# COMPUTING ISOMORPHISMS BETWEEN QUATERNION ALGEBRAS WITH INDEFINITE LLL

TOMMY CHAKROUN AND TRAVIS MORRISON

Abstract. We describe an algorithm for computing an isomorphism between two given definite quaternion algebras over $\mathbb{Q}$. The algorithm uses Watkin's proposed method for computing isometries of isometric quadratic forms with Simon's algorithm for computing maximal isotropic subspaces of quadratic forms. When the quaternion algebras are ramified at precisely one rational prime $p$ and we are given maximal orders in each algebra, the algorithm runs in polynomial time. That a polynomial time algorithm exists is a result of Csahók–Kutas–Montessionos–Zábrádi. The algorithm we describe, however, is practical, even on inputs of cryptographic size, and we give an implementation in Magma.

## 1. Introduction

Computing isomorphisms between quaternion algebras, and more generally, central simple algebras, is a well-studied problem. Ivanyos, Ronyai, and Schicho give a deterministic algorithm that runs in polynomial time, given access to oracles for factoring integers and polynomials over finite fields [IRS12]. The problem of computing an isomorphism between two given quaternion algebras seems to rely on factoring integers: for example, Voight proves in [Voi13, Theorem 8.2] that the problem of deciding whether a quaternion algebra is isomorphic to $M_2(\mathbb{Q})$ is probabilistic polynomial-time equivalent to the Quadratic Residuosity problem, which asks to decide if given integers $a$ and $b$ whether $a$ is a quadratic residue modulo $b'$, where $b'$ is the product of the primes at which $b$ has odd valuation. This problem is related to but not known to be equivalent to the problem of factoring.

There are many approaches to computing an isomorphism between two isomorphic quaternion algebras $B$ and $B'$ over $\mathbb{Q}$, and in this paper, we highlight another, essentially due to Watkins [Wat13, §2.7] using Simon's algorithm [Sim05b] for computing isotropic subspaces of a quadratic space over $\mathbb{Q}$. Watkins observes that if $Q$ and $Q'$ are isometric quadratic spaces, then a maximal isotropic subspace $S$ of the quadratic space $Q \boxplus -Q'$ is the graph of an isometry $Q \to Q'$. Combining this with the well-known fact that two quaternion algebras are isomorphic if and only if the quadratic spaces corresponding to their reduced norms are isometric, we see it suffices to compute an isometry between the ternary quadratic forms $G$ and $G'$ associated to the trace-zero subspaces of $B$ and $B'$. Let us now discuss the application of Simon's algorithm to this case.

Simon gives an algorithm for computing a maximal isotropic subspace of a unimodular quadratic form, i.e. a quadratic form given by a Gram matrix $G$ with determinant $\pm 1$, using the indefinite LLL algorithm [Sim05b, Sim05a]. He also proves that his algorithm for quadratic forms of odd dimension always returns a maximal

*Date*: June 10, 2026.

isotropic subspace. Finally, he gives an algorithm to minimize a quadratic form, given the factorization of its discriminant [Sim05b, Algorithm 2, "Minimization"]. If this algorithm minimizes the form to a unimodular form, then a maximal isotropic subspace can be efficiently computed. We use an argument of Watkins [Wat13] to show that if $G$ is the Gram matrix of the quadratic form $Q \boxplus -Q'$ above, Simon's minimization algorithm outputs a unimodular matrix. Thus, after factoring the discriminant of $G$, one can efficiently compute an isometry $Q \to Q'$ and hence an isomorphism $B \to B'$. Finally, we show that factoring can be avoided completely if we are given maximal orders in $B$ and in $B'$ (not necessarily isomorphic) in the special case that $B \simeq B' \simeq B_{p,\infty}$, so there is a polynomial time algorithm for computing the isomorphism of quaternion algebras. That such a polynomial time algorithm exists was first observed by Csahók–Kutas–Montessionos–Zábrádi[CKMZ22, Proposition 4.1], but, to the best of our knowledge, their algorithm is impractical. We discuss this further in the following section.

We end the introduction by providing some motivation for the above special case, where $B$ and $B'$ are ramified exactly at $\{p, \infty\}$ and we are given maximal orders in $B$ and $B'$. Namely, an algorithm for computing isomorphisms between the algebras of two maximal quaternion orders of discriminant $p$ would allow one to verify output of an algorithm for computing the endomorphism ring of a supersingular elliptic curve. If $E$ is a supersingular elliptic curve over $\overline{\mathbb{F}_p}$, then its endomorphism algebra $\mathrm{End}^0(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra, ramified exactly at $\{p, \infty\}$. The endomorphism ring $\mathrm{End}(E)$ sits inside $\mathrm{End}^0(E)$ as a maximal order. There are various computational problems involving supersingular elliptic curves whose supposed hardness underlies the security of isogeny-based cryptography. The central hard problem is: given a supersingular elliptic curve $E$, compute its endomorphism ring. The inverse problem (given a maximal order $\mathcal{O}$, compute a supersingular elliptic curve $E$ with endomorphism ring isomorphic to $\mathcal{O}$) can be solved in polynomial time. This was proved under various heuristics in [EHL$^+$18] and then unconditionally by Wesolowski in [Wes22] using the algorithm of Kohel–Lauter–Petit–Tignol [KLPT14]. The catch is that the algorithm for this problem requires that $\mathcal{O}$ is embedded in a quaternion algebra $(a, b|\mathbb{Q})$ ramified at $p$ in which one knows a quadratic order $R$ of small discriminant in a maximal order $\mathcal{O}_0$. Thus one could verify the correctness of an algorithm for computing the endomorphism ring by computing its output $\mathcal{O}$ on input $E$, computing an isomorphism $f\colon \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq (a, b|\mathbb{Q})$ using knowledge of the maximal orders $\mathcal{O}$ and $\mathcal{O}_0$, and then computing a supersingular curve $E'$ with endomorphism ring isomorphic to $f(\mathcal{O})$ and checking if $j(E') = j(E)$ or $j(E') = j(E)^p$, where $j$ is the $j$-invariant.

The polynomial-time algorithm of [CKMZ22] for computing isomorphisms of quaternion algebras isomorphic to $B_{p,\infty}$ given maximal orders inside them has been used for theoretical purposes as well. In [HLMW25] Wesolowski and Herlédan Le Merdy give a rigorous reduction between several problems related to computing isogenies and endomorphisms of supersingular elliptic curves, and the reduction in their Proposition 6.2 requires a polynomial time algorithm for computing an isomorphism between two algebras isomorphic to $B_{p,\infty}$, given maximal orders in each.

We introduce quaternion algebras, quadratic forms, and discuss other algorithms for computing quaternionic isomorphisms in Section 2. In Section 3, we discuss an

algorithm for computing an isomorphism between definite rational quaternion algebras using Simon's algorithms and prove it is correct. We also prove that it runs in polynomial time if we are given maximal orders in two isomorphic quaternion algebras of prime discriminant. We implemented the algorithm in Magma, which has Simon's algorithm for isotropic subspaces implemented already. Our implementation is available at `https://github.com/travismo/quaternion_isomorphisms`.

## 2. Background

In this section, we introduce quaternion algebras and their associated ternary quadratic forms. We also give an overview of the various known algorithms for computing an isomorphism between two quaternion algebras. Finally we recall important facts of Simon's algorithm for minimizing and computing isotropic subspaces of quadratic forms in [Sim05b].

2.1. **Quaternion algebras.** For a reference on quaternion algebras, see [Voi21]. We introduce the notation and results we need here. A **quaternion algebra** over $\mathbb{Q}$ is a central simple algebra over $\mathbb{Q}$ of dimension 4. For nonzero rational numbers $a, b \in \mathbb{Q}^\times$ we denote by $(a, b|\mathbb{Q})$ the quaternion algebra with basis $1, i, j, k = ij$ and multiplication table $i^2 = a$, $j^2 = b$, and $ij = -ji$. Every quaternion algebra over $\mathbb{Q}$ isomorphic to $(a, b|\mathbb{Q})$ for some $a, b \in \mathbb{Q}^\times$. The matrix algebra $M_2(\mathbb{Q})$ is isomorphic to to $(1, 1|\mathbb{Q})$ via the isomorphism

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad ij \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The **standard involution** on $B = (a, b|\mathbb{Q})$ is defined by

$$\begin{aligned} \bar{\cdot} \colon B &\to B \\ \alpha = w + xi + yj + zk &\mapsto \overline{\alpha} = w - xi - yj - zk. \end{aligned}$$

The **reduced norm** and **reduced trace** are defined as

$$\begin{aligned} \operatorname{nrd} \alpha &= \alpha\overline{\alpha} \\ &= w^2 - ax^2 - by^2 + abz^2 \end{aligned}$$

and

$$\begin{aligned} \operatorname{trd} \alpha &= \alpha + \widehat{\alpha} \\ &= 2w. \end{aligned}$$

The kernel of trd, the **trace-zero subspace**, is denoted $B^0$. We let $\operatorname{nrd}^0$ denote the restriction of nrd to $B^0$. The **trace pairing** on $B$ is the bilinear map

$$\begin{aligned} B \times B &\to \mathbb{Q} \\ (\alpha, \beta) &\mapsto \operatorname{trd}(\alpha\overline{\beta}). \end{aligned}$$

The quaternion algebra $B$ is **ramified** at a prime $p$ if $B \otimes_p \mathbb{Q}_p$ is a division algebra and is **split** at $p$ if $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$. We similarly define $B$ to be split or ramified at infinity if $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$ or if $B \otimes_{\mathbb{Q}} \mathbb{R}$ is a division algebra. There are only finitely many primes at which $B$ ramifies, and the **discriminant** of $B$ is the product of the ramified primes. The discriminant of $B$ determines $B$ up to isomorphism.

An **order** in $B$ is a (full) lattice that is also a subring. The **discriminant** of an order $\mathcal{O}$ is

$$\operatorname{disc}\mathcal{O} = \det\big(\operatorname{trd}(b_i\overline{b_j})\big)$$

for any basis $\{b_1, b_2, b_3, b_4\}$ of $\mathcal{O}$. An order $\mathcal{O}$ is **maximal** if it is not properly contained in another order. The discriminant $D$ of the algebra $B = \mathcal{O} \otimes_{\mathbb{Q}} \mathbb{Q}$ always divides the discriminant of the order $\mathcal{O}$, and $\mathcal{O}$ is maximal if and only if its discriminant is the discriminant of $B$.

2.2. **Quadratic forms.** Let $V$ be a finite dimensional vector space over a field $k$ of characteristic not equal to 2. A **quadratic form** on $V$ is a function $Q\colon V \to \mathbb{Q}$ such that $Q(av) = a^2 v$ for all $a \in k$ and $v \in V$ and the map $T(x, y) \coloneqq Q(x+y) - Q(x) - Q(y)$ is $k$-bilinear. We call the pair $(V, Q)$ a **quadratic space**. If $\{x_1, x_2, \ldots, x_n\}$ is a basis for $V$, we call $G = (T(b_i, b_j))$ the **Gram matrix** of $Q$ with respect to the basis $\{x_1, x_2, \ldots, x_n\}$. We say two vectors $v, w$ in $V$ are **orthogonal** if $T(v, w) = 0$, and for a subset $W$ of $V$ we let

$$W^{\perp} = \{v \in V : (\forall w \in W)(T(v, w) = 0)\}$$

denote the **orthogonal complement** of $W$ in $V$. We say that a vector $v \in V$ is **isotropic** if $Q(v) = 0$ and a subspace $W$ of $V$ is **isotropic** if every vector in $W$ is isotropic. Say that two quadratic forms $Q$ and $Q'$ on vector spaces $V$ and $V'$ are **isometric** or equivalent if there is an isomorphism $M\colon V \to V'$ such that $Q(Mv) = Q'(v)$ for all $v \in V$. A quadratic form $Q$ over $\mathbb{Q}$ is equivalent over $\mathbb{R}$ to one of the form $X_1^2 + \ldots + X_r^2 - Y_1^2 - \ldots - Y_s^2$; we call the pair $(r, s)$ the **signature** of $Q$. The number $r$ (respectively $s$) is the dimension of the largest subspace on which $Q$ restricts to a positive (respectively negative) quadratic form. The **radical** of $Q$ is the subspace $V^{\perp}$; we say $Q$ is **nondegenerate** if $V^{\perp} = 0$. We call the quadratic form $Q$ **unimodular** with respect to the basis $\{x_1, \ldots, x_n\}$ if its Gram matrix with respect to this basis is unimodular, i.e. has determinant 1 or $-1$.

A **hyperbolic plane** is a two-dimensional quadratic space $H$ with pairing $T$ that contains two isotropic vectors $x$ and $y$ such that $T(x, y) \neq 0$. Thus the Gram matrix for $T$ with respect to the basis $\{x, y\}$ is (possibly after scaling) given by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. A **generalized hyperbolic plane** is a two dimensional space with Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & \epsilon \end{pmatrix}$ with $\epsilon = 0$ or 1.

Let $B = (a, b|\mathbb{Q})$ be a quaternion algebra and let $\mathcal{O}$ be an order in $B$. The **quadratic space** associated to $B$ is the pair $(B, \mathrm{nrd})$ and we similarly define the quadratic space $(B^0, \mathrm{nrd}^0)$. We have that $B \simeq B'$ as quaternion algebras if and only if $B \simeq B'$ as quadratic spaces if and only if $B^0 \simeq (B')^0$ as quadratic spaces [Voi21, Proposition 5.2.4]. In particular, if $f\colon B^0 \to (B')^0$ is an isometry of quadratic spaces, then we extend $f$ to a map $B \to B'$ by defining $f(1) = 1$ and extending linearly; then exactly one of $f$ or $\widehat{f}$, the map obtained by post-composing $f$ with the standard involution on $B'$, is an isomorphism of quaternion algebras. If $B = (a, b|\mathbb{Q})$ and $f(ij) = f(i)f(j)$ then $f$ is an isomorphism of algebras. Otherwise, we have $f(ij) = f(j)f(i)$ and $\widehat{f}$ is an isomorphism of quaternion algebras.

2.3. **Simon's algorithm.** In [Sim05b], Simon gives an algorithm (Algorithm 2, "maximal totally isotropic subspace") for finding a maximal isotropic subspace of

a unimodular quadratic form $G$. He also gives an algorithm (Algorithm 3, "Minimization") for minimizing a given quadratic form's determinant via linear transformations. The rest of Simon's paper concerns finding isotropic vectors of quadratic forms that are not unimodular in dimensions 4, 5, and $n \geq 5$, in which he splits into the cases of odd and even dimension. When $n$ is odd and, given the factorization of $\Delta$, Simon's Algorithm 6 efficiently computes a maximal isotropic subspace of $G$; see Section 6 of [Sim05b]. However, when $n$ is even, Simon's algorithm produces an isotropic subspace that is not guaranteed to be maximal. If the output $G_m$ of Simon's minimization algorithm is unimodular, though, Algorithm 2 will return a maximal isotropic subspace of $G_m$ and hence of $G$. Watkins, in [Wat13, §2.3], highlights the properties proved in [Sim05b, Proposition 10] of a minimized quadratic form. We reproduce it here since we need these properties later, since we will need to show that the minimization of the quadratic forms we consider are unimodular.

**Proposition 2.1** ([Sim05b, Proposition 10],[Wat13, §2.3])**.** *Let $G$ be a symmetric matrix in $M_n(\mathbb{Z})$ with nonzero determinant and let $G_m$ be the output of the Minimization algorithm. Let $\Delta = \det G_m$.*

- *If $n$ is odd, $\det(G)$ is odd and squarefree and the maximal dimension of a totally isotropic subspace at a prime $p | \det G_m$ is $(n-3)/2$.*
- *If $n$ is even, $v_p(\det G) \leq 2$ for all primes $p$ and $v_2(\det G) \leq 1$. If $p^2 | \det G_m$ then the maximal dimension of a totally isotropic subspace at a prime $p$ is $(n-4)/2$.*
- *The kernel of $G$ modulo $p$ has dimension $v_p(\det G)$.*

2.4. **Algorithms for computing an isomorphism of quaternion algebras.** Let $B = (a, b|\mathbb{Q})$ and $B' = (a', b'|\mathbb{Q})$ be quaternion algebras, which we assume are isomorphic and non-split. Let $i, j$ denote the generators of $B$ and let $i', j'$ denote the generators of $B'$. The most natural approach to computing an isomorphism $f\colon B \to B'$ is to first find an element $\mu \in (B')^0$ such that $\mu^2 = a'$. By the Skollem-Noether theorem, there is an element $\nu \in (B')^0$ such that $\mu\nu = -\nu\mu$ and $\nu^2 = b'$. Then the map $i \mapsto \mu, j \mapsto \nu$ extends to an isomorphism $B \to B'$. Thus we must find the elements $\mu$ and $\nu$ in $(B')^0$. Write $\mu = Xi' + Yj' + Zi'j'$. We need to solve the quadratic equation $a'X^2 + b'Y^2 - a'b'Z^2 = a$. The quadratic form on the left-hand side is anisotropic since $B'$ is not split, so we need to find any solution to

$$a'X^2 + b'Y^2 - a'b'Z^2 - aW^2 = 0.$$

This can be done with Simon's algorithm, requiring the factorization of the integers $a, a'$, and $b'$. We now need to find $\nu \in \mu^\perp$ such that $\nu^2 = b$. Let $\xi \in \mu^\perp$ be any nonzero element, which can be found by solving a system of linear equations. Let $\gamma = \xi^2 \in \mathbb{Q}$. The quaternions $\xi$ and $\mu\xi$ form a basis of $\mu^\perp$. Let $\nu = (x + y\mu)\xi$. We want to find $x, y \in \mathbb{Q}$ such that $\nu^2 = b$, which is equivalent to solving the equation $x^2 - ay^2 = \beta/\gamma$. Again one can use Simon's algorithm.

Another approach, which is implemented in Magma, instead solves norm equations over a quadratic extension of $\mathbb{Q}$. The idea is that the quadratic extension $L = \mathbb{Q}(\sqrt{a})$ splits both $B$ and $B'$, so one reduces the problem to solving two norm equations over $L$. This approach works for fields other than $\mathbb{Q}$, but it is not as efficient as the above approach when working with rational quaternion algebras.

We now move on to another approach due to Ivanyos, Rónyai, and Schicho [IRS12]. Since $B \simeq B'$ we have that $B \otimes_{\mathbb{Q}} (B')^{op} \simeq M_4(\mathbb{Q})$. Given an isomorphism $\Phi\colon B \otimes B' \simeq M_4(\mathbb{Q})$, one can efficiently find an isomorphism $f\colon B \to B'$. This

reduces the problem to computing an isomorphism between a central simple algebra $A$ and $M_n(\mathbb{Q})$. Define the **rank** of an element $x \in A$ to be $\dim_{\mathbb{Q}}(Ax)/n$. Then the rank of $x$ is the rank of $\phi(x)$ for any isomorphism $\phi\colon A \simeq M_n(\mathbb{Q})$. The algorithm proceeds as follows:

(1) Compute a maximal order $O \subseteq A$
(2) Find an element $x$ of rank 1 in $\mathcal{O}$
(3) Return the map $A \to \mathrm{End}_{\mathbb{Q}}(Ax)$ given by $b \mapsto [z \mapsto bz]$.

The algorithm is correct: the map is injective since $A$ is simple and by counting dimensions, it is an isomorphism. Finally, we can find an isomorphism $\mathrm{End}_{\mathbb{Q}}(Ax) \simeq M_n(\mathbb{Q})$ by computing a basis of $Ax$.

Let us now return to the case of interest, $A \simeq M_4(\mathbb{Q})$, and consider the complexity of this algorithm; Ivanyos-Rónyai-Schicho prove that it runs in polynomial time given an oracle for factoring integers [IRS12, Corollary 10]. The first step is where factoring comes in. One first computes one order in $A$, and then upgrades it to a locally maximal order for each prime dividing the discriminant of the initial order $\mathcal{O}$. The third step requires only linear algebra and is efficient. Apart from the need to factor, the first step is quite practical. The second step can be done in polynomial time, using an algorithm of Ivanyos, Rónyai, and Schicho, which proceeds as follows. First, embed the maximal order $\Gamma$ into $M_n(\mathbb{R})$ and then find a sufficiently short vector so that it has rank one. This rank one element is an integer linear combination of a certain basis of $\Gamma$ with coefficients bounded by $c_{16} = (\gamma_{16})^8(3/2)^{16}2^{120}$ [IRS12, (2), pg. 5 ]. Thus while the desired rank one vector can be found in polynomial time, the algorithm is impractical, given the size of the search space.

One benefit of the Ivanyos–Rónyai–Schicho algorithm is that, as observed by Csahók–Kutas–Montessionos–Zábrádi [CKMZ22], it can exploit knowledge of maximal orders in $B$ and $B'$ and the factorization pattern of the discriminant of $B$. Suppose $\mathcal{O}$ and $\mathcal{O}'$ are maximal orders in $B$ and $B'$, and we know the ramified primes of $B$ (and hence of $B'$). The order $\mathcal{O} \otimes_{\mathbb{Z}} (\mathcal{O}')^{op}$ is maximal at every prime except the ramified primes of $B$, since its discriminant is $(\operatorname{disc}\mathcal{O}\operatorname{disc}\mathcal{O}')^4$, so given the ramified primes and the orders, there is no need to factor in order to compute a maximal order in $A = B \otimes_{\mathbb{Q}} (B')^{op}$. In particular, if $B \simeq B' \simeq B_{p,\infty}$, the quaternion algebra ramified exactly at $\{p, \infty\}$, there is a polynomial time algorithm to compute an isomorphism $B \simeq B'$ given maximal orders in $B$ and $B'$, since the discriminants of these orders are both equal to $p^2$ [CKMZ22, Proposition 4.1].

In Section 3.1, we will see that Watkin's method of computing an isometry between quadratic forms using Simon's algorithm gives a practical method to compute an isomorphism between two isomorphic non-split quaternion algebras over $\mathbb{Q}$, and that no factoring is needed when applied to the case $B \simeq B' \simeq B_{p,\infty}$ and one is given a maximal order in each of $B$ and in $B'$.

## 3. Isomorphisms between quaternion algebras from isometries

As a warmup, we revisit the problem of computing an isomorphism to $M_2(\mathbb{Q})$ from a split quaternion algebra over $\mathbb{Q}$. This problem is discussed in detail in [Voi13]. Given $x \in B$ such that $x^2 = 0$, Algorithm 4.3 of [Voi13] efficiently computes an isomorphism $B \simeq (1, 1|\mathbb{Q})$. We give another proof of this, in the language of quadratic forms.

**Proposition 3.1.** *Let $B = (a, b|\mathbb{Q})$ be a split quaternion algebra. There is a polynomial time algorithm that, given a nonzero solution to $-aX^2-bY^2+abZ^2 = 0$, returns an isomorphism $B \simeq (1, 1|\mathbb{Q})$.*

*Proof.* Let $S = \mathrm{diag}(-2a, -2b, 2ab)$ be the Gram matrix of the norm form of $B$ restricted to the trace-zero subspace $B^0$ and let $b_1 \in \mathbb{Q}^3$ be a nonzero vector satisfying $b_1^T S b_1 = 0$. Choose a vector $v \in \mathbb{Q}^3$ such that $b_1^T S v = 1$. Define $b_2 = -\frac{q(v)}{2}u + v$. Then $b_1^T S b_2 = 1$ and $b_2^T S b_2 = 0$. The kernel of the $3 \times 2$ matrix $(b_1|b_2)^T S$ has dimension 1 since $b_1$ and $b_2$ are linearly independent, so there is some nonzero vector $w$ in its kernel. We have $b_1^T S w = b_2^T S w = 0$. Let $M' = (b_1|b_2|w)$. Then

$$(M')^T S M' = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

for some $\alpha \in \mathbb{Q}$. In fact, since $\det(S) \in 2\mathbb{Q}^{\times 2}$, we have that $\alpha = -2r^2$ for some nonzero $r \in \mathbb{Q}$. Define $b_3 = r^{-1}w$ and $M = (b_1|b_2|b_3)$. Then

$$M^T S M = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

is the Gram matrix of the quadratic form $UV - W^2$. This quadratic form is equivalent to $-X^2 - Y^2 + Z^2$ via the change of variables $U = Z - Y$, $V = Z + Y$, $W = X$. Thus setting

$$N = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

we get $(MN)^T S MN = \mathrm{diag}(-2, -2, 2)$ as desired. To compute the matrices $M$ and $N$ we need only linear algebra and the computation of a square root of a square rational number, all of which can be done efficiently. □

3.1. **Computing isomorphisms between division quaternion algebras.** We now suppose $B$ and $B'$ are two isomorphic division quaternion algebras over $\mathbb{Q}$. As mentioned in the introduction, to compute an isomorphism $B \simeq B'$ it suffices to compute an isometry between the trace-zero subspaces $B^0$ and $(B')^0$. Watkins [Wat13, §2.7] explains how an isomorphism between two isomorphic quadratic forms $Q$ and $Q'$ can be recovered from a basis of a maximal isotropic subspace for the quadratic form $Q \boxplus -Q'$. Let $G$ and $G'$ be the Gram matrices of their trace-zero subspaces. We desire $M \in \mathrm{GL}_3(\mathbb{Q})$ such that $M^T G_1 M = G_2$. Consider the quadratic form $G = G_1 \boxplus -G_2$ on $\mathbb{Q}^6$. This form has signature $(3, 3)$ and isotropy index 3. Indeed, the matrix $(M^T|I_3)^T$ has rank 3 and its columns span an isotropic subspace:

$$(M^T|I_3)G(M^T|I_3)^T = M^T G_1 M - G_2 = 0.$$

Thus it suffices to compute a maximal isotropic subspace of $G \boxplus -G'$. The algorithm of Simon in [Sim05b] computes an isotropic subspace of a given quadratic form, and the isotropic subspace is maximal of the form can first be reduced to a unimodular one. We prove in the following proposition, with an argument due to Watkins in [Wat13, §2.62], that our quadratic form $G \boxplus -G'$ is minimized to a unimodular quadratic form by Simon's minimization algorithm.

**Proposition 3.2.** *Let $Q = Q_1 \boxplus -Q_2$ be the orthogonal sum of the ternary quadratic forms of two quaternion algebras of discriminant $D > 1$. Let $G$ be the Gram matrix of $Q$. Let $G_m$ denote the minimization of $G$. Then $G_m$ is unimodular.*

*Proof.* The proof is due to Watkins [Wat13, §2.62]. We sketch it here. Suppose $\det(G_m)$ is square-free and not equal to 1 or $-1$. Since $Q$ has an isotropic subspace of dimension 3, we can find a unimodular transformation such that

$$G \simeq H(d_1) \boxplus H(d_2) \boxplus H(d_3)$$

for integers $d_i$, where $H(d_i)$ is the quadratic space with Gram matrix $\begin{pmatrix} 0 & d_i \\ d_i & \epsilon \end{pmatrix}$ for $\epsilon = 0$ or 1. This would imply $\det(G_m) \in -\mathbb{Q}^{\times 2}$, contradicting the assumption that $\det(G_m)$ is squarefree.

Thus if $\det(G_m) \neq -1$, it is divisible by $p^2$ for some odd prime $p$. Then by the properties of a minimized form in Proposition 2.1, the reduction of $G_m$ modulo $p$ has a 2-dimensional kernel. Let $v, w$ be primitive vectors in $\mathbb{Z}^6$ whose images in $\mathbb{F}_p^6$ generate the kernel of $G_m$ modulo $p$. Let $G'$ denote an orthogonal complement to the radical of $G_m$ modulo $p$. Since $G_m$ is minimized, the dimension of a maximal isotropic subspace for $G'$ is 1, again by Proposition 2.1. Thus $G'$ has isotropy index of 1 over $\mathbb{Q}$ as well. Since there is an isotropic subspace of $\mathbb{Q}^6$ for $G_m$ of dimension 3, the isotropy index increases by 2 when we adjoin the vectors $v$ and $w$, so $v$ and $w$ are themselves isotropic. There is a unimodular transformation to a basis $\{v, w, e_3, e_4, e_5, e_6\}$ with Gram matrix

$$\begin{pmatrix} 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 \\ a & 0 & * & * & * & * \\ 0 & b & * & * & * & * \\ 0 & 0 & * & * & * & * \\ 0 & 0 & * & * & * & * \end{pmatrix}$$

where $a \equiv b \equiv 0 \pmod{p}$ since $v$ and $w$ generate the kernel of $G_m$ modulo $p$. Indeed, if $\{v, w, e_3, e_4, e_5, e_6\}$ is any integral basis, then $a_i = v^T G_m e_i \equiv 0 \pmod{p}$ for $3 \leq i \leq 6$, so if $V \in \mathrm{GL}_4(\mathbb{Z})$ puts the row vector $(a_3, a_4, a_5, a_6)$ into Hermite normal form, i.e.

$$(a_3, a_4, a_5, a_6)V = (\gcd(a_i), 0, 0, 0),$$

we have $a = \gcd(a_i) \equiv 0 \pmod{p}$. We similarly put the second row/column into Hermite Normal Form by a unimodular transformation, obtaining the claimed matrix. But this matrix has determinant divisible by $p^4$, so $v_p(\det G_m) \geq 4$, contradicting the assumption that $G_m$ is minimized. □

We thus have the following algorithm:

**Theorem 3.3.** *Algorithm 1 is correct and, given the factorization of* $\det(G) = \det(G')$*, runs in polynomial time in the size of its input.*

*Proof.* Correctness follows from Proposition 3.2. That Algorithms 1 and 5 of [Sim05b] are efficient (apart from the factorization needed for minimization) is proved in [Sim05b]. □

Given the matrix $M$, we have an isomorphism $B^0 \to (B')^0$ which we can extend linearly to an isomorphism $B \to B'$, possibly after post-composing with the

**Algorithm 1** Recovering an isomorphism from trace-zero norm forms

**Require:** Quadratic forms $G, G' \in S_3(\mathbb{Z})$ of the trace-zero subspaces of isomorphic, non-split quaternion algebras

**Ensure:** A matrix $M \in \mathrm{GL}_3(\mathbb{Q})$ such that $M^T G M = G'$

1: Compute the minimized quadratic form

$$G_m \leftarrow \textsc{Minimize}\big(G \boxplus (-G')\big)$$

using [Sim05b, Algorithm 3]

2: Compute a basis

$$W = (A \mid B) \in M_{3\times 6}(\mathbb{Q})$$

of a maximal totally isotropic subspace of $G_m$ using [Sim05b, Algorithm 1]

3: **return** $B^{-1}A$

involution on $B'$. This algorithm runs in polynomial time apart from the factorization of $\det(G)$, and appears to be faster than Magma's algorithm for computing isomorphisms. See Section 4 for more on the implementation and timings.

3.2. **Isomorphisms between algebras isomorphic to $B_{p,\infty}$.** We conclude with a practical, polynomial time algorithm for computing an isomorphism between two quaternion algebras $B$ and $B'$ that are isomorphic to $B_{p,\infty}$, the quaternion algebra ramified at $p$ and $\infty$, given maximal orders $\mathcal{O}$ and $\mathcal{O}'$ in $B$ and $B'$. We do not require that the orders $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic.

**Lemma 3.4.** *Assume $\mathcal{O}$ is a maximal order in a quaternion algebra $B$. If $\{e_1, e_2, e_3\}$ is a basis for the trace-zero subspace $\mathcal{O}^0$ of $\mathcal{O}$, then*

$$\det(\mathrm{trd}(e_i\overline{e_j})) = -2\left(\prod_{p \text{ ramified in } B} p\right)^2.$$

*Proof.* The lattice $L = \mathbb{Z} \oplus \mathcal{O}^0$ is the kernel of the map

$$\begin{aligned} \mathcal{O} &\to \mathbb{Z}/2\mathbb{Z} \\ \alpha &\mapsto \mathrm{trd}\,\alpha \pmod 2. \end{aligned}$$

This map is surjective: since $\mathcal{O}$ is maximal, it has an element of odd trace, as otherwise the discriminant of $\mathcal{O}$ would be divisible by $2^4$. Thus

$$\mathrm{disc}(L) = [\mathcal{O} : L]^2 \,\mathrm{disc}\,\mathcal{O} = 4\,\mathrm{disc}\,\mathcal{O}.$$

On the other hand,

$$\mathrm{disc}(L) = \left|\det\begin{pmatrix} 2 & 0 \\ 0 & (\mathrm{trd}(e_i\overline{e_j})) \end{pmatrix}\right| = 2|\det(\mathrm{trd}(e_i\overline{e_j}))|.$$

We determine the sign of $\det(\mathrm{trd}(e_i\overline{e_j}))$ is negative since the determinant of the Gram matrix of $B^0$ with basis $i, j, ij$ is $\det(diag(2a, 2b, -2ab)) = -4(ab)^2 < 0$. □

**Proposition 3.5** ([CKMZ22, Proposition 4.1],[Wat13],[Sim05b])**.** *There is a polynomial time algorithm that, on input the bases of maximal orders $\mathcal{O}$ and $\mathcal{O}'$ in quaternion algebras $(a, b|\mathbb{Q}) \simeq (a', b'|\mathbb{Q})$ ramified at $\{p, \infty\}$, outputs an isomorphism $(a, b|\mathbb{Q}) \simeq (a', b'|\mathbb{Q})$.*

*Proof.* Compute bases of the trace-zero subspaces $\mathcal{O}^0$ and $(\mathcal{O}')^0$, letting $G$ and $G'$ denote their Gram matrices. Compute a basis of maximal isotropic subspace $W$ of $G \boxplus -G'$ using Simon's algorithm [Sim05b]. The determinant of $G \boxplus -G'$ is $-4p^4$ and thus can be factored easily. By Proposition 3.2, the minimized form is unimodular with determinant $-1$, so [Sim05b, Algorithm 1] efficiently finds a basis $W$ for a maximal isotropic subspace of $G \boxplus -G'$. Thus Algorithm 1 is efficient since we can efficiently factor $\det(G \boxplus -G')$. □

## 4. Implementation

We implemented Algorithm 1 in Magma, using the intrinsic `IsotropicSubspace` to compute a maximal isotropic subspace of $G \boxplus -G'$. We find that even on inputs of large size, say quaternion orders in an algebra $B$ of prime discriminant $p$ of bit length 200, the algorithm takes a small fraction of a second to compute the isometry $G \to G'$. The implementation is available at `https://github.com/travismo/quaternion_isomorphisms`. We tested it with Magma Version 28-15 with a AMD Ryzen 5 3600X 6-Core Processor with 15 gigabytes of RAM running Ubuntu 22.04.5. We found that our algorithm for computing an equivalence of ternary quadratic forms consistently outperformed the Magma intrinsic for quaternion orders of prime discriminant of bitlength $16 \leq b \leq 20$, and once the bitlength reached 32, the Magma intrinsic did not terminate after 10 minutes. Meanwhile, our `Equivalence` function computed the isometry of ternary quadratic forms of quaternion algebras of discriminant $p = 126765060022822940149670320563$, a prime of roughly 100 bits in length, in 6.820 seconds. When given the ternary quadratic forms of maximal orders, it terminates in 0.020 seconds.

## References


[CKMZ22] Tímea Csahók, Péter Kutas, Mickaël Montessinos, and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. *Res. Number Theory*, 8(4):Paper No. 77, 24, 2022.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.

[HLMW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. Unconditional foundations for supersingular isogeny-based cryptography. In *Theory of Cryptography: 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1–5, 2025, Proceedings, Part III*, page 266–297, Berlin, Heidelberg, 2025. Springer-Verlag.

[IRS12] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho. Splitting full matrix algebras over algebraic number fields. *J. Algebra*, 354:211–223, 2012.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion $\ell$-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17:418–432, 2014.

[Sim05a] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Math. Comp.*, 74(251):1531–1543, 2005.

[Sim05b] Denis Simon. Quadratic equations in dimension 4, 5, and more. Preprint, 2005. https://simond.users.lmno.cnrs.fr/maths/Dim4.pdf.

[Voi13] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. *Developments in Mathematics*, 31:255–298, 2013.

[Voi21] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021.

[Wat13] Mark Watkins. Some comments about indefinite LLL. In *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, volume 587 of *Contemp. Math.*, pages 233–243. Amer. Math. Soc., Providence, RI, 2013.

[Wes22] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *FOCS 2021 - 62nd Annual IEEE Symposium on Foundations of Computer Science*, Denver, Colorado, United States, February 2022.

ENS Paris-Saclay, Gif-sur-Yvette, Paris
*Email address*: tommy.chakroun@ens-paris-saclay.fr

Virginia Tech, Blacksburg, Virginia, USA
*Email address*: tmo@vt.edu
*URL*: travismo.github.io