On intersections of classical groups

Peter A. Brooksbank E.A. O'Brien

Abstract

We describe the structure of the subgroup of the general linear group defined over a finite field that preserves two bilinear or sesquilinear forms of the same classical type, at least one of which is non-degenerate. This description underpins an algorithm to construct the intersection of two classical groups of the same type.

1 Introduction

A long-standing and difficult algorithmic problem is the following: *if G and H are two finite subgroups of a common parent group P, determine explicitly $G \cap H$.*

If P is a permutation group, then no polynomial-time algorithm is known to solve the problem; indeed the problem was shown by Luks [9] to be polynomial-time equivalent to other hard permutation group problems, such as set stabilizer. Existing algorithms to solve the problem employ variations of "back track". If $P \leq \mathrm{GL}(n, \mathrm{GF}(q))$, then the approach is practical only for very modest values of n and q. For a discussion of these techniques, see [13, §3.3].

In this paper we provide an explicit description of the group of linear transformations that preserves a pair of bilinear or sesquilinear forms of the same classical type (that is, alternating, symmetric or hermitian) provided that at least one of them is non-degenerate. This description is inspired by the recent work of Goldstein & Guralnick [5]. Consequently we develop an efficient algorithm to construct the intersection of two groups that preserve such forms.

The first author thanks the Department of Mathematics at the University of Auckland for its hospitality while this work was done. Both authors were supported in part by the Marsden Fund of New Zealand via grant UOA 412. We thank Robert Guralnick for providing us with a preprint of [5] and Allan Steel for assistance with our implementation. 2000 *Mathematics Subject Classification*. Primary 20C20, 20C40.

Let M and N be matrices representing bilinear or sesquilinear forms of the same classical type, with M nonsingular. Let G and H be the groups of linear transformations that preserve M and N respectively. An elementary calculation (Theorem 2.5) shows that $G \cap H$ is precisely the subgroup of G that centralises the matrix $A = NM^{-1}$.

In Section 2 we demonstrate that A has the special property relative to M of being *self-adjoint*, and Proposition 2.7 describes the structure of the centraliser of A in G. One consequence of this description is that the centraliser computation reduces to finding centralisers of the primary components of the $F[x]$-module determined by the action of A in some corresponding group of isometries.

In Section 3 we specialise to the case where A determines a primary module – namely, A has minimal polynomial of the form $p(x)^m$ for $p(x)$ irreducible over F – and determine the structure of the centraliser of A in various cases.

In Section 4 we present an algorithm to construct the group of invertible matrices that preserve both M and N. This uses the general results obtained in Section 3 together with matrix calculations to handle various special cases. The result is a practical procedure that will produce the desired group for a very large proportion of input pairs of forms.

If the two forms have the same type but are both singular, then this approach does not apply. Furthermore, the structures of the intersections are much more diverse; in [3] we present an alternative algorithm to solve this problem.

2 Self-adjoint matrices

Let F be a field of size $q = p^k$ for prime p and integer $k \geq 1$, and let $V = F^n$. Let $\mathbb{M}(n, F)$ be the set of $n \times n$ matrices with entries in F. We will often regard $\mathbb{M}(n, F)$ as an algebra over F, having group of units $\mathrm{GL}(n, F)$. If k is even, let L be the subfield of F fixed elementwise by the involutory automorphism $x \mapsto x^{\sqrt{q}}$; otherwise let $L = F$. Let α be an automorphism of F fixing L. Let $\mathcal{C}(n, F)$ denote the set of all matrices $M \in \mathbb{M}(n, F)$ satisfying $M = \varepsilon(M^\alpha)^{\mathrm{tr}}$, where $\varepsilon \in \{1, -1\}$, $\varepsilon = 1$ whenever α is nontrivial, and $X \mapsto X^{\mathrm{tr}}$ denotes transposition. Thus each $M \in \mathcal{C}(n, F)$ is the matrix representing a classical form on V. We say that M has *symplectic type* if $\varepsilon = -1$, *unitary type* if α is nontrivial, or *orthogonal type* otherwise. The bilinear or sesquilinear form associated with M is computed via the assignment $(u, v) := uM(v^\alpha)^{\mathrm{tr}}$ for $u, v \in V$.

For $M \in \mathcal{C}(n, F)$, let F_0 denote the fixed field of α. Thus $F_0 = L$ if M has unitary type, and

$F_0 = F$ otherwise. We define the *isometry group of* M to be the set

$$\mathrm{Isom}(M) \;=\; \{X \in \mathrm{GL}(n,F)\colon XM(X^\alpha)^{\mathrm{tr}} = M\}. \tag{1}$$

We shall often denote the isometry group of M by $\mathrm{Sp}(M)$, $\mathrm{GU}(M)$ or $\mathrm{GO}(M)$ - the symplectic, general unitary, or general orthogonal group of M - if the type of M is known. Observe that our definition of $\mathrm{GO}(M)$ coincides with $\mathrm{Sp}(M)$ if $\mathrm{char}(F) = 2$; thus we consider $\mathrm{GO}(M)$ only in odd characteristic. A matrix $A \in \mathbb{M}(n,F)$ is *self-adjoint relative to* $M \in \mathcal{C}(n,F)$ if $AM = M(A^\alpha)^{\mathrm{tr}}$. The following is an easy extension of [5, Lemma 2.3].

Lemma 2.1 *Let $M \in \mathcal{C}(n,F)$, let A be self-adjoint relative to M, and let $f(x) \in F[x]$. Then $f(A)M = Mf(A^\alpha)^{\mathrm{tr}}$. In particular, if M has symplectic or orthogonal type, then $f(A)$ is always self-adjoint, whereas if M has unitary type, then $f(A)$ is self-adjoint precisely when $f(x)$ has coefficients in F_0.*

The next two lemmas concern self-adjointness relative to nondegenerate forms of unitary type. For convenience, denote the image of $\xi \in F$ under the involutory automorphism α simply by $\overline{\xi}$. Also, for $f(x) \in F[x]$, let $\overline{f}(x)$ denote the polynomial obtained from f by applying α to its coefficients.

Lemma 2.2 *Let $M \in \mathcal{C}(n,F)$ be nonsingular of unitary type and let A be self-adjoint relative to M. Then the minimal polynomial of A over F has coefficients in F_0.*

Proof. Since A is self-adjoint relative to M, and M is nonsingular, it follows that A is similar to $\overline{A}^{\mathrm{tr}}$. However it is well known (see, for example, [14]) that $\overline{A}^{\mathrm{tr}}$ is similar to $\overline{A}$. In particular A and $\overline{A}$ have the same minimal polynomial over F. Clearly if $m_A(x)$ is the minimal polynomial of A, then $m_{\overline{A}}(x) = \overline{m_A}(x)$, whence $m_A(x) = \overline{m_A}(x)$, as claimed. □

Lemma 2.3 *Let $M \in \mathcal{C}(n,F)$ be nonsingular of unitary type and let A be self-adjoint relative to M having minimal polynomial $m_A(x) = p(x)^c$, where $p(x)$ is irreducible over F_0 and has even degree. Then $m_A(x)$ factors over $F[x]$ as $m_A(x) = f(x)\overline{f}(x)$ and the nullspaces of $f(A)$ and $\overline{f}(A)$ are complementary maximal totally isotropic spaces.*

Proof. Suppose that $p(x) \in F_0[x]$ has degree $2l$, and let ω be a root of $p(x)$ in some extension field K of F. If $s = \sqrt{q}$ is the order of F_0, then $\omega, \omega^s, \omega^{s^2}, \ldots, \omega^{s^{2l-1}}$ are the distinct roots of $p(x)$ in K. Since $[F_0(\omega)\colon F_0] = [F(\omega)\colon F] = l$, it follows that ω is the root of some irreducible polynomial $r(x) \in F[x]$ of degree l. Hence $r(x) = (x-\omega)(x-\omega^q)\ldots(x-\omega^{q^{l-1}})$ and $p(x)/r(x) = (x-\omega^s)(x-(\omega^s)^q)\ldots(x-(\omega^s)^{q^{l-1}}) = \overline{r}(x)$.

Let $f(x) = r(x)^c$, let U be the nullspace of $f(A)$ and W be the nullspace of $\overline{f}(A)$. Fix $w_0 \in W$ and let w be any vector in W. Since the restriction of $f(A)$ to W is nonsingular, there exists $w_1 \in W$ with $w = w_1 f(A)$. Now we compute

$$(w_0, w) \;=\; w_0 M \overline{w}^{\mathrm{tr}} \;=\; w_0 M \overline{w_1 f(A)}^{\mathrm{tr}} \;=\; w_0 M \overline{f(A)}^{\mathrm{tr}} \overline{w_1}^{\mathrm{tr}} \;=\; w_0 \overline{f}(A) M \overline{w_1}^{\mathrm{tr}} \;=\; 0.$$

The penultimate equality follows from Lemma 2.1 applied to $\overline{f}(x)$ and the last follows from the fact that W is the nullspace of $\overline{f}(A)$. Hence W is totally isotropic and, by symmetry, so is U. Since $V = U + W$ and U and W are totally isotropic, it follows that they have equal dimension; hence there are maximal totally isotropic spaces. □

Our next result gives a fundamental decomposition of the space $V = F^n$ into A-invariant submodules (cf. [5, Theorem 2.6]).

Lemma 2.4 *Let $M \in \mathcal{C}(n, F)$ be nonsingular and let A be self-adjoint relative to M. Let*

$$m_A(x) = p_1(x)^{c_1} p_2(x)^{c_2} \dots p_t(x)^{c_t}$$

be the decomposition of the minimal polynomial of A into irreducibles over F_0, and let V_i be the nullspace of $p_i(A)^{c_i}$ ($1 \le i \le t$). Then $V_1 \oplus V_2 \oplus \dots \oplus V_t$ is an A-invariant decomposition of V. Moreover, relative to the form associated with M, the subspaces V_i are nonsingular and mutually orthogonal.

Proof. It is a consequence of elementary linear algebra that V is the direct sum of the A-invariant subspaces V_i. That these subspaces are mutually orthogonal follows from an argument similar to that in the proof of Lemma 2.3; see also the proof of [5, Theorem 2.6]. Since the form represented by M is nondegenerate, it follows immediately that the V_i are nonsingular. □

The next result is the key to constructing intersections of classical groups (cf. [5, Lemma 2.2]).

Theorem 2.5 *Let $M, N \in \mathcal{C}(n, F)$ be of the same type with M nonsingular. Then $A := NM^{-1}$ is self-adjoint relative to M, and $\mathrm{Isom}(M) \cap \mathrm{Isom}(N) = C_{\mathrm{Isom}(M)}(A)$, the centraliser of A in $\mathrm{Isom}(M)$.*

Proof. Let $M, N \in \mathcal{C}(n, F)$ be of the same type and let $A = NM^{-1}$. Then, since M and N both satisfy the equation $(Y^\alpha)^{\mathrm{tr}} = \varepsilon Y$, we have

$$M(A^\alpha)^{\mathrm{tr}} \;=\; M(M^{-\alpha})^{\mathrm{tr}} (N^\alpha)^{\mathrm{tr}} \;=\; \varepsilon^2 N \;=\; AM,$$

and A is self-adjoint relative to M. Next, $X \in \mathrm{Isom}(M)$ centralises A if and only if

$$N \;=\; AM \;=\; XAX^{-1}M \;=\; XAM(X^{\alpha})^{\mathrm{tr}} \;=\; XN(X^{\alpha})^{\mathrm{tr}}.$$

Thus $X \in C_{\mathrm{Isom}(M)}(A)$ if and only if $X \in \mathrm{Isom}(M) \cap \mathrm{Isom}(N)$. $\square$

In our description of $\mathrm{Isom}(M) \cap \mathrm{Isom}(N)$, and particularly in the algorithm that constructs this group, we often find it convenient to change the basis of V. The following result, whose proof is an elementary calculation, facilitates this conversion.

Lemma 2.6 *Let $M \in \mathcal{C}(n, F)$, let A be self-adjoint relative to M, and let $B \in \mathrm{GL}(n, F)$. Then the following hold:*

1. *$M' := BM(B^{\alpha})^{\mathrm{tr}}$ is an element of $\mathcal{C}(n, F)$ of the same type as M;*
2. *$A' := BAB^{-1}$ is self-adjoint relative to M'; and*
3. *$C_{\mathrm{Isom}(M)}(A) \;=\; B^{-1}C_{\mathrm{Isom}(M')}(A')B$.*

If M has symplectic type, then the self-adjoint matrix A in Theorem 2.5 has the stronger property that $vAMv^{\mathrm{tr}} = 0$ for all $v \in V$. (For fields of odd characteristic, however, this property is equivalent to the condition $AM = MA^{\mathrm{tr}}$.) The following result, which follows from [5, Theorem 2.6] and [5, Lemma 4.1], describes the intersection of two symplectic groups.

Proposition 2.7 *Let $M \in \mathcal{C}(2m, F)$ be nonsingular of symplectic type, and let A be self-adjoint relative to M. Then there is a change-of-basis matrix $B \in \mathrm{GL}(2m, F)$ such that*

$$A' = BAB^{-1} = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} \quad \textit{and} \quad M' = BMB^{\mathrm{tr}} = \begin{pmatrix} 0 & \Sigma \\ -\Sigma & 0 \end{pmatrix}, \tag{2}$$

where Σ is symmetric and J is self-adjoint relative to Σ. Furthermore, $C_{\mathrm{Sp}(M')}(A')$ consists of all invertible matrices of the form $\left(\begin{smallmatrix} P & Q \\ R & S \end{smallmatrix}\right)$, where the block entries P, Q, R, S all centralise J and satisfy the constraints:

$$\begin{aligned} P\Sigma Q^{\mathrm{tr}} - Q\Sigma P^{\mathrm{tr}} &= 0 \\ R\Sigma S^{\mathrm{tr}} - S\Sigma R^{\mathrm{tr}} &= 0 \\ P\Sigma S^{\mathrm{tr}} - Q\Sigma R^{\mathrm{tr}} &= \Sigma \end{aligned} \tag{3}$$

For the subspaces V_i defined in Lemma 2.4, let A_i (respectively M_i) be the restriction of A (respectively M) to V_i. Then M_i is nondegenerate and A_i is self-adjoint relative to M_i. Combining Theorem 2.5 with Lemma 2.4 we see that the intersection of $\mathrm{Isom}(M)$ and $\mathrm{Isom}(N)$, where M is nonsingular, is the direct product of centralisers of the A_i in the groups $\mathrm{Isom}(M_i)$. In the next section we examine these centralisers in more detail.

3 Centralisers of primary components

Throughout this section we assume that A is a self-adjoint matrix relative to some $M \in \mathcal{C}(n, F)$, *and has minimal polynomial of the form* $p(x)^c$ for some irreducible polynomial $p(x) \in F_0[x]$. We will examine the structure of $C_{\mathrm{Isom}(M)}(A)$, the centraliser of A in $\mathrm{Isom}(M)$. Since Proposition 2.7 describes centralisers of self-adjoint matrices in the symplectic case, we will restrict our attention to matrices M that have orthogonal or unitary type. It is convenient to conjugate A to its generalised Jordan normal form, and replace M by a corresponding matrix as in Lemma 2.6. Note that if A is a scalar matrix, then $C_{\mathrm{Isom}(M)}(A) = \mathrm{Isom}(M)$. Our first result deals with the case when A is cyclic.

Lemma 3.1 *Let M be of unitary or orthogonal type and let A be a cyclic matrix self-adjoint relative to M. Assume that $p(x)$ has odd degree if M has unitary type (so that $p(x)$ is also irreducible over F). Then the following hold:*

1. *If M has orthogonal type then $C_{\mathrm{Isom}(M)}(A) = \{\pm 1\}$.*
2. *If M has unitary type then $C_{\mathrm{Isom}(M)}(A)$ is the group $\{X \in F[A] \colon X\overline{X} = 1\}$.*

Proof. Since A is cyclic, any matrix that centralises A may be written in the form $f(A)$ for some polynomial $f(x) \in F[x]$. Let $f^{(\alpha)}(x)$ denote the polynomial obtained from $f(x)$ by applying α to its coefficients. Thus $f^{(\alpha)}(x) = f(x)$ if M has orthogonal type, and $f^{(\alpha)}(x) = \overline{f}(x)$ if M has unitary type. By Lemma 2.1 applied to $f^{(\alpha)}(x)$, we have $f(A) \in \mathrm{Isom}(M)$ if and only if $f(A)M(f(A)^\alpha)^{\mathrm{tr}} = f(A)f^{(\alpha)}(A)M = M$. If M has orthogonal type, then $f^{(\alpha)}(A) = f(A)$ so that $f(A)^2 = 1$. If M has unitary type, then A is a matrix defined over F_0, so the condition $f(A)f^{(\alpha)}(A) = 1$ asserts that $f(A)\overline{f(A)} = 1$, as required. □

We next consider the case where the $F[x]$-module defined by the action of A is semisimple.

Lemma 3.2 *Let M be of unitary or orthogonal type and let A have minimal polynomial $p(x)$, where $p(x)$ has degree e and is irreducible over F. Then $C_{\mathrm{Isom}(M)}(A)$ is isomorphic to $\mathrm{Isom}(M^*)$, where, for an extension field K of F of degree e, $M^* \in \mathcal{C}(n/e, K)$ and has the same type as M.*

Proof. The generalised Jordan normal form of A is a block diagonal matrix of the form $\mathrm{diag}(J, J, \ldots, J)$, where $J \in \mathbb{M}(e, F_0)$ is irreducible over F. As in Lemma 2.6, by applying a change-of-basis matrix that centralises A, we may assume that M also has block diagonal form $\mathrm{diag}(M_1, \ldots, M_{n/e})$. (If $n = e$ this is trivial; for the general case, A preserves a nonsingular e-space and its orthogonal complement, and the assertion follows by induction.) Since A is

self-adjoint relative to M, we have $JM_i = M_i(J^\alpha)^{\rm tr} = M_iJ^{\rm tr}$ for all i. Since M is nonsingular, each M_i conjugates J to $J^{\rm tr}$, so it follows from [14, Theorem 2] that M_i is symmetric. (This tells us nothing new if M has orthogonal type but, if M has unitary type, it follows that M_i is defined over F_0.)

Write $g \in {\rm GL}(n,F)$ in block form also, say $g = [[X_{ij}]]$, where $X_{ij} \in \mathbb{M}(e,F)$. Then g centralises A if and only if each X_{ij} centralises J. Since J is irreducible over F, it follows that $X_{ij} = f_{ij}(J)$ for some $f_{ij}(x) \in F[x]$.

Let M_0 be any of the diagonal blocks of M and set $S := {\rm diag}(M_0, M_0, \ldots, M_0)$. Observe, for all i, that $M_iM_0^{-1}$ centralises J and hence belongs to the field $F[J]$. In the unitary case, moreover, α induces an involutory automorphism of $F[J]$ that fixes the subfield $F_0[J]$; as M and S are defined over F_0, it follows that α fixes MS^{-1}. Since $M^* := MS^{-1}$ is a block diagonal matrix, it lies in $\mathcal{C}(n/e, F[J])$ as required.

Applying Lemma 2.1 to $f^{(\alpha)}$, observe that $M_0(X_{ji}^\alpha)^{\rm tr} = M_0f_{ji}^{(\alpha)}(J^\alpha)^{\rm tr} = f_{ji}^{(\alpha)}(J)M_0$. Since J is defined over F_0 we have $f_{ji}^{(\alpha)}(J) = (f_{ji}(J))^\alpha = X_{ji}^\alpha$. It follows that $(X_{ji}^\alpha)^{\rm tr}M_0^{-1} = M_0^{-1}X_{ji}^\alpha$. Hence $gM(g^\alpha)^{\rm tr}S^{-1} = gMS^{-1}h$, where h, regarded as an element of $\mathbb{M}(n/e, F[J])$, is equal to $g^{\rm tr}$. It follows that $g \in {\rm GL}(n/e, F[J])$ is in ${\rm Isom}(M^*)$ if and only if

$$MS^{-1} \;=\; M^* \;=\; gM^*g^{\rm tr} \;=\; gMS^{-1}h \;=\; gM(g^\alpha)^{\rm tr}S^{-1},$$

which holds if and only if $gM(g^\alpha)^{\rm tr} = M$. □

We conclude this section by examining the case when M is of unitary type and the minimal polynomial of A splits over F. Recall that A is already assumed to be in generalised Jordan normal form.

Lemma 3.3 *Let M have unitary type and let A be self-adjoint to M having minimal polynomial $p(x)^c$ with $p(x)$ irreducible over F_0 of even degree. Then $A = \left(\begin{smallmatrix} J & 0 \\ 0 & \overline{J} \end{smallmatrix}\right)$, $M = \left(\begin{smallmatrix} 0 & H \\ \overline{H}^{\rm tr} & 0 \end{smallmatrix}\right)$ and $C_{{\rm Isom}(M)}(A)$ consists of matrices of the form $g = \left(\begin{smallmatrix} X & 0 \\ 0 & X^* \end{smallmatrix}\right)$, where X centralises J and $X^* = \overline{H^{-1}X^{-1}H}^{\rm tr}$.*

Proof. As in the proof of Lemma 2.3, write $p(x) = r(x)\overline{r}(x)$, let $U = \ker(r(A)^c)$ and $W = \ker(\overline{r}(A)^c)$; then U and W are complementary maximal totally isotropic spaces. The statements about A and M now follow easily. The centraliser of A in ${\rm GL}(n,F)$ preserves both U and W, so it follows that elements of $C_{{\rm Isom}(M)}(A)$ have the form $\left(\begin{smallmatrix} X & 0 \\ 0 & Y \end{smallmatrix}\right)$, where X and Y centralise J and $\overline{J}$ respectively. The final condition on Y follows directly from the fact that $gM\overline{g}^{\rm tr} = M$. □

4 Constructing intersections

In this section we present an algorithm to construct the intersection of two classical groups preserving bilinear or sesquilinear classical forms of the same type.

In Section 4.1 we outline the main procedure that constructs the intersection of the full groups of isometries of two matrices M and N representing forms of the same type. In Section 4.2 we describe the modifications that are necessary to obtain the intersection of two classical groups of the same type (we exclude orthogonal groups in characteristic 2). Sections 4.3 and 4.4 deal with the specifics of writing down a generating set for $\mathrm{Isom}(M) \cap \mathrm{Isom}(N)$.

4.1 The group preserving two forms

The input to the main procedure consists of matrices $M, N \in \mathcal{C}(n, F)$ representing classical forms of the same type, where M, say, is nonsingular. The output is a generating set for the subgroup of $\mathrm{GL}(n, F)$ that preserves both of these forms.

Intersection of Isometry Groups (M, N)
/ Input: Matrices $M, N \in \mathcal{C}(n, F)$ of the same type, with M nonsingular */*
/ Output: A generating set for $\mathrm{Isom}(M) \cap \mathrm{Isom}(N)$ */*

Step 0. Let α denote the automorphism of F associated with the type of M and N, and let F_0 be the subfield of F fixed by α.

Step 1. Set $A := NM^{-1}$ and compute the minimal polynomial $m_A(x)$ over F.

Step 2. Obtain a factorisation $m_A(x) = p_1(x)^{c_1} p_2(x)^{c_2} \dots p_t(x)^{c_t}$, where each $p_i(x) \in F_0[x]$ is irreducible over F_0.

Step 3. For $1 \leq i \leq t$, compute a basis $\mathcal{B}_i$ for the nullspace V_i of the matrix $p_i(A)^{m_i}$ of dimension n_i. The concatenation of the bases $\mathcal{B}_i$ gives a change-of-basis matrix B such that BAB^{-1} is a block diagonal matrix $\mathrm{diag}(A_1, A_2, \dots, A_s)$, and $BM(B^\alpha)^{\mathrm{tr}}$ is a block diagonal matrix $\mathrm{diag}(M_1, M_2, \dots, M_s)$.

Step 4. For $1 \leq i \leq s$, write down a generating set $\mathcal{T}_i$ for the subgroup $C_{\mathrm{Isom}(M_i)}(A_i)$ of $\mathrm{GL}(n_i, F)$; obtain a subset $\mathcal{S}_i$ of $\mathrm{GL}(n, F)$ whose elements induce the corresponding element of $\mathcal{T}_i$ on V_i and the identity on $V_1 \oplus \dots \oplus V_{i-1} \oplus V_{i+1} \oplus \dots \oplus V_s$.

Step 5. Set $\mathcal{S} := \mathcal{S}_1 \cup \mathcal{S}_2 \cup \dots \cup \mathcal{S}_s$, and return the set $\{C^{-1}XC \colon X \in \mathcal{S}\}$.

We now comment on the steps of the algorithm.

Step 1. Various algorithms exist to construct the minimal polynomial of a matrix defined over a finite field; see, for example, [7, p. 226].

Step 2. Algorithms to factorise polynomials defined over finite fields are discussed in [12, Chapter 14].

Step 3. The nullspace of a matrix is obtained readily by solving a system of linear equations over F. For further details see [7, p. 223].

Step 4. If M (and therefore N) has symplectic type, the subgroups $C_{\mathrm{Isom}(M_i)}(A_i)$ are described in Proposition 2.7; this description is used in Section 4.3 to write down generators.

If M has unitary or orthogonal type, the results of Section 3 may be used to write down generators for $C_{\mathrm{Isom}(M_i)}(A_i)$ for certain matrices A_i. We describe how this is done in more detail in Section 4.4 and give generating sets for other specific cases.

4.2 Intersections of general classical groups

We define G to be a *classical subgroup* of $\mathrm{GL}(V)$ if it preserves a bilinear or sesquilinear form on V having matrix $M \in \mathcal{C}(n, F)$, and one of the following holds:

1. M has symplectic type, and $G = \mathrm{Sp}(M)$.
2. M has unitary type, and $\mathrm{SU}(M) \leq G \leq \mathrm{GU}(M)$, where $\mathrm{SU}(M)$ is the subgroup of $\mathrm{GU}(M)$ consisting of determinant 1 matrices; thus $GU(M)/SU(M)$ is a cyclic group of order $q + 1$.
3. M has orthogonal type, and $\Omega(M) \leq G \leq \mathrm{GO}(M)$, where $[\mathrm{GO}(M) \colon \mathrm{SO}(M)] = 2$ (recall q is odd in this case) and $\Omega(M)$ is the derived group of $\mathrm{GO}(M)$.

We now present an algorithm to solve the following algorithmic problem:

> *Given classical subgroups G, H of $\mathrm{GL}(V)$ of the same type, find generators for $G \cap H$.*

The algorithm of Niemeyer and Praeger [11] can be used to decide whether the given groups G and H satisfy the necessary requirements. We note that kernels of homomorphisms can be computed effectively in our limited context.

Classical Intersection $(G,\ H)$

/ Input: Classical subgroups $G = \langle X \rangle$ and $H = \langle Y \rangle$ of $\mathrm{GL}(n, F)$ of the same type */*

/ Output: A generating set for $G \cap H$ */*

Step 0. Find matrices M and N for the forms preserved by G and H respectively.

Step 1. Compute $K := \mathrm{Isom}(M) \cap \mathrm{Isom}(N)$ using the procedure in Section 4.1.

Step 2. If M and N have unitary type, set $C := \{\xi \in F^* \colon \xi^{q+1} = 1\}$, and modify K as follows.

(a) Set $C_0 := \langle \det(x) \colon x \in X \rangle \cap \langle \det(y) \colon y \in Y \rangle \leq C$.

(b) Construct a homomorphism $\psi \colon K \to C/C_0$, sending $a \mapsto \det(a)C_0$.

(c) Replace K with $\ker(\psi)$.

Step 3. If M and N have orthogonal type, set $C := \{-1, 1\} \times \{-1, 1\}$, where $\{-1, 1\}$ is the multiplicative group $\mathbb{Z}_2$, and modify K as follows.

(i) */* Construct the spinor map $\sigma_M \colon \mathrm{GO}(M) \to \{-1, 1\}$ with respect to M */*

(a) Set $C_0 := \langle (\det(x), \sigma_M(x)) \colon x \in X \rangle \leq C$.

(b) Construct a homomorphism $\psi_M \colon K \to C/C_0$, sending $a \mapsto (\det(a), \sigma_M(a))C_0$.

(c) Replace K with $\ker(\psi_M)$.

(ii) */* Construct the spinor map $\sigma_N \colon \mathrm{GO}(N) \to \{-1, 1\}$ with respect to N */*

(a) Set $C_0 := \langle (\det(y), \sigma_N(y)) \colon y \in Y \rangle \leq C$.

(b) Construct a homomorphism $\psi_N \colon K \to C/C_0$, sending $a \mapsto (\det(a), \sigma_N(a))C_0$.

(c) Replace K with $\ker(\psi_N)$.

Step 4. Return K.

Commentary. In Step 0, the form for each group is obtained by constructing an isomorphism between the natural module for that group and its dual; see [2, Section 4.2].

In general the subgroup K constructed in Step 1 will be an overgroup of $G \cap H$.

In the unitary case, Step 2 modifies K so that it contains only elements having determinant equal to that of some element of $G \cap H$.

In the orthogonal case, Step 3 modifies K so that it contains only elements having appropriate spinor norms relative to M and N. The spinor maps σ_M and σ_N are constructed using Wall forms; see [15, p. 163].

4.3 Symplectic groups

Let $A = A_i$ and $M = M_i$ be the block matrices obtained in Step 3 of the main algorithm in Section 4.1. By Proposition 2.7 we may assume that $A = \left(\begin{smallmatrix} J & 0 \\ 0 & J \end{smallmatrix}\right)$ and $M = \left(\begin{smallmatrix} 0 & \Sigma \\ -\Sigma & 0 \end{smallmatrix}\right)$, where $J, \Sigma \in \mathbb{M}(m, F)$ and Σ is symmetric. Let $\mathcal{B}$ be any $\mathrm{GF}(p)$-basis for the solution space of the linear system $\{Q \in \mathbb{M}(m, F) \colon JQ = QJ,\ \Sigma Q^{\mathrm{tr}} = Q\Sigma\}$, and set

$$\mathcal{S} := \left\{ \begin{pmatrix} I & Q \\ 0 & I \end{pmatrix},\ \begin{pmatrix} I & 0 \\ Q & I \end{pmatrix} \colon Q \in \mathcal{B} \right\} \tag{4}$$

The block entries of the matrices in $\mathcal{S}$ clearly satisfy equation (3), so $\mathcal{S} \subseteq C_{\mathrm{Sp}(M)}(A)$.

If J is a cyclic matrix (one whose characteristic and minimal polynomials coincide) then its centraliser in $\mathbb{M}(m, F)$ is simply $F[J]$, the subalgebra of $\mathbb{M}(m, F)$ generated by J. In that case, the block entries P, Q, R, S in equation (3) are all polynomials in J. Moreover, since J is self-adjoint relative to Σ, it follows from Lemma 2.1 that P, Q, R, S are all self-adjoint relative to Σ. Hence the conditions in equation (3) reduce to the single constraint $PS - QR = 1$, and it follows that $g \in \mathrm{Sp}(M)$ if and only if $g \in \mathrm{SL}(2, F[J])$. Hence, if J is cyclic, the elements of $\mathcal{S}$ are analogues of transvections in $\mathrm{SL}(2, F[J])$, where $F[J]$ is a local ring. It follows from [8, Proposition 1.3.5] that $\mathcal{S}$ generates $C_{\mathrm{Sp}(M)}(A)$ in this case.

If J is a scalar matrix, it is well known that $\mathcal{S}$ generates $C_{\mathrm{Sp}(M)}(A) = \mathrm{Sp}(M)$ (see, for example, [2, Section 5]).

Recently, Goldstein and Guralnick [6] proved that $\mathcal{S}$ always generates $C_{\mathrm{Sp}(M)}(A)$.

4.4 Orthogonal and unitary groups

We now assume that $M \in \mathcal{C}(n, F)$ has orthogonal or unitary type and that $A \in \mathrm{GL}(n, F)$ is self-adjoint relative to M having minimal polynomial $p(x)^c$ for some $p(x)$ irreducible over F_0. We begin by describing generating sets for each of the cases considered in Section 3.

Lemma 3.1: Here A is cyclic and $p(x)$ is irreducible over F. In the orthogonal case there is nothing to do since $C_{\mathrm{GO}(M)}(A) = \{\pm 1\}$. Suppose that M has unitary type. If A is irreducible, then $F[A]$ is a field and $C_{\mathrm{GU}(M)}(A) = \mathrm{GU}(1, F[A])$. In general, however, constructing generators for the norm group of a given ring is a difficult problem; Lemma 4.3 describes such generators for the case when $p(x)$ is linear.

Lemma 3.2: This is the semisimple case in which $C_{\mathrm{Isom}(M)}(A)$ is the full group of isometries of a suitable form over an extension field; it is trivial to write down generators here.

Lemma 3.3: Here M has unitary type and $p(x)$ splits over F as a product of an irreducible polynomial and its conjugate. The key to constructing generators for $C_{\mathrm{GU}(M)}(A)$ is to construct the centraliser in $\mathrm{GL}(n,F)$ of a given matrix J. This can be done using methods described in [10, Chapter 2], or using more general techniques for constructing the group of units of a matrix algebra (see, for example, [3, Section 2]).

In the remainder of this section we assume that the minimal polynomial of A has the form $(x-\lambda)^c \in F_0[x]$, where $c > 1$. Assume further that A is in Jordan normal form. We describe generating sets for $C_{\mathrm{Isom}(M)}(A)$ in three other important cases; the results are all readily verified by direct calculation.

Lemma 4.1 *Suppose that $c = 2$ and that A is a block diagonal matrix*

$$\mathrm{diag}(J_2(\lambda), J_2(\lambda), \ldots, J_2(\lambda)),$$

where $J_2(\lambda)$ denotes the 2×2 Jordan block $\left(\begin{smallmatrix}\lambda & 1\\ 0 & \lambda\end{smallmatrix}\right)$. Then, relative to a suitable basis, A has the form $\left(\begin{smallmatrix}\lambda I & I\\ 0 & \lambda I\end{smallmatrix}\right)$, where I is the identity of $\mathrm{GL}(n/2,F)$, and M has the form $\left(\begin{smallmatrix}M_1 & M_2\\ M_2^\alpha & 0\end{smallmatrix}\right)$ for symmetric matrices M_1, M_2. Furthermore, $C_{\mathrm{Isom}(M)}(A)$ is generated by matrices of the form

$$\begin{pmatrix} X & Q \\ 0 & X \end{pmatrix} \tag{5}$$

as X runs over a generating set for $\mathrm{Isom}(M_2)$ and, for each X, Q runs over a suitable subset of matrices satisfying $QM_2(X^\alpha)^{\mathrm{tr}} + XM_2(Q^\alpha)^{\mathrm{tr}} = M_1 - XM_1(X^\alpha)^{\mathrm{tr}}$.

Lemma 4.2 *Suppose that $c = 2$ and A has the form $\lambda I + E_{n-1,n}$, where E_{ij} denotes the elementary matrix with 1 in position (i,j) and 0 in all other positions. Then, relative to a suitable basis, A and M have the form*

$$\begin{pmatrix} \lambda & 0 & 1 \\ 0 & \lambda I_{n-2} & 0 \\ 0 & 0 & \lambda \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & M_1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

respectively, where $M_1 \in \mathcal{C}(n-2,F)$ has the same type as M. Furthermore, $C_{\mathrm{Isom}(M)}(A)$ is generated by matrices of the form

$$\begin{pmatrix} \nu & 0 & 0 \\ 0 & I_{n-2} & 0 \\ 0 & 0 & \nu \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & v & \lambda \\ 0 & I_{n-2} & (w^\alpha)^{\mathrm{tr}} \\ 0 & 0 & 1 \end{pmatrix}, \tag{6}$$

where: $\nu = -1$ *if* M *has orthogonal type, and* ν *generates the subgroup* $\{\xi \colon \xi\overline{\xi} = 1\}$ *of* F^* *if* M *has unitary type;* X *runs over a generating set for* $\mathrm{Isom}(M_1)$*; and* v *runs over a basis for* F^{n-2}*,* $w = -vM_1$*, and* λ *satisfies* $\lambda + \lambda^\alpha = -vM_1(v^\alpha)^{\mathrm{tr}}$*.*

The final result in this section describes generators when A is cyclic having minimal polynomial $(x-\lambda)^n$ in the unitary case (recall that the analogous orthogonal case is covered by the first part of Lemma 3.1).

Lemma 4.3 *Suppose that* $c = n$ *and that* M *has unitary type. Then*

$$A = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \lambda & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}$$

and $C_{\mathrm{GU}(M)}(A)$ *is a direct product of the cyclic group* $\langle \mathrm{diag}(\nu, \nu, \dots, \nu) \colon \nu\overline{\nu} = 1 \rangle$ *of order* $q+1$ *and the subgroup consisting of all matrices of the form*

$$\begin{pmatrix} 1 & \xi_1 & \xi_2 & \dots & \xi_{n-2} & \xi_{n-1} \\ 0 & 1 & \xi_1 & \xi_2 & \dots & \xi_{n-2} \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & 1 & \xi_1 & \xi_2 \\ \vdots & \vdots & & & 1 & \xi_1 \\ 0 & 0 & \dots & \dots & 0 & 1 \end{pmatrix},$$

where the dot product $(\xi_1, \xi_2, \dots, \xi_{n-1}) \cdot \overline{(\xi_{n-1}, \xi_{n-2}, \dots, \xi_1)} = 0$*. Furthermore, this group is generated by a set of size* $(n-1)\log_p(|F|) + 1$*.*

5 Concluding remarks

We implemented the algorithm of Section 4 in MAGMA [1]; our implementation is publicly available. Its effectiveness is limited only by the cost of computing and factorising minimal polynomials. In practice, it constructs in at most one minute the intersection of classical groups of dimension in the hundreds defined over moderate sized fields.

Recall that, for orthogonal and unitary groups, we wrote down explicit generating sets for the intersection only for certain classes of matrices. By running over representatives of conjugacy classes of $\mathrm{GL}(d, q)$ we estimated, for small d and q, the proportion of elements covered by our analysis in Section 4.4; by one measure, more than 99% were covered. Typically the matrices A_i induced on the primary modules are cyclic. This observation is supported by the analysis of Fulman, Neumann & Praeger [4], who prove that, for fixed q, a matrix chosen uniformly at random from $\mathrm{GL}(d, q)$ is cyclic with probability approaching 1 as $d \to \infty$. Furthermore, it is possible to extend the case-by-case analysis to any outstanding case of interest.

References

[1] W. Bosma, J. Cannon and C. Playoust. The MAGMA algebra system I: The user language. J. Symbolic Comp. 24 (1997) 235–265.

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

[3] Peter A. Brooksbank and E.A. O'Brien. Constructing the group preserving a system of forms. Internat. J. Algebra Comput. To appear.

[4] Jason Fulman, Peter M. Neumann, and Cheryl E. Praeger. A generating function approach to the enumeration of matrices in classical groups over finite fields. Mem. Amer. Math. Soc. 176, Number 830 (2005).

[5] Daniel Goldstein and Robert M. Guralnick. Alternating forms and self-adjoint operators. J. Algebra 308 (2007), 330–349.

[6] Daniel Goldstein and Robert M. Guralnick. In preparation.

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

[8] Norbert H.J. Lacroix. Two-dimensional linear groups over local rings. Canad. J. Math. 21 1969 106–135.

[9] Eugene M. Luks. Permutation groups and polynomial-time computation. Groups and computation (New Brunswick, NJ, 1991), 139–175, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 11, Amer. Math. Soc., Providence, RI, 1993.

[10] Scott H. Murray. Conjugacy classes in maximal parabolic subgroups of the general linear group. PhD Thesis, University of Chicago, 2000.

[11] Alice C. Niemeyer and Cheryl E. Praeger. A recognition algorithm for classical groups over finite fields. Proc. London Math. Soc. (3) 77 (1998), no. 1, 117–169.

[12] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*, Cambridge University Press, 2002.

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

[14] O. Taussky and H. Zassenhaus. On the similarity transformation between a matrix and its transpose. Pacific J. Math. 9 (1959), 893–896.

[15] Donald E. Taylor. The geometry of the classical groups. Heldermann, Berlin, 1992.

Peter A. Brooksbank
Department of Mathematics
Bucknell University
Lewisburg, PA 17837
United States
pbrooksb@bucknell.edu

E.A. O'Brien
Department of Mathematics
University of Auckland
Private Bag 92019
New Zealand
obrien@math.auckland.ac.nz