two ways. Firstly, as a word in a generating set parameterised by the field, and secondly as an element of a group P_2 given by a presentation with a bounded number of generators and relations. We also compute canonical representatives for cosets of Ω , which are needed for the conjugacy problem in Section 4.

Our main theorem is

Theorem 3.1. *Let $\Omega \leq \text{GL}_d(q^u)$ be a quasisimple classical group fixing a known classical form, and let $\Delta = \text{N}_{\text{GL}_d(q^u)}(\Omega)$. We refer to Table 1 for details.*

- (1) *The quotient $G := \Delta/\Omega$ has a presentation $P_1 = \langle X_1 \mid R_1 \rangle$, as in the table. The image of $g \in \Delta$ as a canonical word in the generators of P_1 can be computed with cost given in the table.*
- (2) *A polycyclic presentation $P_2 = \langle X_2 \mid R_2 \rangle$ for G is given in the table. The number of discrete logarithm calls needed to compute the image of $g \in G$ as a canonical word in the generators of P_2 is also given.*
- (3) *A canonical representative of the coset Ωg can be computed in the time given in the table.*

Note that Theorem 1.2 is just a simplified version of this result.

The main difficulties are with the orthogonal case. As an example we start with a proof of the unitary case.

Unitary case. We prove only the unitary case, the other cases are easier. By [KL90, Table 2.1.C], $[\Delta : \Omega] = q^2 - 1$. The group G has the same order since $B := \langle b(\zeta) \rangle$ is cyclic of order $q + 1$, and $G/B = \langle a(\zeta)B \rangle$ is cyclic of order $q - 1$. So it suffices to check the presentation: $A(\lambda)A(\mu) = A(\lambda\mu)$ implies $a(\lambda)a(\mu) = a(\lambda\mu)$, and similarly for $b(\lambda)b(\mu) = b(\lambda\mu)$; to show that $a(\lambda)^{q-1} = b(\lambda)^d$ it suffices to see that $A(\lambda)^{q-1}B(\lambda)^{-d}$ has determinant 1 and fixes the standard form, and similarly for $b(\lambda)^{q+1} = 1$.

Use Theorem 1.1 to find X such that $\text{SU}_d(q, \beta) = \text{SU}_d(q)^X$. Take the coset representative of $g \in \Delta$ to be $(A(\tau(g))B(\mu^{-d} \det(g)))^X$ where μ is the canonical solution of $\mu^{q+1} = \tau(g)$ (Proposition 2.2). This element has the same image under \det and τ as g , and so must be in the same coset of $\text{SU}_d(q)$. The image in G of $g \in \Delta$ is $a(\tau(g))b(\mu^{-d} \det(g))$, which can be written as $a^i b^j$ by computing the appropriate discrete logarithms i and j . \square

We now give an explicit presentation for the quotient of $\text{CO}_d^\epsilon(q) := \Delta$ by $\Omega_d^\epsilon(q)$, since, to our knowledge, such presentations only exist in the literature for the projective groups [KL90, Sections 2.5–2.8]. We assume from now on that $d \geq 3$ if q is even then d is even, to ensure that Ω is quasisimple. For $\epsilon \in \{+, -, \circ\}$ we write $G = G^\epsilon(q) := \text{CO}_d^\epsilon(q)/\Omega_d^\epsilon(q)$.

TABLE 1. Presentations and complexity for classical groups

Case	Generators for CO	X_1	R_1	Presentation F_1	cost in $O(\text{field ops})$	X_2	Presentation P_2	cost. in dlogs	coset rep. cost in $O(\text{field ops})$
$SL_d(q)$	$A(\lambda) = \text{diag}(\lambda, 1, \dots, 1)$	$a(\lambda)$	(*)		d^ω	$a := a(\xi)$	R_2	1	d^ω
$Sp_d(q)$	$A(\lambda) = \begin{cases} \lambda^{q/2} I_d & q \text{ even} \\ \lambda I_m \oplus I_m & q \text{ odd} \end{cases}$	$a(\lambda)$	(*)		d^2	$a := a(\xi)$	a^{q-1}	1	$\begin{cases} d^2 \log q & q \text{ even} \\ d^\omega & q \text{ odd} \end{cases}$
$SU_d(q)$	$A(\lambda) = \lambda^{q/2} I_d$ $B(\lambda) = (\lambda^q) \oplus I_{d-2} \oplus (\lambda^{-1})$	$a(\lambda),$ $b(\lambda)$	(*), $b(\lambda)^{q+1},$ $a(\lambda)^{q-1} = b(\lambda)^d$		$d^\omega + \log q + \log^2 p$ Las Vegas	$a := a(\xi),$ $b := b(\xi)$	$a^{q-1} = b^d,$ $b^{q+1}, [a, b]$	2	$d^\omega + \log q + \log^2 p$
$\Omega_d^-(q),$ $d \text{ even}, q \text{ odd}$	$R_0, C(\lambda) = \lambda^{q/2} I_d$	$r_0, c(\lambda)$	(*), $[r_0, c(\lambda)]$		d^ω	$r_0, c := c(\xi)$	$[r_0, c], c^{q-1}$	1	d^2
$\Omega_d^+(q),$ $d \text{ odd}, q \text{ odd}$	$R_0, R_1,$ $C(\lambda) = \lambda^2 I_m \oplus (\lambda) \oplus I_m$	$r_0, r_1, c(\lambda)$	(*), $[r_i, c(\lambda)],$ $c(-1) = r_0$		$d^\omega + \log q$	$r_0, r_1,$ $c := c(\xi)$	$[r_0, c], [r_1, c]$	1	$d^2 + \log q$
$\Omega_d^-(q),$ $d \text{ odd}, q \text{ odd}$	$R_0, R_1,$ $C(\lambda) = \lambda I_m \oplus I_m$	$r_0, r_1, c(\lambda)$	(*), $r_i^c(\lambda) = r_{i+t}(\lambda)$		$d^\omega + \log q$	$r_0, r_1,$ $c := c(\xi)$	$r_0^c = r_1,$ $r_1^c = r_0,$ c^{q-1}	1	$d^2 + \log q$
$\Omega_d^-(q),$ $d \text{ odd}, q \text{ odd}$	$R_0, R_1,$ $C(\lambda) = \lambda^2 I_m \oplus \lambda I_2 \oplus I_m$ $C_0^- = \gamma I_m \oplus \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \oplus I_m$	$r_0, r_1, c(\lambda)$	(*), $[r_i, c(\lambda)],$ $c(-1) = r_0 r_1$ $[c_0, c(\lambda)], c_0^2 = c(\gamma),$ $r_i^{c_0} = r_{i+1}$		$d^\omega + \log q$	$r_0, r_1,$ $c := c(\sqrt{\xi\gamma^{-1}})c_0$	$r_0^c = r_1,$ $r_1^c = r_0,$ c^{q-1}	1	$d^2 + \log q$

(*) The following relations apply whenever relevant: $a(\lambda)a(\mu) = a(\lambda\mu), b(\lambda)b(\mu) = b(\lambda\mu), c(\lambda)c(\mu) = c(\lambda\mu), r_0^2 = r_1^2 = (r_0 r_1)^2 = 1.$

We define $a(\lambda)$ to be the coset $\Omega A(\lambda)$, and similarly for $b(\lambda), r_0, r_1, c(\lambda), c_0$, for $\lambda, \mu \in \mathbb{F}_q^\times$ and $i \in \mathbb{Z}/2\mathbb{Z}.$

Take γ as in Proposition 2.3.

Take R_0, R_1 as in Proposition 2.12.

Proposition 3.2. *The group $\text{CO}_d^\epsilon(q)$ is generated by $\Omega_d^\epsilon(q)$ together with the generators in Table 1. Also $P_1 = \langle X_1 | R_1 \rangle$ is a presentation for $G_d^\epsilon(q)$.*

Proof. It is easy to check that $C^\epsilon(\lambda) \in \text{CO}_d^\epsilon(q)$ and $C_0^- \in \text{CO}_d^-(q)$. 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. One may check that $\tau(C_0^-) = \gamma$.

The kernel of τ on $\text{CO}_d^\epsilon(q)$ is $\text{GO}_d^\epsilon(q)$, and its image is \mathbb{F}_q^\times if d is even, and $\mathbb{F}_q^{\times 2}$ otherwise [KL90, §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 $\tau(C_0^-) = \gamma$ generate \mathbb{F}_q^\times , since γ is nonsquare. Since $\text{GO}_d^\epsilon(q)$ is generated by $\Omega_d^\epsilon(q)$ and the reflections, $\text{CO}_d^\epsilon(q)$ is generated by the given elements.

For q even or d odd, $G^\epsilon(q) = \langle r_0 \rangle \times \langle c(\xi) \rangle \cong \mathbb{F}_2^+ \times \mathbb{F}_q^\times$. 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 $\text{CO}_d^\epsilon(q)/\Omega_d^\epsilon(q)$ [KL90, § 2.1]. It therefore suffices to show that the relations hold.

All relations involving only r_0 and r_1 hold because the quotient $\text{GO}_d^\epsilon(q)/\Omega_d^\epsilon(q)$ is an elementary abelian 2-group. For the relations involving r_0 or r_1 conjugated by $c(\lambda)$ or c_0 , note that $\text{refl}_v^g = \text{refl}_{vg}$ for $v \in V$ and $g \in \text{CO}_d^\epsilon(q)$. 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, $C_{2m+1}^\circ(-1) = I_m \oplus (-1) \oplus I_m = \text{refl}_x$, and since $Q^\circ(x) = 1$ we deduce $c(-1) = r_0$. Finally, $C^-(\lambda)$ commutes with C_0^- ; $(C_0^-)^2 = C^-(\gamma)$; and $C^-(-1) = I_m \oplus -I_2 \oplus I_m = \text{refl}_x \text{refl}_y$, so $c(-1) = r_0 r_1$. \square

By setting $c = c(\xi)$, or $c = c(\sqrt{\xi\gamma^{-1}})c_0$ for q odd and $\epsilon = -$, we get presentations for the same groups with a bounded number of generators and relations:

Corollary 3.3. $P_2 = \langle X_2 | R_2 \rangle$ is a presentation for $G_d^\epsilon(q)$.

Any element of P_2 can now be written uniquely as:

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

Proposition 3.4. *Let Q be a nondegenerate quadratic form, and let $g \in \text{GO}_d(q, Q)$. 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 $O(d^\omega + \log q)$ (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 $\text{sp}(g)$ in $O(d^\omega)$ field operations. For the coset representative we return $\text{refl}_v^{\text{sp}(g)}$ as in Proposition 2.12.

For q odd, compute $\det(g)$ and $\text{sp}(g)$ in $O(d^\omega + \log q)$ field operations. The image of g is $(a, \text{sp}(g))$, where $a = \text{sp}(g)$ if $\det(g) = 1$ and $a = \text{sp}(g) + 1 \pmod{2}$ otherwise. We find R_1 and R_2 in Las Vegas $O(d^2 + \log q)$ (Proposition 2.12). A representative is $R_1^a R_2^{\text{sp}(g)}$. \square

We can now prove our main result for the orthogonal groups. If q is odd and Q is of $-$ type, we assume that the discrete log of γ has been precomputed in (2). We only give the case where q is odd, d is even, and the form is of $-$ type, as the other cases largely similar.

Proof. For (1), we first find a canonical isometry X from the standard form to F in $O(d^\omega + d \log q)$ 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 $\lambda = \sqrt{\tau(g)\gamma^{-1}}$, $z = c_0c(\lambda)$, and $C = C_0^-C^-(\lambda)$. We then let $h = g^{X^{-1}}C^{-1}$, find $a = \det(h)$ and $b = \text{sp}(h)$ in $O(d^\omega + \log q)$ field operations. We map g to $r_0^{b'}r_1^bz$, 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 $r_0^{b'}r_1^bc^k$. For (3) we write down R_0 and R_1 from §3 in $O(d^2 + \log q)$, then the representative is $(R_0^{b'}R_1^bC)^X$. \square

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

4. APPLICATION: CONJUGACY

Suppose that we can solve the element conjugacy problem in the group Δ . In this section, we briefly describe how to solve the same problem for groups G with $\Omega \leq G \leq \Delta$. This is a slight generalisation of the results of [Wal80], and is based on the following lemma:

Lemma 4.1. *Let Δ be a group, A a finite group, and $\phi : \Delta \rightarrow A$ an epimorphism. Let Ω be the kernel of ϕ . Suppose G is a group with $\Omega \leq G \leq \Delta$. Given g in G , the G -classes contained in g^Δ correspond to the elements of $A/\phi(C_\Delta(g)G)$ under the map*

$$(g^h)^\Delta \mapsto \phi(C_\Delta(g)Gh)$$

for h in Δ .

Proof. Clearly every G -class in g^Δ is of the form $(g^h)^G$ for some $h \in \Delta$. Now $(g^h)^G = (g^{h'})^G$ if and only if $g^{hg'} = g^{h'}$ for some $g' \in G$, that is, $hg'h'^{-1}$ is in $C_\Delta(g)$ for some $g' \in G$. Since G is normal, this is equivalent to h being in $C_\Delta(g)Gh'$, which means $C_\Delta(g)Gh = C_\Delta(g)Gh'$. Since $A/\phi(C_\Delta(g)G)$ is naturally isomorphic to $\Delta/C_\Delta(g)G$, we are done. \square

Hence, in order to compute the classes in G from the classes in Ω , we need to know the images of centralisers under ϕ and we need representatives $h_a \in \phi^{-1}(a)$ for all $a \in A$. If G is not normal in Δ , we need to apply this lemma more than once: since Δ/Ω is soluble for our groups, every G with $\Omega \leq G \leq \Delta$ must be subnormal in Δ .

The basic problems to be solved for G are:

- (1) find a set of representatives of the conjugacy classes of G ;
- (2) given $x \in G$ find $g \in G$ such that x^g is a canonical class representative; and
- (3) given a class representative x , find generators for $C_G(x)$.

These problems justify the need for canonical coset representatives in the previous sections. Problem (1) is only possible for relatively small groups, but if our algorithms give canonical elements we can solve (2) and (3) without first solving (1). It would be possible to give algorithms conjugating an element to any other element in the same class, but it would be less memory efficient. Using class representatives allows us to work with a single element x (since the representative itself is implicit in the algorithm but does not need to be written down). Class representatives also simplify the centraliser problem (3), and allow us to compare results between different runs of our algorithm. A detailed description of these algorithms will be given in [HM07].

A similar, but more complex, application is the construction of maximal subgroups of classical groups. Usually these are constructed as matrix groups preserving any convenient form and then mapped via an isometry to preserve the same classical form as the standard classical group defined by MAGMA [HRD05]. This results in different conjugates of the maximal subgroup being found on different runs of the same procedure, whereas using Theorem 1.1 the *same*

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

Type	d	p					3^i			2^i				
		5	17	47	73	10000019	3^6	3^{11}	3^{16}	2^5	2^{10}	2^{20}	2^{40}	2^{80}
o	15	1	1	1	1	1	1	2	5					
	55	4	9	9	9	11	11	28	184					
	95	11	27	27	28	34	45	140	1083					
+	20	1	1	1	1	1	1	3	10	–	–	–	4	4
	60	4	11	10	11	13	13	38	246	–	1	12	60	78
	100	12	28	28	27	33	50	153	1408	2	7	57	311	413
–	20	1	1	2	1	1	1	3	10	–	–	–	4	3
	60	4	11	11	11	14	14	36	256	–	1	12	60	82
	100	11	28	27	26	33	48	148	1373	4	7	56	289	390

subgroup can now be constructed each time. This is not currently essential, but is often useful: for example when investigating containments between subgroups.

5. TIMINGS

In this section we present various tables of timings data for a MAGMA v2.14-9 [BC07] 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 to find coset representatives for elements of the general orthogonal group lies between that taken to compute the spinor norm and to find coset representatives in the conformal orthogonal group.

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.

REFERENCES

- [Asc84] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.
- [Bab97] László Babai. Randomization in group algorithms: conceptual questions. In *Groups and computation, II (New Brunswick, NJ, 1995)*, pages 1–17. Amer. Math. Soc., Providence, RI, 1997.
- [BC07] W. Bosma and J.J. Cannon. *Handbook of Magma functions*. School of Mathematics and Statistics, University of Sydney, Sydney, 2.14 edition, 2007.
- [BCS97] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1997.
- [BGM93] I.F. Blake, S. Gao, and R.C. Mullin. Explicit factorization of $x^{2^k} + 1$ over \mathbf{F}_p with prime $p \equiv 3 \pmod{4}$. *Appl. Algebra Engrg. Comm. Comput.*, 4(2):89–94, 1993.
- [Bri06] John R. Britnell. Cyclic, separable and semisimple transformations in the finite conformal groups. *J. Group Theory*, 9(5):571–601, 2006.

TABLE 3. Coset representatives in $\text{CO}_d^e(q, Q)$

Type	d	p					3^i			2^5	2^{10}	2^{20}	2^{40}	2^{80}
		5	17	47	73	10000019	3^6	3^{11}	3^{16}					
o	15	3	4	4	4	6	3	5	13					
	55	33	48	55	47	59	46	72	392					
	95	147	201	184	176	211	189	317	2342					
+	20	6	7	7	7	10	7	10	34	1	2	4	8	14
	60	46	62	68	65	77	76	148	936	17	18	26	124	170
	100	168	224	209	226	257	305	627	5645	49	67	127	553	629
-	20	7	9	9	9	11	153	15	40	1	1	3	7	11
	60	50	72	71	70	90	244	196	1168	14	12	25	131	154
	100	153	225	217	229	257	474	799	7969	71	60	119	553	736

[Bro01] 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.

[Bro03] P.A. Brooksbank. Constructive recognition of classical groups in their natural representation. *J. Symbolic Comput.*, 35(2):195–239, 2003.

[CMT04] Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor. Computing in groups of Lie type. *Math. Comp.*, 73:1477–1498, 2004.

[GCL92] K.O. Geddes, S.R. Czapora, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992.

[Gro02] L.C. Grove. *Classical groups and geometric algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[HM07] Sergei Haller and Scott H. Murray. Computing conjugacy in finite classical groups. Unpublished, 2007.

[HRD05] D.F. Holt and C.M. Roney-Dougal. Constructing maximal subgroups of classical groups. *LMS J. Comput. Math.*, 8:46–79, 2005.

[JLPW95] C. Jansen, K. Lux, R. Parker, and R. Wilson. *An Atlas of Brauer Characters*. Oxford University Press, Oxford, UK, 1995.

[KL90] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*. Cambridge University Press, Cambridge, 1990.

[Lan93] Serge Lang. *Algebra*. Addison-Wesley Publishing Co., Reading, Mass., third edition, 1993.

[LG01] 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.

[Lüb] F. Lübeck. <http://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol>.

[Ser03] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[Sta06] M.J. Stather. *Algorithms for Computing with Finite Matrix Groups*. PhD thesis, University of Warwick, 2006.

[Str69] V. Strassen. Gaussian elimination is not optimal. *Numer. Math.*, 13:354–356, 1969.

[SZ93] Gary M. Seitz and Alexander E. Zalesskii. On the minimal degrees of projective representations of the finite Chevalley groups. II. *J. Algebra*, 158(1):233–243, 1993.

[Tay92] D.E. Taylor. *The geometry of the classical groups*. Heldermann Verlag, Berlin, 1992.

[Wal80] G. E. Wall. Conjugacy classes in projective and special linear groups. *Bull. Austral. Math. Soc.*, 22(3):339–364, 1980.

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, UNIVERSITY OF ST ANDREWS, FIFE KY16 9SS, UK.
 E-mail address: colva@mcs.st-and.ac.uk