Computing Isometry Groups of Hermitian Maps

Peter A. Brooksbank and James B. Wilson

Abstract. A theorem is proved on the structure of the group of isometries of an Hermitian map \( b : V \times V \to W \), where \( V \) and \( W \) are vector spaces over a finite field of odd order. Also a Las Vegas polynomial-time algorithm is presented which, given an Hermitian map, finds generators for, and determines the structure of its isometry group. The algorithm can be adapted to construct the intersection of the members in a set of classical subgroups of \( \text{GL}(V) \), yielding the first polynomial-time solution of this old problem. The approach develops new algorithmic tools for algebras with involution, which in turn have applications to other computational problems of interest. Implementations of the various algorithms in the MAGMA system demonstrate their practicability.

1. Introduction

The purpose of this paper is to expand the structural understanding of intersections of classical groups defined naturally on a common vector space, and to demonstrate the algorithmic practicability of computing such intersections. Just as classical groups in odd characteristic are defined in terms of isometries of Hermitian forms on a vector space, so intersections of classical groups are naturally described as isometries of Hermitian maps between vector spaces.

Let \( F_q \) denote the field of \( q \) elements. An \( F_q \)-bilinear map \( b : V \times V \to W \) between vector spaces \( V \) and \( W \) is Hermitian if there is a \( \theta \in \text{GL}(W) \) such that, for all \( u, v \) in \( V \),

\[
b(u, v) = b(v, u) \theta. \tag{1.1}
\]

The isometry group of \( b \) is

\[
\text{Isom}(b) = \{ f \in \text{GL}(V) : b(uf, vf) = b(u, v), \ \forall u, v \in V \}. 
\]

We define a general classical subgroup of \( \text{GL}(V) \) to be the group of isometries of a nondegenerate reflexive (symmetric, alternating, or Hermitian) form \( \varphi : V \times V \to F_{\varphi} \), where \( F_{\varphi} \) is a finite extension of \( F_q \).

With this notation we can state our first result.

Theorem 1.1. Let \( V \) and \( W \) be finite vector spaces over a finite field \( F_q \) of odd characteristic \( p \), \( b : V \times V \to W \) an Hermitian map, and \( 0 = V_0 < \cdots < V_t = V \) a composition series of \( V \) as an \( \text{Isom}(b) \)-module. Then the following hold.

(i) For each \( i \in \{1, \ldots, t\} \), there is a field extension \( F_i \) over which \( V_i = V_i/V_{i-1} \) becomes an \( F_i \)-vector space and \( \text{Isom}(b) \) acts on \( V_i \) as a general classical group in its defining representation.

(ii) There are subgroups \( H_1, \ldots, H_m \) of \( \text{Isom}(b) \), such that each \( H_j \) acts faithfully as a classical group on some (possibly several) \( V_i \) as in (i), and

\[
\text{Isom}(b) = O_p(\text{Isom}(b)) \times (H_1 \times \cdots \times H_m).
\]

Date: May 15, 2010.

Key words and phrases. \( \ast \)-algebra, Hermitian map, classical group, isometry group, polynomial-time algorithm.
(iii) The kernel of the induced action of $\text{Isom}(b)$ on $\bigoplus_{i=1}^{t} V_i$ is $O_p(\text{Isom}(b))$ and, evaluating $z \mapsto z + \sqrt{1 + z^2}$ as a power series, $O_p(\text{Isom}(b))$ is precisely
\[ \{ z + \sqrt{1 + z^2} : b(uz, v) = -b(u, vz), \forall u, v \in V, \text{ and } V_i z \subseteq V_{i-1}, \forall i, 1 \leq i \leq t \} \]

Our second result is an algorithmic version of Theorem 1.1. To compute with groups and rings of matrices it is helpful to employ randomization. The randomized algorithms used in this paper are of the *Las Vegas* variety: algorithms which guarantee correct output, but which may terminate with no output (an upper bound on the probability of the latter is prescribed by the user). An algorithm runs in polynomial time if the number of basic operations it uses is bounded by a polynomial in the length of the input. An Hermitian map $b : V \times V \to W$ over a field $F_q$ is input as an array of structure constants with respect to fixed bases for $V$ and $W$, and so the input length is $\dim V \cdot \dim W \cdot \log q$. We prove the following result.

**Theorem 1.2.** There is a polynomial-time Las Vegas algorithm which, given an Hermitian map $b : V \times V \to W$, where $V$ and $W$ are finite-dimensional vector spaces over a finite field of odd order, constructs a generating set for $\text{Isom}(b)$ and exhibits the structure described in Theorem 1.1. The algorithm uses $O(\{ \dim V + \dim W \} \log^2 q)$ basic operations.

The complexity estimate in Theorem 1.2 arises from the number of basic operations used to solve certain systems of linear equations. There is a deterministic variant of Theorem 1.2 for small characteristic, which simply replaces the Las Vegas algorithms cited in our proof with established deterministic algorithms for small characteristic; see Remark 2.1.

This work is motivated by the study of automorphisms of $p$-groups (see [ELO, Section 10] and [Wi1, Proposition 3.8]) and central products of $p$-groups (see [Wi2, Section 5]). A fundamental problem that arises from both studies is that of computing intersections of classical subgroups of $\text{GL}(V)$. With natural modifications, our methods provide complete solutions to this problem when $V$ has odd order, and partial solutions when $V$ has even order.

An intersection of general classical groups preserves every member of a set $\Phi$ of reflexive forms on $V$. Rather than deal with individual forms, it is helpful to work with the single Hermitian map $(\cap \Phi) : V \times V \to \bigoplus_{\varphi \in \Phi} F_{\varphi}$ defined by $(\cap \Phi)(u, v) = (\varphi(u, v) : \varphi \in \Phi)$ for all $u, v \in V$. It follows that
\[
\text{Isom}(\cap \Phi) = \{ f \in \text{GL}(V) : \varphi(uf, vf) = \varphi(u, v), \forall \varphi \in \Phi, \forall u, v \in V \}
\]
(1.2)
\[
= \bigcap_{\varphi \in \Phi} \text{Isom}(\varphi).
\]

In Equation (1.2) we do not require all of the forms in $\Phi$ to be of the same geometric type; each one may be symmetric, alternating, or Hermitian. In fact, we also allow the forms to be degenerate.

Through Equation (1.2) we connect Theorem 1.1 with a number of related results. In the language of intersections of classical groups, Wagner has shown that if $V$ and $W$ are (finite) vector spaces of odd order and $b : V \times V \to W$ is a nondegenerate Hermitian map, then $\text{Isom}(b)/O_p(\text{Isom}(b))$ is isomorphic to a product of classical groups [Wa, Theorem 3]; a proof using algebraic groups is given by Bayer-Fluckiger [BF, Section 1.6]. Using ring theory and operating from the perspective of Hermitian maps, [Wi1, Theorem 4.39] gives a proof of Theorem 1.1(ii). Also,
Goldstein and Guralnick explore the intersection of symplectic groups and determine, among other things, when such an intersection contains more than scalar matrices [GG, Sections 4–5].

In relation to Theorem 1.2, Brooksbank and O’Brien [BO1, Section 4] present a highly effective algorithm to construct the group preserving two reflexive forms of the same geometric type. Intersections of arbitrary sets of classical subgroups of $\text{GL}(V)$ are considered in [BO2, Section 4.4] using heuristic methods. While those heuristics have proven practical value, they often founder for inputs of fairly modest size, and cannot describe the structure of the resulting group. Theorem 1.2 applies to arbitrary systems of forms in odd characteristic, and determines the structure of the group.

We have not found a treatment of Hermitian maps, systems of forms, or intersections of classical groups which anticipates Theorem 1.1 parts (i) or (iii); in particular, the representation of $\text{Isom}(b)$ in relation to $O_p(\text{Isom}(b))$ and $\text{Isom}(b)/O_p(\text{Isom}(b))$ does not appear to have precedent in the literature. Part of the problem is that for algebraic groups it is customary to produce unipotent elements in the group by exponentiation of certain nilpotent elements in a Lie algebra. However, when the nilpotence class is larger than the characteristic (a situation that can easily arise in our context) exponentiation is impossible. In the proof of Theorem 1.1(ii) we overcome this obstacle by using the following power series in $(\mathbb{Z}[1/2])[\![x]\!]$: 

\begin{equation}
    x + \sqrt{1 + x^2} = 1 + x - 2 \sum_{n=1}^{\infty} C(n-1) \left( -\frac{1}{4} \right)^n x^n,
\end{equation}

where $C(j)$ is the $j^{th}$ Catalan integer. This map has many of the same desirable properties as exponentiation, but requires only division by 2.

Unfortunately, these power series tricks do not work when the base field of $b$ has characteristic 2. In that case, $U = O_2(\text{Isom}(b))$ may not split in $\text{Isom}(b)$ as it does in Theorem 1.1(ii). Unsurprisingly, Theorem 1.2 survives intact when $O_2(\text{Isom}(b)) \neq 1$. If $O_2(\text{Isom}(b)) \neq 1$, we can at least identify the types, dimensions, and fields of the classical groups involved in $\text{Isom}(b)/O_2(\text{Isom}(b))$.

**Overview of the paper.** In the spirit of earlier work of Weil [We], Wagner [Wa, Section 3], and [Wi1, Section 4.3], our strategy is to describe $\text{Isom}(b)$ in terms of certain units in an associative algebra that possesses a natural, involutory anti-automorphism $\ast$.

The basic theorems of $\ast$-algebras are laid out in Section 2. We see, in particular, that such algebras have a radical–semisimple structure analogous to that of ordinary matrix algebras. This section also contains the necessary algorithmic background.

Section 3 introduces Hermitian maps and describes their intimate connection with $\ast$-algebras. Parts (i) and (ii) of Theorem 1.1 are proved in that section.

In Section 4 we present polynomial-time algorithms for $\ast$-algebras of matrices. Over fields of odd characteristic, a result of Taft (Theorem 2.4) shows that the radical has a $\ast$-invariant semisimple complement. This splitting solves the (nontrivial) problem of lifting generators for $\text{Isom}(b)/O_p(\text{Isom}(b))$ to $\text{Isom}(b)$, leading to a proof of Theorem 1.1 parts (i) and (ii). For Theorem 1.2, an algorithmic version of Taft’s theorem is required, and is provided by Proposition 4.3. Although some algorithms for $\ast$-algebras were previously described in [Wi2, Corollary 5.9], no attention was given there to the associated group of units, and the algorithms presented here are much more practical than their predecessors.
In Section 5 we prove Theorem 1.1(iii), and also present the isometry group algorithm that establishes Theorem 1.2.

Sections 4 and 5 establish the polynomial-time complexity of our algorithms. In Section 6, we comment on aspects of our implementation of these algorithms in the MAGMA system and present the results from a range of performance tests that demonstrate the practicability of the methods.

2. Preliminaries

In this section we collect properties of *-algebras, and summarize the necessary algorithmic background. In the interest of exposition we restrict our summary to the specific contexts that arise in the subsequent sections.

We write \( \mathbb{F}_q \) for a finite field of order \( q \); \( V \) and \( W \) for finite-dimensional \( \mathbb{F}_q \)-vector spaces, and \( M_d(\mathbb{F}_q) \) for the set of \((d \times d)\)-matrices over \( \mathbb{F}_q \).

2.1. Rings and algebras with involution. Let \( R \) be an associative, unital, Artinian ring. The ring \( R^{op} \) is the additive group \( R \) equipped with the product \( x \cdot \text{op} y = yx \), for all \( x \) and all \( y \in R \). An involution on \( R \) is a ring automorphism \( * : R \to R^{op} \) of order at most 2. If \( R \) admits an involution \( * \) we say that the pair \((R, *)\) is a *-ring; we refer to \( R \) as a *-ring if the involution is unambiguous. If \( R \) admits a central action by \( \mathbb{F}_q \), then we call \( R \) an \( \mathbb{F}_q \)-algebra or simply an algebra. A *-algebra is an \( \mathbb{F}_q \)-algebra that admits an \( \mathbb{F}_q \)-linear involution. For the most part our *-rings are also *-algebras, but we continue to use the term *-ring, especially when considering extension fields over which the involution is not necessarily linear. Natural examples of *-algebras include full matrix algebras with the transpose involution, and group algebras with the involution determined by inversion of the group elements. General results for *-algebras appear in [Al, Chapter X], and a modern treatment may be found in [Le].

Associated to each *-ring \((R, *)\) are two natural subsets:

\[
R^+ := (R, *)^+ = \{ r \in R : r^* = r \} \quad \text{and} \quad R^- := (R, *)^- = \{ r \in R : r^* = -r \}. 
\]

The former is a natural Jordan algebra and the latter a natural Lie algebra. If \( 2R = R \) (for instance when \( R \) is an \( \mathbb{F}_q \)-algebra and \( q \) is odd) then, for each \( r \in R \), \( r = s + a \in R^+ \oplus R^- = R \), where \( s = \frac{1}{2}(r + r^*) \) and \( a = \frac{1}{2}(r - r^*) \), so that \( r^* = s - a \). The group of unitary elements of \((R, *)\) is

\[
R^\# := (R, *)^\# = \{ r \in R^\times : rr^* = 1 \} = \{ r \in R : rr^* = 1 = r^*r \}. 
\]

As will be made clear in Section 3, to each Hermitian map one may associate a ring with involution whose group of unitary elements is equal to the isometry group of the map. Thus \( R^\# \) is our main object of study.

The category of *-rings has all the usual structures. A *-homomorphism \((R, *) \to (S, \bullet)\) is a (unital) ring homomorphism \( \varphi : R \to S \) satisfying \( r^* \varphi = r \varphi^* \). A *-ideal of \((R, *)\) is an ideal \( I \) of \( R \) such that \( I^* = I \). If \( I \) is an ideal of \( R \) then \( I + I^* \) and \( I \cap I^* \) are *-ideals. We say that \( R \) is a simple *-ring if its only *-ideals are 0 and \( R \).

**Theorem 2.1** (Radical-semisimple structure of *-rings). The following hold for a *-ring \( R \), where \( R \) is an Artinian ring.

(i) The Jacobson radical \( J(R) \) is a *-ideal.

(ii) The quotient \( R/J(R) \) (with induced involution) is *-isomorphic to

\[
(S_1, *) \oplus \cdots \oplus (S_m, *),
\]
where, for \(1 \leq i \leq m\), \((S_i, \ast)\) is a simple \(*\)-ring and either \(S_i\) is simple as a ring (a classical type) or \(S_i\) is the direct sum of two isomorphic simple rings with the involution interchanging the two summands (an exchange type).

(iii) The group \(U = R^\# \cap (1 + J(R))\) is a unipotent normal subgroup of \(R^\#\) (i.e., for every \(u \in U\) there is an \(n \in \mathbb{N}\) such that \((u - 1)^n = 0\)) and

\[
R^\# / U \cong (R/J(R))^\# \cong S_{1}^\# \times \cdots \times S_{m}^\#.
\]

Proof. (Parts (i) and (ii) are evident in Albert [Al, Chapter X] but we include a short version as the details are relevant to Section 4.) For (i), \(J(R)\) is the intersection over the set of maximal left ideals of \(R\) as well as over the set of all maximal right ideals of \(R\), and \(\ast\) interchanges these two sets. For (ii), if \(I\) is a minimal ideal of \(R/J(R)\) then so is \(I^\ast\) and so \(I \cap I^\ast = 0\) or \(I\). If \(I = I^\ast\) then \((I, \ast)\) is a simple \(*\)-ring of classical type. If \(I \neq I^\ast\) then \(I + I^\ast = I \oplus I^\ast\) and so \((I \oplus I^\ast, \ast)\) is a simple \(*\)-ring where the involution interchanges the two simple ring factors \(I\) and \(I^\ast\). In any case, \(R/J(R)\) is a direct sum of its minimal ideals, and hence a direct sum of its minimal \(*\)-ideals. Finally, for (iii), observe that every element of \(J(R)\) is nilpotent since \(R\) is Artinian. Hence \(U\) is unipotent and the rest follows from (ii).

In the finite case there is an explicit description of the simple \(*\)-rings and their associated unitary elements.

**Theorem 2.2** (Classification of finite simple \(*\)-rings). A finite simple \(*\)-ring \((R, \ast)\) is \(*\)-isomorphic to one of the following types, for some \(n\) and \(q\).

(i) Orthogonal: \(O^\ast(n, F_q) = (M_n(F_q), X \mapsto DX^tD^{-1})\), where \(D \in \{I_n, I_{n-1} \oplus \omega\}\) \((\omega \in F_q\) a non-square) and \(\epsilon \in \{+, -, \circ\}\) according to whether \(d(u, v) = uDv^t\) induces an orthogonal geometry of type \(\epsilon\). The group of unitary elements of the \(*\)-ring \(O^\ast(n, F_q)\) is the general orthogonal group \(GO^\ast(n, F_q)\).

(ii) Unitary: \(U(n, F_{q^2}) = (M_n(F_{q^2}), X \mapsto \bar{X}^t)\) where \(\alpha \mapsto \bar{\alpha}\) is the field automorphism of \(F_{q^2}\) of order 2. The group of unitary elements of the \(*\)-ring \(U(n, F_{q^2})\) is the general unitary group \(GU(n, F_{q^2})\).

(iii) Exchange: \(X(n, F_q) = (M_n(F_q) \oplus M_n(F_q), (X, Y) \mapsto (Y^t, X^t))\). The group of unitary elements of the \(*\)-ring \(X(n, F_q)\) is the diagonally embedded general linear group \(\{g, g^{-1t}: g \in GL(n, F_q)\} \cong GL(n, F_q)\).

(iv) Symplectic: \(S(2n, F_q) = (M_{2n}(F_q), X \mapsto JX^tJ^{-1})\), where \(J = J_2 \oplus \cdots \oplus J_2\) and \(J_2 = \begin{bmatrix} 0 & I_n \n I_n & 0 \end{bmatrix}\). The group of unitary elements of the \(*\)-ring \(S(2n, F_q)\) is the symplectic group \(Sp(2n, F_q)\).

Proof. This follows from [Al, Theorem 11] and [Ja, Chapter IX.10-11] in the context of finite fields. A proof can also be extracted from Sections 4.2 and 4.3 below.

**Corollary 2.3.** If \((R, \ast)\) is a finite simple \(*\)-ring and \(\rho: R \to M_n(F_q)\) is an absolutely irreducible representation of \(R\) (as an ordinary ring), then the following hold:

(a) \(\rho\) is faithful if and only if \((R, \ast)\) is of type (i), (ii), or (iv).

(b) \(R^\#\rho\) is \(GL(n, F_q)\)-conjugate to the appropriate rank \(n\) classical group over \(F_q\).

Our final structure theorem is a special case of [Ta, Theorem 1].

**Theorem 2.4** (Taft). If \((R, \ast)\) is a finite-dimensional \(*\)-algebra over a finite field of odd characteristic, then there is a \(*\)-subalgebra \(S \subseteq R\) such that \(R = J(R) \oplus S\).
2.2. Fast algorithms for matrix algebras and effective homomorphisms.

We now summarize computational methods for rings of matrices, and for the modules upon which they act. In complexity statements we write \( g(n) = O(f(n)) \) if there are positive constants \( C \) and \( N \) such that \(|g(n)| \leq C|f(n)|\) for all \( n \geq N \). We write \( g(n) = O^*(f(n)) \) if there are positive constants \( C, c, \) and \( N \) such that \(|g(n)| \leq C|f(n)| \log^c n\) for all \( n > N \).

We assume that matrix rings are input by a set \( \mathcal{X} = \{x_1, \ldots, x_k\} \subseteq M_d(F_q) \) of generators; as our rings are unital, we shall assume that \( 1 \in \mathcal{X} \). Write \( R = \text{Env}(\mathcal{X}) \) for the enveloping algebra of \( \mathcal{X} \), namely the \( F_q \)-linear span of the monoid \( \langle \mathcal{X} \rangle \) generated by \( \mathcal{X} \). A (right) ideal \( I \) of \( R \) is specified by a set \( \mathcal{Y} \) such that \( I = \mathcal{Y}R \). An \( R \)-module \( U = F_q^n \) (possibly different from the natural \( F_q^d \)-module) is specified by a set \( \{a_1, \ldots, a_k\} \subseteq M_n(F_q) \), where, for \( 1 \leq i \leq k \), \( a_i \) is the matrix representing the transformation induced by \( x_i \) on \( U \) relative to a fixed basis of \( U \).

The time required for operations in \( R \) is \( O(d^\omega) \), where \( \omega \) is the exponent for the matrix multiplication in use by our algorithm. It is well-known that \( 2 \leq \omega \leq 3 \); for convenience we will use \( \omega = 3 \) in all of the estimates to follow.

Randomized algorithms for matrix algebras hypothesize the ability to select independent, uniformly distributed random elements from the algebra \( R \). We shall denote by \( \text{Rand}(R) \) an upper bound on the time required to construct such an element. With an \( F_q \)-basis for \( R \), uniformly random scalars produce uniformly random linear combinations in \( R \) and in that way \( \text{Rand}(R) = O(d^3 \dim R) \) [Iv, p. 177].

Ronyai [Ró] gave the first polynomial-time algorithms for \( F_q \)-algebras \( R \), which have complexity of \( O((\dim R)^3) \) field operations (which is \( O(d^3) \) for some rings \( R \subseteq M_d(F_q) \)). The work of Eberly and Giesbrecht [EG] and Ivanyos [Iv] has led to remarkable and practical improvements for rings of matrices. The following result, which can be deduced from [Iv, Corollary 1.5] and [EG, Theorem 3.6], provides the algorithmic platform that we need.

**Theorem 2.5.** There is a Las Vegas algorithm which, given \( R = \text{Env}(\mathcal{X}) \subseteq M_d(F_q) \), computes the following:

(i) The Jacobson radical, \( J(R) \), of \( R \) and a subring \( S \) of \( R \) (both specified by generating sets of size \( |\mathcal{X}| \) such that \( R = J(R) \oplus S \) and

(ii) An epimorphism \( \tau: R \to M_{n_1}(F_1) \oplus \cdots \oplus M_{n_\ell}(F_\ell) \) with kernel \( J(R) \), and, for each \( j \in \{1, \ldots, \ell\} \), elements \( \omega_j = \sum_{i=1}^k \lambda_i y_i \) \( \tau \), with \( \lambda_i \in F_q \) and \( y_i \in \langle \mathcal{X} \rangle \), such that \( F_j = \text{Env}(\{1, \omega_j\}) \) is a field extension of \( F_q \).

The algorithm uses \( O^*(|\mathcal{X}|(d^3 + d^2 \log q) + \text{Rand}(R)) \) operations in \( F_q \).

Furthermore, there are deterministic algorithms using \( O(d^2) \) field operations for each of the following:

(iia) Given \( r \in R \), compute \( r \tau \); and

(ii.b) Given \( t \in M_{n_1}(F_1) \oplus \cdots \oplus M_{n_\ell}(F_\ell) \), compute \( s \in S \) with \( s \tau = t \).

**Remark 2.1.** There are deterministic variants of the algorithms of Ronyai [Ró], having complexity polynomial in \( p + |\mathcal{X}|d^2 \log q \). Using those algorithms instead of Theorem 2.5 makes the algorithm of Theorem 1.2 deterministic, with complexity polynomial in \( p + |\mathcal{X}|d^2 \log q \). Observe, however, that the randomized version is more practical since its complexity does not depend on the size of characteristic \( p \).

**Remark 2.2.** In Section 5.2 we require the generators for \( J(R) \) to exhibit the terms of its nilpotent series. Specifically, if \( c \) is the nilpotence class of \( J(R) \), and \( J(R) \) is
generated as an ideal by \( U \subset J(R) \), then \( J(R)^i \) is generated as an ideal by \( U \cap J(R)^i \), for all \( 1 \leq i \leq c \). The algorithm for Theorem 2.5(i) is easily tailored to return such a set \( U \).

Throughout the paper we shall use the term effective homomorphism in the sense of (ii.a) and (ii.b) to mean any homomorphism of algebraic structures \( A \to B \) with polynomial-time algorithms to compute images and preimages. We refer to a decomposition of a ring \( R \) such as that occurring in Theorem 2.5(i) as a Wedderburn decomposition.

The following result is well-known, but we have not found a reference in the form we require.

**Lemma 2.6 (Spinning Algorithm).** There is a deterministic algorithm which, given isomorphic, absolutely irreducible representations \( U \) and \( U' \) of \( \text{Env}(X) \), computes an isomorphism \( U \to U' \). The algorithm uses \( O(|X|^2 \dim_{F_q} U) \) field operations.

**Proof.** Suppose that \( U \) and \( U' \) have fixed bases \( u_1, \ldots, u_n \) and \( u_1', \ldots, u_n' \), and the action of \( \text{Env}(X) = \{ x_1, \ldots, x_k \} \) is specified by sets \( \{ a_1, \ldots, a_k \} \subseteq M_n(F_q) \) and \( \{ a_1', \ldots, a_k' \} \subseteq M_n(F_q) \), respectively. Since \( U \) and \( U' \) are isomorphic, absolutely irreducible \( \text{Env}(X) \)-modules, it follows that \( \text{Hom}_{\text{Env}(X)}(U, U') \) is 1-dimensional. It suffices, therefore, to establish a suitable image for \( u_1 \); images of the remaining \( u_i \) are then computed via the action of \( \text{Env}(X) \). Thus we require \( u' = \sum_{i=1}^n \lambda_i u'_i \in U' \) such that \( u_{1,i} a_i = a'_{i,i} u' \) for all \( 1 \leq i \leq k \). This amounts to solving a system of \( k \) equations in the \( n \) unknowns \( \lambda_1, \ldots, \lambda_n \). The result now follows. \( \square \)

3. Hermitian maps, adjoints, and isometries

In this section we introduce the \( * \)-algebra of adjoints as a method to construct isometries of an Hermitian map. In particular, we prove Theorem 1.1 parts (i) and (ii) and lay the groundwork for Theorem 1.2. We also recast the classification of simple \( * \)-rings given in Theorem 2.2 as the classification of nondegenerate finite-dimensional Hermitian forms over finite fields; this viewpoint will be useful in Sections 4.2 and 4.3.

3.1. Hermitian and bilinear maps. Let \( V \) and \( W \) be finite-dimensional vector spaces over \( F_q \). A function \( b: V \times V \to W \) is \( F_q \)-bilinear if

\[
(3.1) \quad b(\lambda u + v, \tau u' + v') = \lambda \sigma b(u, v) + \lambda b(u', v) + \tau b(u', v) + b(u, v')
\]

for all \( u, v \in V \) and all \( \lambda, \tau \in F_q \). We say that \( b \) is Hermitian if there exists \( \theta \in \text{GL}(W) \) such that, for all \( u, v \in V \), \( b(u, v) = b(v, u)\theta \). For convenience we insist that \( W = \langle b(u, v) : u, v \in V \rangle \), which requires that \( \theta^2 = 1 \). Hermitian maps include the usual symmetric, alternating, and Hermitian forms. (In the Hermitian form case, \( W = F_q^2 \) is regarded as an \( F_q \)-space. Hence the automorphism \( \alpha \to \alpha^q \) of \( F_q^2 \) lies in \( \text{GL}(W) \), and \( b \) is \( F_q \)-bilinear, so we do not need sesquilinear terminology.)

In general we allow our bilinear maps \( b \) to be degenerate in the sense that \( \text{rad} b = \{ v \in V : b(v, V) = 0 \} \) may be nontrivial. Given a degenerate bilinear map \( b \) we may always induce a nondegenerate bilinear map \( c: V/\text{rad} b \times V/\text{rad} b \to W \) with \( c(u + \text{rad} b, v + \text{rad} b) = b(u, v) \) for all \( u, v \in V \).
3.2. **Rings of adjoints and isometry groups.** To each Hermitian $F_q$-bilinear map $b : V \times V \to W$ one may associate the ring
\begin{equation}
\text{Adj}(b) := \{ (f, g) \in \text{End} V \oplus (\text{End} V)^{\text{op}} : b(uf, v) = b(u, vg), \forall u, v \in V \},
\end{equation}
called the ring of adjoints of $b$. If $(f, g) \in \text{Adj}(b)$ then for all $u, v \in V$,
\begin{equation}
b(u, vg) = b(v, ug) = b(vf, u) = b(u, vf).
\end{equation}
Thus, $(f, g) \mapsto (g, f)$ induces an involution on $\text{Adj}(b)$ which we denote by $\ast$.

If $b$ is nondegenerate then we adopt more convenient notation. Specifically, if $(f, g) \in \text{Adj}(b)$ then $(f, g') \in \text{Adj}(b)$ if and only if $g = g'$. We therefore denote $g$ by $f^\ast$, and identify $\text{Adj}(b)$ with its isomorphic image in $\text{End} V$.

If $b : V \times V \to W$ is degenerate and $c : V/\text{rad} b \times V/\text{rad} b \to W$ is the nondegenerate map induced by $b$, then $\text{Adj}(c)$ is naturally isomorphic to $\text{Adj}(b)/I$ where
\begin{equation}
I := \{ (f, 0), (0, f) \in \text{End} V \oplus (\text{End} V)^{\text{op}} : Vf \subseteq \text{rad} b \}.
\end{equation}

Considering Equation (1.1), we can now translate our main object of study into the language of adjoints:
\begin{equation}
\text{Isom}(b) = \{ f \in \text{GL}(V) : (f, f^{-1}) \in \text{Adj}(b) \}.
\end{equation}

If $b$ is degenerate, and $c : V/\text{rad} b \times V/\text{rad} b \to W$ is the nondegenerate map induced by $b$, then
\begin{equation}
\text{Isom}(b) = U \times (\text{GL}(\text{rad} b) \times \text{Isom}(c)),
\end{equation}
where $U = \{ 1 + h : h \in \text{Hom}(V, \text{rad} b) \}$. Hence, to construct generators for $\text{Isom}(b)$, it suffices to construct generators for $\text{Isom}(c)$.

If $b$ is nondegenerate, then it follows from Equation (3.5) that $(f, g) \mapsto f$ restricts to the isomorphism
\begin{equation}
\text{Adj}(b)^\# \overset{\cong}{\longrightarrow} \text{Isom}(b),
\end{equation}
which allows us to study $\text{Isom}(b)$ as $\text{Adj}(b)^\#$ within $\text{Adj}(b)$.

3.3. **Hermitian forms and simple $\ast$-rings.** To clarify our correctness proofs in Sections 4.2 and 4.3, we now recast the classification of Theorem 2.2 in the language of adjoints (cf. [Wi1, Corollary 4.30(i)]).

(i) If $\varphi : V \times V \to F_q$ is a nondegenerate symmetric bilinear form, then $\text{Adj}(\varphi)$ is an orthogonal type simple $\ast$-ring.

(ii) If $\varphi : V \times V \to F_{q^2}$ is a nondegenerate Hermitian form with respect to the quadratic field involution of $F_{q^2}$, then $\text{Adj}(\varphi)$ is a unitary type simple $\ast$-ring.

(iii) If $V = U \oplus U, \psi : U \times U \to F_q$ is a nondegenerate bilinear form, and we define $\varphi : V \times V \to F_q \oplus F_q$ by $\varphi(u \oplus w, u' \oplus w') = \psi(u, w') \oplus \psi(w, u')$, then $\varphi$ is Hermitian and $\text{Adj}(\varphi)$ is a simple $\ast$-ring of exchange type.

(iv) If $\varphi : V \times V \to F_q$ is a nondegenerate alternating bilinear form, then $\text{Adj}(\varphi)$ is a symplectic type simple $\ast$-ring.
3.4. Proof of Theorem 1.1 parts (i) and (ii). Theorem 1.1(ii) is already proved in [Wi1, Theorem 4.39], but the following detailed study of that proof also establishes Theorem 1.1(i).

Let $b: V \times V \to W$ be a nondegenerate Hermitian $F_q$-bilinear map with $q$ odd. Let $R$ denote the $*$-algebra $\text{Adj}(b)$, and let $J = J(R)$. By Theorem 2.1(ii) there are simple $*$-rings $S_1, \ldots, S_m$ such that $R/J \cong S_1 \oplus \ldots \oplus S_m$.

Next, let $0 = U_0 < U_1 < U_2 < \ldots < U_s = V$ be a composition series for the $R$-module $V$ and, for $1 \leq j \leq s$, let $U_j = U_j/U_{j-1}$. Evidently $J$ is the kernel of the induced action of $R$ on $\bigoplus U_i$. Hence, $U_j$ decomposes into a sum of isomorphic irreducible $S_i$-$\#$-modules $X_j$ such that $X_j \oplus U_i \cong U_j \oplus S_i F_i$ (see Remark 3.1 below).

Finally, as the $F_q$-enveloping algebra of $R^\#$ is a subset of $R$, it follows that any composition series $0 = V_0 < V_1 < \ldots < V_t = V$ of $R^\#$ is a refinement of a composition series for $V$ as an $R$-module where each factor is an irreducible $S_i$-$\#$-module for some $1 \leq i \leq m$. This proves Theorem 1.1(i).

For each $1 \leq i \leq t$, set $V_i = V_i/V_{i-1}$. Note that the kernel $U$ of the action of $R^\#$ on $V_1 \oplus \ldots \oplus V_t$, is unipotent, as $\{V_1, \ldots, V_t\}$ is a set of composition factors of $V$ as an $R^\#$-module. Hence, $U \leq O_p(R^\#)$. Furthermore,

$$(3.8) \quad R^\#/\{1 + u: u \in J\} \cong S_1^\# \times \cdots \times S_m^\#.$$ 

For each $1 \leq i \leq m$, $S_i$ has a faithful irreducible representation in characteristic $p$ and so $O_p(S_i^\#) = 1$. Thus, $O_p(R^\#) \leq R^\# \cap (1 + J) \leq U$. Hence $U = O_p(R^\#)$, as required to prove Theorem 1.1(ii).

Remark 3.1. The $S_i$-$\#$-module $U_j \oplus S_i F_i$ is often irreducible, but not always. For instance, $O^\#(1, q^\#)$ acts absolutely irreducibly on $F_q$, but $O^\#(1, q^\#)^\# = \text{GO}^\#(1, q^\#) = \{\pm 1\}$ acts completely reducibly on $F_q$. Nevertheless, the irreducible factors of the $O^\#(1, q^\#)^\#$-module are isomorphic and, when tensored with $F_q$, are isomorphic to the original representation of $O^\#(1, q^\#)$. This is one reason that we chose not to describe the relationship of $t$ and $m$ in Theorem 1.1.(i) and (ii).

4. Algorithms for $*$-algebras of matrices

In this section we present algorithms to compute effectively with finite $*$-algebras of matrices, leading to algorithmic versions of Theorems 2.1, 2.2, and 2.4. These results serve as the platform for the isometry group algorithm in Section 5.

In Section 4.1 we apply the results of Section 2.2 to obtain the radical-semisimple structure of a $*$-algebra. In Sections 4.2 and 4.3 we show how to construct an explicit isomorphism from a given simple $*$-algebra to one of the $*$-algebras defined in Theorem 2.2, a process known as constructive recognition. Section 4.4 analyzes the complexity of the algorithms in Sections 4.1 through 4.3 and establishes their polynomial timing (Theorem 4.1). Finally, in Section 4.5, we specialize to $*$-algebras of odd characteristic and prove an algorithmic version of Theorem 2.4.
We assume that a \(*\)-algebra is input as \(R = \text{Env}(\mathcal{X}) \subseteq M_d(F_q)\) together with a function that computes \(r^*\) for each \(r \in R\). We let \(\text{Star}(R, \ast)\) denote an upper bound on the number of field operations needed to apply \(*\) to a single \(r \in R\). While \(\text{Star}(R, \ast)\) depends on the method the user provides, its complexity need not exceed \(O(d^2 \dim R)\). For, if \(B\) is an \(F_q\)-basis for \(R\), then we may store \(\{b^* : b \in B\}\), and evaluate \(*\) on \(R\) as follows:

\[
\left( \sum_{b \in B} \lambda_b b \right)^* = \sum_{b \in B} \lambda_b b^*, \quad \text{where, for all } b \in B, \lambda_b \in F_q.
\]

4.1. Computing the radical-semisimple structure of a \(*\)-ring. In this section we apply Theorem 2.5 to produce an algorithm which constructs the radical, semisimple quotient, and simple \(*\)-factors of a \(*\)-ring, as described by Theorem 2.1 parts (i) and (ii). Recall from Section 2.2 that a homomorphism is effective if there are polynomial-time algorithms to compute images and preimages.

Let \((R, \ast)\) be a \(*\)-ring, where \(R = \text{Env}(\mathcal{X}) \subseteq M_d(F_q)\). Temporarily ignoring the \(*\)-structure, we use the algorithm for Theorem 2.5 to construct a Wedderburn decomposition \(R = J(R) \oplus S\) along with an effective epimorphism

\[
\tau : R \to M_{n_1}(F_{l_1}) \oplus \ldots \oplus M_{n_{\ell}}(F_{l_{\ell}})
\]

where \(J(R)\) is a \(R\)-linear involution defined so that for \(t \in R\), \(t^* := r^*\tau\), where \(r \in R\) and \(r\tau = t\). In this way \(\tau\) induces an effective \(*\)-isomorphism \((R/J(R), \ast) \to (T, \ast)\). By Theorem 2.5(ii.b), \(\text{Star}(T, \ast) = O(d^2 + \text{Star}(R, \ast))\).

Next we identify the simple \(*\)-ring factors of the semisimple \(*\)-ring \((T, \ast)\). For that we construct the permutation \(\gamma\) on \(\{1, \ldots, \ell\}\) such that \(M_{n_j}(F_j)^{\ast} = M_{n_j}(F_j^{\gamma})\). This is done using primitive central idempotents in \(T\). Specifically, if

\[
E_j := (0_{n_1}, \ldots, 0_{n_{j-1}}, \lambda_{n_j}, 0_{n_{j+1}}, \ldots, 0_{n_{\ell}}) \in T,
\]

then \(j\gamma\) is the unique component in which \(E_j^*\) is nonzero. As \((E_j^*)^* = E_j, \gamma^2 = 1\).

Take \(\Delta \subset \{1, \ldots, \ell\}\) to be a set of representatives of the cycles in \(\gamma\). For each \(j \in \Delta\) set \((T_j, \ast) = (M_{n_j}(F_j) + M_{n_{j\gamma}}(F_j^{\gamma}), \ast)\). According to Theorem 2.1(ii), \(T_j = M_{n_j}(F_j)\) if \(j = j\gamma\); else, \(T_j = M_{n_j}(F_j) \oplus M_{n_{j\gamma}}(F_j^{\gamma})\). It follows that \(T = \bigoplus_{j \in \Delta} T_j\) is a decomposition of \(T\) into simple \(*\)-algebras. Let \(Y_j\) be the image of \(Y\) under projection onto \(T_j\); then \(T_j = \text{Env}(Y_j)\).

Complexity. The Wedderburn decomposition of \(R\) uses \(O^*(\mathcal{X}|\{d^3 + d^2 \log q\}) + \text{Rand}(R)\) field operations (Theorem 2.5). The construction of the permutation \(\gamma\) involves \(O(\ell \cdot \text{Star}(T, \ast)) = O(d^3 + d \cdot \text{Star}(R, \ast))\) field operations.

Remark 4.1. If \(S\) is \(*\)-invariant, then the restriction of \(\tau\) to \(S\) is a \(*\)-isomorphism \(S \to T\) (cf. Theorem 4.4). This will be important in Section 5.4 because it enables one to lift certain elements of \(T\) to \(R\).

4.2. Constructive recognition of classical simple \(*\)-rings. Suppose that we are given \(T = \text{Env}(S) = M_n(F_q[\omega])\) with an \(F_q\)-linear involution \(\ast\), where \(F = F_q[\omega]\) is a field extension of degree \(e\) over \(F_q\). We describe an algorithm to determine a \(*\)-isomorphism from \((T, \ast)\) to one of the simple \(*\)-algebras listed in Theorem 2.2 parts (i), (ii), or (iv).

First we determine a field automorphism on \(F\) and use it to replace \(\ast\) with an \(F\)-linear involution on \(T\). Since \(\ast\) is an \(F_q\)-linear ring anti-isomorphism it preserves...
the center \( \{ \lambda I_n : \lambda \in F \} \) of \( T = M_n(F) \). Thus \( \bullet \) determines an \( F_q \)-linear field automorphism \( \alpha \mapsto \overline{\alpha} \) on \( F \) such that \( (\alpha I_n) = \overline{\alpha} I_n \). This automorphism is computed on \( \omega \), determining its effect on the \( F_q \)-basis \( 1, \omega, \ldots, \omega^{q-1} \) for \( F \) over \( F_q \), and hence, by linearity, on \( F \). The automorphism extends to \( M_n(F) \), sending \( X \mapsto \overline{X} \), where \( \overline{X}_{ij} = \overline{X}_{ij} \), for all \( X \in M_n(F) \) and all \( i, j \in \{1, \ldots, n\} \). Hence, \( X \mapsto \overline{X} \) is an \( F \)-linear automorphism on \( T \).

Next we find \( \Phi \in \text{GL}(n,F) \) such that \( \overline{X} = \Phi^{-1}X\Phi \). The existence of such a \( \Phi \) follows from the Skolem-Noether theorem [CR, (3.62)], whose proof motivates the following algorithm. Let \( U = F^n \) be the natural (right) \( T \)-module. Define the (left) \( T \)-module \( U^* \) by \( Xu = u\overline{X} \) for all \( u \in U \) and all \( X \in T \). Also define \( \overline{U}^{\star} = \text{Hom}_F(U^*,F) \), a natural (right) \( T \)-module. As \( T \) is simple and represented absolutely irreducibly on \( U \) and on \( \overline{U}^{\star} \), these two \( T \)-modules are isomorphic. Use Lemma 2.6 to find a matrix \( \Phi \) representing an \( F \)-linear isomorphism \( U \mapsto \overline{U}^{\star} \) as \( T \)-modules; then \( uX\Phi = u\Phi\overline{X} \) for all \( X \in T \) and all \( u \in U \). It follows that

\[
(4.4) \quad X\Phi = \Phi\overline{X} \quad \text{for all } X \in M_n(F).
\]

Finally, define a nondegenerate reflexive bilinear form \( \varphi : F^n \times F^n \to F \) by

\[
(4.5) \quad \varphi(u,v) := u\Phi \overline{v} \quad \text{for all } u,v \in F^n.
\]

It follows from Equation (4.4) that

\[
(4.6) \quad \text{Adj}(\varphi) = \{X \in M_n(F) : \varphi(uX,v) = \varphi(u,vX) \quad \text{for all } u,v \in V\}
\]

as in Section 3.3. Find a change-of-basis matrix \( c \in \text{GL}(n,F) \) that transforms the coordinate basis of \( F^n \) to a standard basis for the form \( \varphi \) (algorithms for that task are standard; see, for example, [Wi3]). As in Section 3.3, \( \text{Adj}(\varphi)^c \) is one of the algebras listed in Theorem 2.2 (i), (ii), or (iv).

**Complexity.** We have \( T = \text{Env}(S) \), so \( O(|S| \cdot \text{Star}(T,\bullet)) \) field operations in \( F_q \) are required to define the inner automorphism of \( T \) on generators. The construction of \( \Phi \) and the change-of-basis matrix both use \( O(n^3) \) operations in \( F \), which translates to \( O(n^3e^3) \) operations in \( F_q \). Thus, the total complexity is \( O(|S|\text{Star}(T,\bullet) + n^3e^3) \).

### 4.3. Constructive recognition of exchange simple \( \ast \)-rings.

Suppose that we are given \( T = \text{Env}(S) = M_n(F) \oplus M_n(F) \) with an involution \( \bullet \) that interchanges the two minimal ideals of \( T \). We describe an algorithm to compute a \( \ast \)-isomorphism from \( (T,\bullet) \) to the simple \( \ast \)-ring given in Theorem 2.2(iii).

First we define a field involution \( \alpha \mapsto \overline{\alpha} \) on \( F \) similar to Section 4.2. Indeed,

\[
(4.7) \quad (\omega I_n, 0_n)^{\ast} = (0_n, \overline{\omega} I_n)
\]

defines \( \omega \mapsto \overline{\omega} \), which then uniquely determines \( \alpha \mapsto \overline{\alpha} \) on \( F = F_q[\omega] \).

In this setting \( T \) acts on \( F^n \) in four relevant ways. For each \( X = (X_1, X_2) \in T \), define the \( T \)-module \( U = F^n \) by \( uX := uX_1 \) for all \( u \in U \), and \( W = F^n \) by \( wX := wX_2 \) for all \( w \in W \). Also define \( \overline{U}^{\star} = \text{Hom}_F(U^*,F) \) and \( \overline{W}^{\star} = \text{Hom}_F(W^*,F) \), as in the classical case above.

For all \( (X_1, X_2) \in T \), we know that \( (X_1, X_2)^{\ast} = (X_2, X_1)^{\ast} \) for some \( X_1, X_2 \in M_n(F) \). Thus, the absolutely irreducible representations of \( T \) on \( U \) and \( \overline{W}^{\star} \) have the common annihilator \( \{0, X_2 : X_2 \in M_n(F)\} \), and hence are isomorphic. Use Lemma 2.6 to construct a matrix \( \Phi \) representing an \( F \)-linear isomorphism from \( U \)
to \(W^{\text{str}}\) as \(T\)-modules. (Note that if \(\Psi\) is any isomorphism from \(W\) to \(U^{\text{str}}\) then \(\Phi = \lambda \Psi^{-1}\) for some \(\lambda \in F\).) Define \(\varphi\) \(:(F^n \oplus F^n) \times (F^n \oplus F^n) \rightarrow F \oplus F\) by
\[
\varphi(u_1 \oplus w_1, u_2 \oplus w_2) := (u_1 \Phi w_2^{\text{str}}) \oplus (u_2 \Phi w_1^{\text{str}})
\]
for all \(u_1 \oplus w_1, u_2 \oplus w_2 \in F^n \oplus F^n\). As in Equation (4.6), \((T, \bullet) = \text{Adj}(\varphi)\). Using row-reduction, compute matrices \(A, B \in \text{GL}(n, F)\) such that \(A\Phi B^{\text{str}} = I_n\). Define \(c \in \Gamma \text{L}(n, F) \times \Gamma \text{L}(n, F)\), sending \(u \oplus w \mapsto uA \oplus wB\). Then, for \(u_1 \oplus w_1, u_2 \oplus w_2 \in U \oplus V\),
\[
\varphi((u_1 \oplus w_1)c, (u_2 \oplus w_2)c) = (u_1 A \Phi (w_2B)^{\text{str}}) + (u_2 A \Phi (w_1B)^{\text{str}}) = (u_1 w_2^{\text{str}}) \oplus (u_2 w_1^{\text{str}}).
\]

As in Section 3.3, \(\text{Adj}(\varphi)^c\) is the exchange type simple \(*\)-algebra in Theorem 2.2(iii).

**Complexity.** The complexity analysis is the same as for Section 4.2.

4.4. **Total complexity.** The algorithms presented so far construct the radical, the semisimple quotient, and the simple \(*\)-ring factors of finite \(*\)-algebras of matrices. Combining the complexity estimates for these sections we obtain the following analogue of Theorem 2.5 for \(*\)-algebras.

**Theorem 4.1.** There is a Las Vegas algorithm which, given a \(*\)-algebra \((R, *)\) with \(R = \text{Env}(\mathcal{A}) \subseteq M_d(F_q)\), finds each of the following:

(i) The Jacobson radical, \(J(R)\), of \(R\);

(ii) An effective \(*\)-isomorphism \(R/J(R) \rightarrow T_1 \oplus \ldots \oplus T_m\), where \(T_j\) \((1 \leq j \leq m)\) is a simple \(*\)-algebra represented over its natural field \(F_j\); and

(iii) For \(1 \leq j \leq m\), an effective \(*\)-isomorphism from \(T_j\) to one of the simple \(*\)-algebras described in Theorem 2.2.

The complexity of the algorithm is \(O^\sim(|\mathcal{A}|[d^3 + d^2 \log q + d \cdot \text{Star}(R, *)] + \text{Rand}(R))\).

4.5. **The Taft decomposition algorithm.** Theorem 4.1 reveals, algorithmically, the radical-semisimple structure of a matrix \(*\)-ring \(R\). When \(R\) has odd characteristic we can do more, and this will be important in our application to isometry groups.

If \(R\) is a matrix \(*\)-ring of odd characteristic, then Theorem 2.4 establishes the existence of a subring \(S\) such that \(R = J(R) \oplus S\) and \(S^* = S\); we call such a decomposition a **Taft decomposition** of \(R\).

We now present an algorithmic version of Taft’s theorem based on his original proof. If \(R = J(R) \oplus S\) is a Wedderburn decomposition of \(R\), then we have a projection homomorphism \(\pi: R \rightarrow S\) afforded by the decomposition. As \(J(R)\) is a \(*\)-ideal, we define an involution on \(S\) by \(s^\bullet := s^\pi \pi\), for each \(s \in S\). In an algorithmic context, this induced \(*\)-algebra has \(\text{Star}(S, \bullet) = O(d^2 + \text{Star}(R, *))\).

**Lemma 4.2 (Taft).** Let \((R, \ast)\) be a \(*\)-ring, with \(2R = R\) and \(J(R)^2 = 0\). Suppose that \(R = J(R) \oplus S\) for some subring \(S\) of \(R\). Then \(s \mapsto \frac{1}{2}(s + s^\ast\ast)\) is a \(*\)-ring monomorphism \(\varphi: (S, \bullet) \rightarrow (R, \ast)\). In particular, \(R = J(R) \oplus S\varphi\) is a **Taft decomposition**.

**Proof.** The proof follows from [Ta, Proposition 1], but can also be seen as an application of Hochschild cohomology. Specifically, for an additive function \(\delta: S \rightarrow J(R)\), the map \(S \rightarrow R\) sending \(s \mapsto s - s\delta\) is an embedding of rings if and
only if $\delta$ is a derivation. Now, since $s \mapsto s^{**}$ is an embedding, it follows that $s \mapsto s - s^{**}$ is a derivation. Thus $s \mapsto \frac{1}{2}(s - s^{**})$ is a derivation, so that $s \mapsto s - \frac{1}{2}(s - s^{**}) = \frac{1}{2}(s + s^{**}) = s\varphi$ is also an embedding of rings. Furthermore, $s^{*}\varphi = \frac{1}{2}(s^{*} + s^{*}) = \frac{1}{2}(s^{**} + s) = s\varphi^{*}$, so $\varphi$ is a $*$-monomorphism.  

This observation leads to the following.

**Proposition 4.3.** There is a Las Vegas algorithm which, given a $*$-ring $R = \text{Env}(\langle X \rangle) \subseteq M_d(F_q)$ with $F_q$ of odd characteristic, returns a Taft decomposition of $R$. The complexity of the algorithm is $O^*(|\langle X \rangle| \{d^3 + d^2 \log q + \text{Star}(R,*)\} + \text{Rand}(R))$.

**Proof.** We use the algorithm $\text{TaftDecomposition}$.

```plaintext
TaftDecomposition ( R , * )
1   J(R) ⊕ S := WedderburnDecomposition ( R )
2   if J(R) = 0 then
3      return ( R , * )
4   else
5      /* Let $S = \text{Env}(\langle Y \rangle)$ with $|\langle Y \rangle| \leq |\langle X \rangle|$ */
6      $\mathcal{Y}' := \{ \frac{1}{2} (y + y^{**}) : y \in \langle Y \rangle \}$
7      $D := J(R)^2 + \text{Env}(\langle Y' \rangle)$
8      return TaftDecomposition ( D , * )
```

We establish correctness by induction on the solvable length of $J(R)$ (the smallest $n \in \mathbb{N}$ satisfying $J(R)^{2^n} = 0$). If $n = 0$ then $J(R) = 0$ and the output on line 3 is correct. Otherwise, the algorithm constructs the subring $D$ of $R$ in line 6. It suffices to show that $D^{*} = D$, $J(D) = J(R)^2$, and $D/J(D) \cong R/J(R) \cong S$. (For then we may recurse with $(D,*$) in the role of $(R,*)$ and the algorithm halts after $n$ recursive calls.)

As $J(R)^2$ is a $*$-ideal, $R/J(R)^2$ has a naturally induced involution $\circ$. Furthermore, $R/J(R)^2 = J(R)/J(R)^2 \oplus (S + J(R)^2)/J(R)^2$ is a Wedderburn decomposition. Thus, by Lemma 4.2, $R/J(R)^2 = J(R)/J(R)^2 \oplus D/J(R)^2$ is a Taft decomposition. Hence $D/J(R)^2$ is semisimple so that $J(R)^2 \leq J(D) \leq J(R)^2$. Moreover, $(D/J(R)^2)^{\circ} = D/J(R)^2$, which is to say that $D^{*} = D$. This completes the proof of correctness.

For the timing, since $J(R) \subseteq M_d(F_q)$, it follows that $J(R)^d = 0$. Hence $n \leq \log_2 d$ and the stated complexity estimate follows from Theorem 2.5(i).

**Remark 4.2.** $\text{TaftDecomposition}$ works over any field of characteristic not 2 for which one can construct a Wedderburn decomposition. In particular it applies to the field of rational numbers.

Combining this result with Remark 4.1 and Theorem 2.5 we obtain the following refinement of Theorem 4.1.

**Theorem 4.4.** There is a Las Vegas algorithm which, given a $*$-ring $(R,*)$ with $R = \text{Env}(\langle X \rangle) \subseteq M_d(F_q)$ of odd characteristic, finds each of the following:

(i) A Taft decomposition $R = J(R) \oplus S$; and
(ii) An effective ∗-isomorphism τ: S → T_1 ⊕ ... ⊕ T_m, where T_j (1 ≤ j ≤ m) is one of the simple ∗-algebras described in Theorem 2.2, defined naturally over a field extension F_j of F_q.

The complexity of the algorithm is O~(|X|)[d^3 + d^2 \log q + d \cdot \text{Star}(R, ∗)] + \text{Rand}(R).

5. Constructing the Isometry Group of an Hermitian Map

In this section we present an algorithm to construct the isometry group of an Hermitian map, resulting in the proof of Theorem 1.2. Along the way we establish Theorem 1.1(iii), thus completing the proofs of our main theorems. In Section 5.6, we discuss an application of Theorem 1.2 to computing intersections of classical groups.

We begin by giving an overview of the algorithm. The input is an Hermitian map b: V × V → W, where V and W are finite-dimensional vector spaces over a finite field F_q of odd characteristic p.

**IsometryGroup (b: V × V → W)**
1. c := b|_{V/\text{rad} b} : (V/\text{rad} b) × (V/\text{rad} b) → W
2. (R, ∗) := \text{Adj}(c) / R = R^+ ⊕ R^- ∗ /
3. J(R) ⊕ S := \text{TaftDecomposition} (R, ∗)
4. U := \text{UnipotentRadical} (J(R), R^-)
5. H_1 × ... × H_m := \text{SemisimpleFactors} (S)
6. return Isom(b) := (1 + \text{Hom}(V, \text{rad} b), U) × (H_1 × ... × H_m × \text{GL}(\text{rad} b))

Line 2 computes a basis for (R, ∗) = \text{Adj}(c) that exhibits the subspaces R^+ and R^-; this elementary task is discussed in Section 5.1. Line 3 uses the algorithm for Theorem 4.4 to obtain a decomposition R = J(R) ⊕ S, where J(R) is the Jacobson radical of R, and S is a ∗-invariant semisimple complement. This step also constructs a ∗-isomorphism τ: S → T_1 ⊕ ... ⊕ T_m, where T_i is a simple ∗-algebra of known type (as described in Theorem 2.2).

The remainder of this section mostly concerns lines 4 and 5. By Theorem 2.1 and Equation (3.7) we know that Isom(c)/U ≅ T_1# × ... × T_m#, where U = O_p(Isom(c)) is the unipotent radical of Isom(c). The splitting \text{Adj}(c) = J(R) ⊕ S leads to a corresponding splitting of Isom(c) as O_p(R#) × S#, so it suffices to construct generators for these two factors independently. In Section 5.2, a useful characterization of O_p(R#) is derived, which uses the power series for the function z + \sqrt{1 + z^2}.

That characterization provides the basis for an algorithm to construct generators for O_p(R#), which we present in Section 5.3. The construction of S# is described in Section 5.4. Following those steps, (3.6) explains why the isometry group of b is returned in line 6.

Note that both \text{TaftDecomposition} and \text{UnipotentRadical} make critical use of division by 2 and only apply to fields of odd characteristic.

5.1. Computing \text{Adj}(b).

The following result states that the algebra of adjoints associated with an Hermitian map can be constructed efficiently.

**Proposition 5.1.** There is a deterministic algorithm which, given a nondegenerate Hermitian map b: V × V → W, constructs the following:

(i) A basis, \mathcal{X}, for \text{Adj}(b) in \text{End} V (if |F_q| is odd, then \mathcal{X} is the disjoint union of bases for \text{Adj}(b)^+ and \text{Adj}(b)^-); and
Theorem 5.2. Let $z$ some $m$.

Similarly, $x$ $x$ $x$

Furthermore, if $z$ as a power series with coefficients in $\mathbb{R}$. Proof. The space $\text{Adj}(b)$ is defined as the solution to a system $\dim^2 V \cdot \dim W$ linear equations over $\mathbb{F}_q$ with $\dim^2 V$ unknowns. Thus it is possible to compute a basis $X$ for the image $\text{Adj}(b)|_V$ of the projection $(f, f^*) \to f$ of $\text{Adj}(b) \to \text{End} V$, along with its image, $X^*$. Then $*$ is defined on $\text{Adj}(b)$ as in Equation (4.1), and the stated complexity for $\text{Star}(\text{Adj}(b))$ follows. □

5.2. Constructing the unipotent radical. In this section we introduce a method to convert nilpotent elements of $R^-$ into unipotent elements of $R^\#$. This allows us to construct generators for the unipotent radical of $R^\#$. Since our approach is new for $*$-rings, we prove it in the generality of Artinian rings $R$ with $2R = R$ though no harm will come from considering only finite rings of prime characteristic other than 2. Our method replaces the well-known ‘exponential’ method (cf. [Ta, Section 4]) which has limited use for finite rings.

Using the usual calculus and manipulation of coefficients it follows that

$$\sqrt{1 + x} = 1 - 2\sum_{n=1}^{\infty} C(n - 1) \left(-\frac{1}{4}\right)^n x^n$$

where $C(n) = \frac{(2n)!}{n!n!}$ is the $n$-th Catalan number, so that $\sqrt{1 + x}$ can be viewed as a power series with coefficients in $\mathbb{Z}[1/2]$. From the Catalan recurrence relation $C(n + 1) = \sum_{m=0}^{n} C(m)C(n - m)$, the relation $(\sqrt{1 + x})^2 = 1 + x$ holds within $(\mathbb{Z}[1/2])[x]$.

**Theorem 5.2.** Let $(R, *)$ be a $*$-ring with $2R = R$. If $z \in R^-$ with $z^m = 0$ for some $m \in \mathbb{N}$, then

$$z + \sqrt{1 + z^2} = 1 + z - 2\sum_{n=1}^{m/2} C(n - 1) \left(-\frac{1}{4}\right)^n z^{2n} \in R^\#.$$  

Furthermore, if $x = z + \sqrt{1 + z^2}$ then $z = \frac{1}{2}(x - x^*)$.

Proof. As $z$ is nilpotent and $2R = R$, it follows that $x = z + \sqrt{1 + z^2}$ is the evaluation at $z$ of a polynomial, so that $x \in R$. Since $z \in R^-$, it follows that $z^2 \in R^+$ and so $\sqrt{1 + z^2} \in R^+$. It follows that

$$xx^* = \left(z + \sqrt{1 + z^2}\right) \left(-z + \sqrt{1 + z^2}\right) = -z^2 + \left(\sqrt{1 + z^2}\right)^2 = 1.$$  

Similarly, $x^*x = 1$ so that $x \in R^\#$ and $x^* = x^{-1}$. Finally,

$$\frac{1}{2}(x - x^*) = \frac{1}{2} \left(z + \sqrt{1 + z^2} - \left(-z + \sqrt{1 + z^2}\right)\right) = z.$$  

□

**Theorem 5.3.** If $(R, *)$ is an Artinian $*$-ring with $2R = R$, and $I \subseteq J(R)$ is a $*$-ideal of $R$ then

$$R^\# \cap (1 + I) = \{z + \sqrt{1 + z^2} : z \in R^- \cap I\}.$$  

In particular, the unipotent radical of $R^\#$ is

$$R^\# \cap (1 + J(R)) = \{z + \sqrt{1 + z^2} : z \in R^- \cap J(R)\}.$$
Proof. As $R$ is Artinian, $J(R)$ is nilpotent. Hence, by Theorem 5.2,
\begin{equation}
\{z + \sqrt{1+z^2} : z \in R^- \cap I\} \subseteq R^\# \cap (1 + I).
\end{equation}
For the reverse inclusion we induct on the nilpotence class $c$ of $I$ (the smallest $c \in \mathbb{N}$ where $I^{c+1} = 0$). If $c = 0$ then the result is vacuous. Now suppose that $c > 0$ and fix $x \in R^\# \cap (1 + I).

Set $S = R/I^c$. As $I^c$ is a *-ideal, $S$ has an induced involution * and the projection epimorphism $\pi : R \to S$ is a *-homomorphism. Since $x \pi \in S^\# \cap (1 + I\pi)$, by induction there is an $s \in S^- \cap I\pi$ with $x \pi = s + \sqrt{1+s^2}$. Let $r \in I$ such that $r \pi = s$ and set $z = \frac{1}{2}(r - r^*) \in R^- \cap I$. Note that $z \pi = s$. Set $u = x - (z + \sqrt{1+z^2}) \in I^c$.

By Theorem 5.2 we know that $(z + \sqrt{1+z^2}) (z + \sqrt{1+z^2})^* = 1$. Thus
\begin{equation}
1 = xx^* = (u + (z + \sqrt{1+z^2})) (u^* + (-z + \sqrt{1+z^2})) = uu^* + u(-z + \sqrt{1+z^2}) + (z + \sqrt{1+z^2})u^* + 1.
\end{equation}
However, $uI, uI^* \subseteq I^{c+1} = 0$; whence, $uu^* = 0$, $u(-z + \sqrt{1+z^2}) = u$, and $(z + \sqrt{1+z^2})u^* = u^*$. Thus, $1 = u + u^* + 1$ which shows that $u \in R^- \cap I$. Hence, $z + u \in R^- \cap I$.

Since $zu = 0 = uz$ and $u^2 = 0$ it follows that $(u + z)^{2n} = z^{2n}$ for all $n \in \mathbb{N}$. Thus,
\begin{equation}
(u + z) + \sqrt{1+(u+z)^2} = u + z + 1 - 2 \sum_{n=1}^{\infty} C(n-1) \left(-\frac{1}{4}\right)^n z^{2n} = u + z + \sqrt{1+z^2} = x.
\end{equation}
This establishes the reverse inclusion and completes the theorem. \hfill \Box

We can now complete the proof of our first theorem.

Proof of Theorem 1.1(iii). By Theorem 2.1(iii) we know the unipotent radical $O_p(\text{Adj}(b)^\#) = \text{Adj}(b)^\# \cap (1 + J(\text{Adj}(b)))$. By Theorem 5.3 it follows that $O_p(\text{Isom}(b)) = O_p(\text{Adj}(b)^\#) = \{z + \sqrt{1+z^2} : z \in \text{Adj}(b)^- \cap J(\text{Adj}(b))\}$. \hfill \Box

5.3. Computing generators for the unipotent radical. The following consequence of Theorem 5.3 is needed for algorithmic use.

Lemma 5.4. Let $(R,*)$ be an Artinian *-ring. If $I = \langle Z \rangle$ is a *-ideal of $R$ such that, for all $m \in \mathbb{Z}^+$, $R^- \cap I^m$ is generated as an additive group by $Z \cap I^m$, then
\begin{equation}
R^\# \cap (1 + I^m) = \langle z + \sqrt{1+z^2} : z \in Z \cap I^m \rangle, \quad \forall m \in \mathbb{Z}^+.
\end{equation}

Proof. We proceed by induction on the nilpotence class $c$ of $I$, the case $c = 0$ being trivial. Let $c > 0$, $G = R^\# \cap (1 + I)$, $K = R^\# \cap (1 + I^c)$, and $H = G/K$. By Theorem 5.3, $H = (R/I^c)^\# \cap (1 + I/I^c)$. Hence, by induction $H$ is generated by $\{z + \sqrt{1+z^2} + I^c : z \in Z\}$. Set $L = \langle z + \sqrt{1+z^2} : z \in Z \rangle \leq G$ and note that $\langle L, K \rangle/K = H = G/K$; that is, $G = \langle L, K \rangle$.

As $I^{c+1} = 0$ it follows that $z + \sqrt{1+z^2} = 1 + z$ for all $z \in Z \cap I^c$. Thus, $z \mapsto z + \sqrt{1+z^2}$ is an isomorphism from the additive group $R^- \cap I^c$ to the abelian group $K$. By assumption $R^- \cap I^c = \langle z + \sqrt{1+z^2} : z \in Z \cap I^c \rangle$, so it follows that $K \leq L$. Since $G = \langle L, K \rangle$, it follows that $L = G$, as required. \hfill \Box

We now use the power series method to compute the unipotent radical of $R^\#$. 

Proposition 5.5. There is a deterministic algorithm which, given a $*$-ring $R = \mathrm{Env}(X) \subseteq M_d(F_q)$, where $F_q$ is a finite field of odd characteristic $p$, returns generators for the group $O_p(R^\#)$. The complexity of the algorithm is $O((\dim_{F_q} J(R))^3 + (\dim_{F_q} J(R)) \cdot (d^2 c + d^3 \log c)) = O^*(d^3)$ field operations.

Proof. First obtain a decomposition $R = R^+ \oplus R^-$ by finding $F_q$-bases for $R^\pm$ as subspaces of $R$. Next obtain an $F_q$-basis for $J(R)$ that exhibits the nilpotent series of $J(R)$ (cf. Remark 2.2). Thus we have a decomposition $J(R) = J_1 \oplus \ldots \oplus J_c$ as $F_q$-spaces, where a subset of the basis for $J_i$ projects to a basis for $J^i / J^{i+1}$, for $1 \leq i \leq c$, and $c$ is the nilpotence class of $J(R)$. We complete the proof using the procedure $\text{UnipotentRadical}$. 

\begin{verbatim}
\text{UnipotentRadical} ( J = J_1 \oplus \ldots \oplus J_c , R^- )
1 \text{ Z } := \emptyset
2 \text{ for i } \in \{1, \ldots, c\} \text{ do}
3 \quad \text{ U } := \text{ basis for the } F_q\text{-space } R^- \cap J_i
4 \quad \text{ U}_p := \text{ write } U \text{ as an } F_p\text{-basis}
5 \quad \text{ Z } := \text{ Z } \cup \text{ U}_p
6 \text{ U } := \langle z + \sqrt{1 + z^2} : z \in \text{ Z} \rangle
7 \text{ return U.}
\end{verbatim}

Theorem 1.1(iii) states that $U = O_p(R^\#)$. Lemma 5.4 ensures that $\text{UnipotentRadical}$ constructs generators for $U$. The construction of bases for the $F_q$-spaces $R^- \cap J_i$ requires a total of $O((\dim_{F_q} J(R))^3)$ operations in $F_q$. Expanding that basis to an $F_p$-basis uses $O(|U| \log q)$ operations in $F_p$. Finally, computing $z + \sqrt{1 + z^2}$ requires $O(c)$ additions and $O(\log c)$ multiplications in $R$ for a total of $O(\dim_{F_q} J(R)) \cdot (cd^2 + d^3 \log c)$ field operations. Note that $c \leq d$. \hfill \square

5.4. Constructing the semisimple factors. In this section we construct generators for the semisimple factor of $\text{Isom}(b)$. This section applies in all characteristics. Indeed, we suppose only that $\tau : S \to T_1 \oplus \ldots \oplus T_m$ is an effective $*$-isomorphism (i.e. it has polynomial-time algorithms to compute images and preimages) where, for $1 \leq j \leq m$, $T_j$ is the standard copy of a simple $*$-algebra over a field $F_j$. For instance, $\tau$ may be the output of the algorithm for Theorem 4.1(ii).

Proposition 5.6. There is a polynomial-time algorithm which, given an effective $*$-isomorphism $\tau : S \to T_1 \oplus \ldots \oplus T_m$, returns a generating set for $S^\#$ of size $2m$.

Proof. We call the algorithm $\text{SemisimpleFactors}$; its steps are somewhat predictable. For each $i \in \{1, \ldots, m\}$, $T_i$ is one of the simple $*$-algebras $O^+, O^-, O^c$, $U$, $X$, $S$ described in Theorem 2.2, defined naturally in dimension $d_i$ over an extension $F_i$ of $F_p$. Therefore $T^\#_i$ is the classical group associated to the algebra. (To be clear, in the exchange case, the classical group is $\text{GL}(d_i, F_i) \hookrightarrow \text{GL}(2d_i, F_i)$ where $g \mapsto (g, g^{-\text{tr}})$.)

The algorithm selects, for each $i \in \{1, \ldots, m\}$, a pair $\{g_i, h_i\}$ of generators for $T^\#_i$ (in the exchange case replacing them with $\{(g_i, g_i^{-\text{tr}}), (h_i, h_i^{-\text{tr}})\}$), and then lifts the generating pair into $T_1 \oplus \ldots \oplus T_m$ as the identity in each block $T_j$ where $j \neq i$. In this way, we obtain a generating set of size $2m$ for $T^\#_1 \times \cdots \times T^\#_m$. Using the inverse of $\tau$ we construct generators for $S^\#$. Generating pairs for all classical
groups in their defining representation were given by Steinberg [St] and fine-tuned for computation in [Ty, RT].}

5.5. Proof of Theorem 1.2: total complexity. The correctness of the algorithm IsometryGroup has been established. It remains to determine its complexity. Let \( d = \dim V \) and \( e = \dim W \). Line 2 uses \( O(d^3e) \) field operations and computes a basis \( X \) for \( \text{Adj}(b) \) (Proposition 5.1). Line 3 uses \( O^\ast(\{d^3 + d^2 \log q + d \cdot \text{Star}(R, *)\} + \text{Rand}(R)) \) field operations (Theorem 4.4). Line 4 uses \( O((\dim F_q J(R))^3 + (\dim F_q J(R)) \cdot (d^2 c + d^3 \log c)) = O^\ast(\{|X|^3 + |X|d^3\}) \) field operations. Finally, line 5 uses \( O^\ast(d^3) \) field operations (Proposition 5.6). As \( |X| = O(d^2) \), the overall complexity (in elementary operations rather than field operations) is

\[
O^\ast(\{d^3 + d^2 \log q + d \cdot \text{Star}(R, *) + |X|^2 + d^3\} \log^2 q + d^d e \log^2 q + \text{Rand}(R))
\]

This establishes Theorem 1.2. □

5.6. Intersections of classical groups. We now recast Theorem 1.2 in the language of classical groups, yielding a polynomial-time solution to the general classical group intersection problem for fields of odd characteristic.

Let \( \{G_1, \ldots, G_n\} \) be a set of general classical groups acting irreducibly on an \( F_q \)-vector space \( V \) of dimension \( d \), where the natural action of each classical group is over a field extension of \( F_q \). Thus each \( G_i \) is conjugate in \( \text{GL}(d, q) \) to one of \( \text{Sp}(m_i, F_q) \), \( \text{GU}(m_i, F_q) \), or \( \text{GO}^\epsilon(m_i, F_q) \), \( \epsilon_i \in \{-, \circ, +\} \), where \( m_i \) divides \( d \) and \( [F_q; F_q] = d/m_i \). It follows that \( G_i = \text{Isom}(\varphi_i) \) for some nondegenerate reflexive form \( \varphi_i : V \times V \to F_q \). As in Equation (1.2), \( G_1 \cap \cdots \cap G_n = \text{Isom}(b) \) for the Hermitian map \( b : V \times V \to F_1 \oplus \cdots \oplus F_n \) defined by \( b(u, v) = (\varphi_1(u, v), \ldots, \varphi_n(u, v)) \).

The structure of the intersection of classical groups is described by Theorem 1.1, and we have the following consequence of Theorem 1.2.

Corollary 5.7. There is a Las Vegas polynomial-time algorithm which, given a set \( \{G_1, \ldots, G_n\} \) of general classical subgroups of \( \text{GL}(V) \), where \( V \) is a finite vector space of odd order, returns generators for \( G_1 \cap \cdots \cap G_n \).

Proof. It suffices to find, for each \( 1 \leq i \leq n \), a reflexive nondegenerate form \( \varphi_i \) on \( V \) such that \( G_i = \text{Isom}(\varphi_i) \). Suitable forms are computed in a manner similar to Section 4.2, we detail this below.

Fix \( 1 \leq i \leq n \), and let \( G = G_i \), so that \( G = \text{Isom}(\varphi) \) for some reflexive form \( \varphi \). As \( G \) acts irreducibly, \( \text{Env}(G) \cong M_n(F) \) for a finite field extension \( F \) of \( F_q \). Use the algorithm for Theorem 2.5(ii) with input \( \text{Env}(G) \) to find \( \omega := \lambda_1 y_1 + \cdots + \lambda_k y_k \in \text{Env}(G) \) such that \( F \cong F_q[\omega] \), \( \lambda_1, \ldots, \lambda_k \in F_q \), and \( y_1, \ldots, y_k \in G \). Thus \( G \) acts absolutely irreducibly on \( U := V \otimes_G F_q[\omega] \).

Next we identify a suitable field involution of \( F \). As \( G = \text{Isom}(\varphi) \) or \( 0 \leq \text{GL}(U) \) and acts absolutely irreducibly, it follows that \( \varphi : V \times V \to F \). Also, \( \omega \in \text{Adj}(\varphi) \) and \( G = \text{Adj}(\varphi)^\# \), so that

\[
(5.11) \quad \omega^* = \lambda_1 y_1 + \cdots + \lambda_k y_k = \lambda_1 y_1^{-1} + \cdots + \lambda_k y_k^{-1}.
\]

Hence, we set \( \varpi := \omega^* = \lambda_1 y_1^{-1} + \cdots + \lambda_k y_k^{-1} \). This enables us to define the field automorphism \( \sum_{i=0}^{e-1} \lambda_i \omega^i \mapsto \sum_{i=0}^{e-1} \lambda_i \varpi^i \) on \( F = \text{Env}(1, \omega) \), where \( e = \dim F_q \).

Finally, define \( \overline{U} \) to be the (left) \( G \)-module defined by \( gu = u\varpi^{-1} \) for all \( u \in U \) and all \( g \in G \). Then \( \overline{W} := \text{Hom}_F(\overline{U}, F) \) is a right \( G \)-module. Use Lemma 2.6 to
construct a matrix $\Phi$ representing a $G$-module isomorphism from $U$ to $W$. Defining $\varphi(u, v) := u \Phi v^t$ for all $u, v \in U$, we see that $G = \text{Isom}(\varphi)$. □

Further classical groups. The algorithm for Corollary 5.7 can be modified to find the intersection of a broader set of classical groups than simply the general versions. Let $\{G_1, \ldots, G_n\}$ be a set of subgroups of $\text{GL}(V)$ preserving reflexive forms $\{\varphi_1, \ldots, \varphi_n\}$ on $V$, where $\text{Isom}(\varphi_i)' \leq G_i \leq \text{Isom}(\varphi_i)$ for $1 \leq i \leq n$.

As above we construct $I := \bigcap_{i=1}^n \text{Isom}(\varphi_i)$, whence $I' \leq \bigcap_{i=1}^n G_i \leq I$. Using the combination of determinant and spinor conditions that define each $G_i$, a generating set for $I$ can be modified to a generating set for the desired intersection. A similar approach appears in [BO2, Section 4.2].

6. Implementation

We have implemented versions of the various algorithms presented in Sections 3 through 5 for the Magma system [BCP]; code is available on request from either author. In this final section we discuss the key aspects of the implementation that differ from the description given in our proofs above. We also report on the results of a series of performance tests carried out on our implementation.

The algorithms of Eberly and Giesbrecht, and of Ivanyos, which, via Theorem 2.5, provide the platform for our polynomial-time theorems for $*$-rings, are not currently implemented in Magma [BCP]. Instead, our implementation uses Meataxe machinery [HR, IL] for which there is a highly optimized implementation distributed with Magma. This approach is described in some detail in [BO2, Section 2.1]; for completeness we summarize the main ideas here.

The fundamental component of the Meataxe is an algorithm that tests modules for irreducibility. Iterating yields an algorithm to construct a composition series for the natural module $V = \mathbb{F}_q^d$ of a given $R = \text{Env}(\mathcal{X}) \subseteq \mathbb{M}_d(\mathbb{F}_q)$. One can also use the Meataxe to test for isomorphism between each pair of composition factors. A change of basis now reveals the structure of the semisimple quotient $R/J(R)$, where the simple factors are embedded as blocks on the diagonal. Finally, the Meataxe can be applied again to a single factor to test for absolute irreducibility; if the result of such a test is negative then it also computes a generator for the centralizing field.

In this way, one obtains an effective epimorphism $\tau: R \to M_{n_1}(F_1) \oplus \cdots \oplus M_{n_\ell}(F_\ell)$ having kernel $J(R)$ exactly as in Theorem 2.5(ii). The asymptotic complexity of the Meataxe approach is somewhat worse than the algorithms for Theorem 2.5 but it is no worse than $O(d^6)$ (the overall complexity of our algorithms). In practice, this has not been a bottleneck in the performance of our implementation.

We also adapted generic Magma code for algebras defined via structure constants to produce a practical method for constructing a Wedderburn complement to the Jacobson radical of a matrix algebra, as in Theorem 2.5. Again, the underlying algorithm has asymptotic complexity no worse than $O(d^6)$. We would like to express our gratitude to W. de Graaf for his assistance in this matter.

Performance tests. We carried out two series of tests on the implementation of the IsometryGroup algorithm. The tests were carried out on a 3.2 GHz Intel Xeon microprocessor, running Version 2.15-4 of Magma. These tests and others are available with the implementation.

We decided for our first series of tests to use as input Hermitian maps for which the structure of the associated isometry group could be prescribed. In this way the
Table 1. Performance in seconds to find generators for \( \text{Sp}(d,q) \cap \text{GO}^+(d,q) \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( d = 20 )</th>
<th>( d = 40 )</th>
<th>( d = 60 )</th>
<th>( d = 80 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p = 3 )</td>
<td>0.119</td>
<td>1.684</td>
<td>7.946</td>
<td>28.322</td>
</tr>
<tr>
<td>( p = 5 )</td>
<td>0.161</td>
<td>2.679</td>
<td>52.726</td>
<td>62.626</td>
</tr>
</tbody>
</table>

The correctness of the output is verifiable, and, by tweaking the input parameters, the performance of various internal components of the algorithm could be scrutinized.

We summarize the results for two such bilinear maps.

The first test example, \( b_1 : \mathbb{F}_7^5 \times \mathbb{F}_7^5 \to \mathbb{F}_5^9 \), was constructed so that \( O_5(\text{Isom}(b_1)) \) has order \( 5^{15} \) and nilpotence class 7, and so that \( \text{Isom}(b_1)/O_5(\text{Isom}(b_1)) \) is isomorphic to \( \text{GO}^+(2,5) \times \text{GU}(3,5) \). In each of 10 runs, \( b_1 \) was written relative to a random basis for \( \mathbb{F}_7^5 \), and the average completion time was 218 seconds.

The second example, \( b_2 : \mathbb{F}_3^3 \times \mathbb{F}_3^3 \to \mathbb{F}_3^6 \), was constructed so that \( O_3(\text{Isom}(b_2)) \) has order \( 3^{30} \) and nilpotence class 4, and so that \( \text{Isom}(b_2)/O_3(\text{Isom}(b_2)) \) is isomorphic to \( \text{Sp}(4,9) \times \text{GL}(4,9) \) (the latter direct factor arising from a simple factor of \( \text{Adj}(b_2) \) of exchange type). The average time for 10 runs was 119 seconds.

Both examples illustrate that the unipotent radical is accurately computed even when the nilpotence class exceeds the characteristic of the base field. They also probe the effectiveness of the \text{TaftDecomposition} part of the algorithm, since this algorithm iterates down the derived series of the Jacobson radical of \( \text{Adj}(b) \).

For our second series of tests we computed the intersections of two classical groups of different types. This is one case where the methods of [BO1, BO2] cannot be applied. For our tests we computed the intersection of random conjugates of \( \text{Sp}(d,q) \) and \( \text{GO}^+(d,q) \) for \( d \in \{20, 40, 60, 80\} \) and \( q \in \{3, 5\} \). The results of these tests are summarized in Table 1.

Remark 6.1. After computing the structure of \( \text{Sp}(d,q) \cap \text{GO}^+(d,q) \) for various values of \( d \) and \( q \) it emerged that the corresponding algebra of adjoints had only simple factors of unitary or exchange type of rank 1 over an extension of the base field. (Compare this with intersection of symplectic groups as in [GG, Lemma 4.1].) Although we cannot yet explain this computational phenomenon, it demonstrates the experimental scope that our methods provide.

Acknowledgments

The authors would like to thank W. deGraaf and G. Ivanyos for their helpful advice on algorithms for associative rings. The second author also thanks Bucknell University for its hospitality during a recent visit in which parts of this research took place. Finally, we thank the referee for various helpful suggestions that have improved the clarity of the paper.

References


DEPARTMENT OF MATHEMATICS, BUCKNELL UNIVERSITY, LEWISBURG, PA 17837
E-mail address: pbrooksb@bucknell.edu

DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, COLUMBUS, OH 43210,
E-mail address: wilson@math.ohio-state.edu