Internship Report

Computing Explicit Isomorphisms Between Quaternion Algebras: Algorithms and Elliptic Curve Applications

Tommy Chakroun

Supervised by

Travis Morrison

June 2025

Abstract

This report addresses the computational problem of finding an explicit isomorphism between two quaternion algebras over the field of rational numbers, $\mathbb{Q}$. Quaternion algebras, which are 4-dimensional central simple algebras, are fundamental objects in number theory. They arise naturally in the study of ternary quadratic forms and, crucially, as the endomorphism algebras of supersingular elliptic curves, which provides the primary motivation for this work.

We investigate, implement, and compare three distinct algorithmic approaches. The first is a direct method that translates the isomorphism problem into solving a sequence of quadratic equations over $\mathbb{Q}$, relying on algorithms for finding rational points on quadrics. The second method is more theoretical, leveraging the structure of central simple algebras. It reduces the problem to explicitly splitting the tensor product algebra $A \otimes B^{\mathrm{op}} \cong \mathrm{M}_4(\mathbb{Q})$, a task for which polynomial-time algorithms exist but are currently impractical to implement. The third, and most effective, method utilizes the correspondence between quaternion algebras and ternary quadratic forms. The problem is reframed as finding an explicit equivalence between two quadratic forms, which we achieve by computing a maximal isotropic subspace of a related 6-dimensional quadratic form.

Our analysis shows that the complexity of all three methods is fundamentally tied to integer factorization. While the first method is direct, its performance degrades due to the size of intermediate coefficients. The third method proves to be the most practical and efficient, providing a feasible algorithm whose main bottleneck is the initial factorization of the algebra parameters.

Ce rapport traite du problème algorithmique de la construction d'un isomorphisme explicite entre deux algèbres de quaternions sur le corps des nombres rationnels, $\mathbb{Q}$. Les algèbres de quaternions, qui sont des algèbres simples centrales de dimension 4, sont des objets fondamentaux en théorie des nombres. Elles apparaissent naturellement dans l'étude des formes quadratiques ternaires et, de manière cruciale, en tant qu'algèbres d'endomorphismes des courbes elliptiques supersingulières, ce qui constitue la principale motivation de ce travail.

Nous étudions, implémentons et comparons trois approches algorithmiques distinctes. La première est une méthode directe qui traduit le problème d'isomorphisme en la résolution d'une suite d'équations quadratiques sur $\mathbb{Q}$, en s'appuyant sur des algorithmes de recherche de points rationnels sur des quadriques. La deuxième méthode est plus théorique et s'appuie sur la structure des algèbres simples centrales. Elle réduit le problème à la décomposition explicite de l'algèbre produit tensoriel $A \otimes B^{\mathrm{op}} \cong \mathrm{M}_4(\mathbb{Q})$, une tâche pour laquelle des algorithmes en temps polynomial existent mais sont actuellement impraticables à implémenter. La troisième méthode, la plus efficace, utilise la

correspondance entre les algèbres de quaternions et les formes quadratiques ternaires. Le problème est reformulé comme la recherche d'une équivalence explicite entre deux formes quadratiques, ce qui est réalisé en calculant un sous-espace isotrope maximal d'une forme quadratique associée en dimension 6.

Notre analyse montre que la complexité des trois méthodes est fondamentalement liée à la factorisation des entiers. Alors que la première méthode est directe, ses performances se dégradent en raison de la taille des coefficients intermédiaires. La troisième méthode s'avère être la plus pratique et la plus efficace, fournissant un algorithme réalisable dont le principal goulot d'étranglement est la factorisation initiale des paramètres des algèbres.

Mathematics Subject Classification: 11R52, 11E12, 11-04

Keywords: Quaternion algebras, computational number theory, quadratic forms, isomorphism.

Contents

1. Introduction

Quaternion Algebras. Quaternion algebras are central simple algebras of dimension 4. When $\mathrm{char}(F) \neq 2$, these algebras admit a very concrete description: they have a basis $1, i, j, ij$ with $i^2 = a \in F^\times$, $j^2 = b \in F^\times$, and $ij = -ji$. We denote such an algebra by $\left(\frac{a,b}{F}\right)$. See [Voi21].

Isomorphism of Quaternion Algebras: Statement of the Problem. The central computational task of this report is to solve the following problem. Let $\alpha, \beta, a, b \in \mathbb{Z}$.

Problem `IsoQuatAlg`(α, β, a, b) : Assuming $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ are isomorphic as $\mathbb{Q}$-algebras, compute an explicit isomorphism $f : A \to B$.

For complexity analysis, we consider the size of the input to be t the maximum of the size of the integers α, β, a, b, where the size of an integer is its bit length.

Motivation from Elliptic Curve Theory. See [Voi21, Chapter 42] for a complete overview about the link with elliptic curve. Elliptic curves are special projective plane curves that carry a natural abelian group structure. The computational properties of these groups are of great interest in cryptography due to the hardness of the discrete logarithm problem. On a more abstract level, one can define *isogenies* between elliptic curves—morphisms of algebraic varieties that are also group homomorphisms. For an elliptic curve E, the set $\mathrm{End}(E)$ of isogenies from E to itself forms a ring. This endomorphism ring gives rise to computational problems with cryptographic applications. A key result is that for certain elliptic curves, called *supersingular*, the endomorphism algebra $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ has the structure of a quaternion algebra over $\mathbb{Q}$.

Methods of this Report. Let $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ (where α, β, a, b are integers) be two isomorphic quaternion algebras over $\mathbb{Q}$. We investigate three main approaches to compute an explicit isomorphism $f : A \to B$.

- The first method, a natural and direct approach, is to determine the algebraic conditions that the images of the basis elements of A must satisfy in B. This requires solving quadratic equations of dimensions 3 and 4 over the rationals. This can be done using the algorithms of Denis Simon ([Sim05b], [Sim05a]). **Complexity**: Requires factorizing the parameters a, b, c, d, plus an additional

rational number that is difficult to control. Expecting these factorizations, the algorithm then runs in polynomial time in the size of the input. **Implementation**: We provide a feasible implementation in SageMath.

- The second method is more conceptual and relies on the structure theory of central simple algebras. A key theorem states that $A \cong B$ if and only if $A \otimes_{\mathbb{Q}} B^{\mathrm{op}} \cong \mathrm{M4}\mathbb{Q}$. Letting $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$, this builds a bridge to a special case of a classical problem in computational algebra:

  Problem `SplittingMatrixAlgebraDegree4`$(c_{i,j,k})$: Given a $\mathbb{Q}$-algebra C by its structure constants $c_{i,j,k}$, which is known to be isomorphic to $\mathrm{M}_4(\mathbb{Q})$, compute an explicit isomorphism from C to $\mathrm{M}_4(\mathbb{Q})$.

  It is generally believed ([IRS12] and [ILR12]) that it is easier to solve this problem if we know a *maximal order* in C. For our purpose, where $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$, we can make use of the knowledge of maximal orders within A and B and the knowledge of ramified primes to compute maximal orders in C ([Csa+22], [IR93]). **Complexity**: Given maximal orders in A and B and their ramified primes, this method yields an algorithm that runs in polynomial time in the size of the coefficients α, β, a, b. **Implementation**: However, to my knowledge, this algorithm is theoretical and cannot be implemented in practice due to a prohibitively large search space. We still provide an implementation of several reduction steps in SageMath.

- The last method uses the correspondence between quaternion algebras and ternary quadratic forms. The isomorphism problem translates to an equivalence problem for quadratic forms. We use an idea by Mark Watkins, which reduces the problem to finding a maximal isotropic subspace of a quadratic form over $\mathbb{Q}^6$. This last step is accomplished using an algorithm by Denis Simon. **Complexity**: In general, this requires factorizing the parameters a, b, c, d, and then runs in polynomial time. If maximal orders and ramified primes are given, the algorithm runs in practical polynomial time. **Implementation**: Feasible; we provide an implementation of this method in Magma.

State of the Art.

- In [Voi12], Voight presents some algorithms around the problem of isomorphism between a quaternion algebra and the matrix ring. He also studied some results on theoretical complexity.

- In [IS96], Ivanyos gives a polynomial-time algorithm to compute an isomorphism between an algebra and the matrix ring $\mathrm{M}_2(\mathbb{Q})$ given a maximal order.

- In [Csa+22, Proposition 4.1], there is a theoretical polynomial-time algorithm to compute the isomorphism of a quaternion algebra ramified at a prime and at infinity, given a maximal order in each. The method can be immediately extended when given quaternion algebras and their set of ramified primes.
- This last algorithm relies on the work of Ivanyos, Rónyai, and Schicho [IRS12] and [ILR12] about the splitting problem applied to degree 4.
- The computer system Magma has implemented a function `IsIsomorphism(A,B:Isomorphism:=True)` which computes an isomorphism between two quaternion algebras if one exists. This algorithm also works for algebras over a number field, and it is based on Method 1 6.

Contents. This report is structured as follows. In Section 2, we introduce quaternion algebras and their fundamental properties, including their connection to quadratic forms. Section 3 reviews the problem of deciding whether two quaternion algebras over $\mathbb{Q}$ are isomorphic, highlighting its equivalence to integer factorization under standard assumptions. We discuss the crucial role of orders in Section 4, defining maximal orders and their discriminants. The special case of finding an isomorphism for split algebras is detailed in Section 5.

The core of the report presents three distinct methods for computing an explicit isomorphism. **Method 1**, detailed in Section 6, follows a direct approach by solving systems of quadratic equations. **Method 2**, explored in Section 7, takes a more abstract route by reducing the problem to splitting a 16-dimensional matrix algebra. **Method 3**, described in Section 8, leverages the theory of quadratic forms to provide the most practical algorithm.

Finally, Appendix A provides a brief overview of the theory of central simple algebras, and Appendix **??** discusses details of the algorithms' implementations and their performance.

Implementation. An implementation of most of the algorithms presented in this report is available on GitHub:

`https://github.com/TommyChakroun/quat_alg_project`

2. Quaternion Algebras

Definition. Let F be a field with $\mathrm{char}(F) \neq 2$. For all $a, b \in F^\times$, there exists a unique unitary and associative F-algebra B, up to F-algebra isomorphism, containing elements i, j such that $1, i, j, ij$ form an F-basis and satisfy the relations:

$$i^2 = a, \quad j^2 = b, \quad \text{and} \quad ij = -ji. \tag{1}$$

We denote such an algebra by

$$\left(\frac{a, b}{F}\right) = F \oplus Fi \oplus Fj \oplus Fij.$$

These are called *quaternion algebras*. Their existence can be verified by constructing the multiplication table defined by these relations and checking associativity.

An important example is the matrix algebra $\mathrm{M}_2(F)$. If $\mathrm{char}(F) \neq 2$, then $\mathrm{M}_2(F) \cong \left(\frac{1,1}{F}\right)$ via the basis:

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

We show in Appendix A that quaternion algebras are precisely the central simple algebras over F of dimension 4.

Standard Involution. Let $B = \left(\frac{a,b}{F}\right)$ be a quaternion algebra. The F-subspace of *pure quaternions* is $B_0 = Fi \oplus Fj \oplus Fij$. This subspace can be characterized intrinsically as the set of elements $x \in B$ such that $x \notin F$ and $x^2 \in F$. For any element $s = t + \xi$ with $t \in F$ and $\xi \in B_0$, we define its *conjugate* as

$$\overline{s} := t - \xi.$$

The *reduced trace* trd and *reduced norm* nrd of $s = t + xi + yj + z(ij) \in B$ are:

$$\begin{aligned} \mathrm{trd}(s) &:= s + \overline{s} = 2t, \\ \mathrm{nrd}(s) &:= s\overline{s} = t^2 - ax^2 - by^2 + abz^2. \end{aligned}$$

The reduced trace coincides with the general definition for central simple algebras (see Appendix A). To see this, one can check that for $s \in B$, the matrix of the left-multiplication-by-s map, $L_s : B \to B$, in the basis $(1, i, j, ij)$ has trace $\mathrm{Tr}_{B/F}(L_s) = 4t$. Thus, we have the relation $\mathrm{Tr}_{B/F}(L_s) = 2\,\mathrm{trd}(s)$.

As is easily checked, the reduced trace $\mathrm{trd} : B \to F$ is F-linear, and its kernel is B_0. The reduced norm $\mathrm{nrd} : B \to F$ is multiplicative: $\mathrm{nrd}(1) = 1$ and $\mathrm{nrd}(xy) = \mathrm{nrd}(x)\,\mathrm{nrd}(y)$ for all $x, y \in B$.

Quadratic Forms. Quaternion algebras are closely related to quadratic forms. Since $\mathrm{char}(F) \neq 2$, a quadratic form Q on F^n can be defined by a homogeneous polynomial of degree 2, or equivalently by a symmetric matrix $S \in \mathrm{M}_n(F)$ such that $Q(X) = X^T S X$. Two quadratic forms Q_1, Q_2 (with matrices S_1, S_2) are *equivalent* if there exists an invertible matrix $M \in \mathrm{GL}_n(F)$ such that $Q_2(X) = Q_1(MX)$, i.e., $S_2 = M^T S_1 M$.

Theorem 2.1. *Let F be a field with $\mathrm{char}(F) \neq 2$ and let $a, b, \alpha, \beta \in F^\times$. Then*

$$\left(\frac{\alpha, \beta}{F}\right) \cong \left(\frac{a, b}{F}\right) \iff -aX^2 - bY^2 + abZ^2 \sim -\alpha X^2 - \beta Y^2 + \alpha\beta Z^2.$$

Moreover, the equivalence is explicit: from an explicit equivalence of the forms, one can deduce an explicit isomorphism of the algebras.

Proof. An algebra isomorphism $f : \left(\frac{a,b}{F}\right) \to \left(\frac{\alpha,\beta}{F}\right)$ must map pure quaternions to pure quaternions and preserve the reduced norm. This implies that the respective normic forms are equivalent. Conversely, given an equivalence of quadratic form $M \in \mathrm{GL}_3(\mathbb{Q})$ that is $M^T \mathrm{diag}(a, b, -ab) M = \mathrm{diag}(\alpha, \beta, -\alpha\beta)$. Then in B, $\mu := M_{1,1}i + M_{2,1}j + M_{3,1}ij$ and $\nu := M_{1,1}i + M_{2,1}j + M_{3,1}ij$ satisfy $\mu^2 = \alpha$ $\nu^2 = \beta$ and $\mu\nu = -\nu\mu$. Consequently the F-linear map $f : A \to B$ caraterize by $f(1) = 1, f(i) = \mu, f(j) = \nu$ and $f(ij) = \mu\nu$ is an isomorphism of F-algebra. □

3. Deciding the Isomorphism Problem over $\mathbb{Q}$

From now on, we work over the field $\mathbb{Q}$ of rational numbers. We first review the literature regarding the problem of deciding whether two quaternion algebras are isomorphic.

Problem `DecideIsoQuatAlg`(α, β, a, b) : Let $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. Determine if A and B are isomorphic as $\mathbb{Q}$-algebras.

Currently, the best-known method to solve this is based on the Hasse-Minkowski theorem.

Theorem 3.1 (Hasse-Minkowski for Quaternion Algebras)**.** *Let α, β, a, b be non-zero integers. Then*

$$\left(\frac{\alpha,\beta}{\mathbb{Q}}\right) \cong \left(\frac{a,b}{\mathbb{Q}}\right) \iff \left(\frac{\alpha,\beta}{\mathbb{Q}_p}\right) \cong \left(\frac{a,b}{\mathbb{Q}_p}\right) \text{ for all primes } p.$$

Proof. See Voight [Voi21], Theorem 14.1.3. □

For any p-adic field $\mathbb{Q}_p$, there are, up to isomorphism, only two quaternion algebras: the matrix algebra $\mathrm{M}_2(\mathbb{Q}_p)$ and a unique division algebra (see [Voi21, Theorem 2.1.5]). We distinguish these using the *Hilbert symbol*.

$$(a,b)_p = \begin{cases} 1 & \text{if } \left(\frac{a,b}{\mathbb{Q}_p}\right) \cong \mathrm{M}_2(\mathbb{Q}_p) \\ -1 & \text{if } \left(\frac{a,b}{\mathbb{Q}_p}\right) \text{ is a division algebra.} \end{cases}$$

A prime p is a *ramified prime* of $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ if $(a,b)_p = -1$. The set of ramified primes is denoted $\mathrm{Ram}(B)$. An important fact is that: $p \nmid 2ab \implies (a,b)_p = 1$. In other words, $\mathrm{Ram}(B)$ is a finite subset of $\{p \mid p \text{ divides } 2ab\}$. Given two quaternion algebras A, B over $\mathbb{Q}$, the isomorphism condition $A \cong B$ is equivalent to $\mathrm{Ram}(A) = \mathrm{Ram}(B)$. We can then study this other problem, given two integers a, b:

Problem `RamifiedPrimes`(a, b) : Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. Compute the set of ramified primes $\mathrm{Ram}(B)$.

We also denote the integer factorization problem for an integer N:

Problem `Factor`(N) : Factor the integer N.

The `RamifiedPrimes` problem and the `Factor` problem are of the same difficulty in the following sense. Recall that for an integer, its size is its number of bits, and the size of a tuple of integers is the maximum of the sizes of the elements.

Assumption A. For any integer $N > 1$ that is not a perfect square, the smallest odd prime p such that the Legendre symbol $\left(\frac{N}{p}\right) = -1$ is bounded by $3\log(4N)^2$.

Remark 3.2. This assumption holds under the Generalized Riemann Hypothesis. It is an application of a theorem by Bach [Bac90, Theorem 5]. We set $m = 4N$ and define a subgroup $G = \{a \in (\mathbb{Z}/m\mathbb{Z})^\times \mid (\frac{N}{a}) = 1\}$, where $(\frac{N}{a})$ is the Kronecker symbol.

The map $\chi(a) = (\frac{N}{a})$ is a well-defined character on $(\mathbb{Z}/m\mathbb{Z})^\times$ due to the law of quadratic reciprocity. Since N is not a square, χ is non-trivial, making G a proper subgroup.

Bach's theorem [Bac90, Theorem 5] states that the smallest integer x coprime to m with $\chi(x) = -1$ satisfies $x < 3\log(m)^2$. By the multiplicative property of the symbol, any such x must have a prime factor p for which $(\frac{N}{p}) = -1$. The minimality of x then requires that x itself must be this prime.

Theorem 3.3 (Equivalence of Factor and RamifiedPrimes)**.** *Under Assumption A, the problems* ***RamifiedPrimes*** *and* ***Factor*** *are polynomial-time equivalent. Specifically:*

1. *Given an oracle for* ***Factor****(N) for all N with* $\text{size}(N) \le t$*, for* $\text{size}(a, b) \le t$*, the problem* ***RamifiedPrimes****(a,b) can be solved in time polynomial in* $\text{size}(a, b)$*.*
2. *Assuming Assumption A, given an oracle for* ***RamifiedPrimes****(a,b) for all a, b with* $\text{size}(a, b) \le t$*, for* $\text{size}(N) \le t$*, the problem* ***Factor****(N) can be solved in time polynomial in* $\text{size}(N)$*.*

Proof. `Factor` $\implies$ `RamifiedPrimes`: Assume an oracle for `Factor` is given for inputs of size at most t. Let a, b be given of size at most t. We first use the `Factor` oracle to find the prime factorization of $2ab$. For each such prime p, we compute the Hilbert symbol $(a, b)_p$ using the explicit computation from [Voi21, Section 12.4.8].

If $p \neq 2$, let $a = p^r u$ and $b = p^s v$, where u and v are not divisible by p. The symbol is given by the formula [Voi21, Formula 12.4.10] :

$$(a, b)_p = (-1)^{rs\frac{p-1}{2}} \left(\frac{u}{p}\right)^s \left(\frac{v}{p}\right)^r .4 \tag{2}$$

The p-adic valuations r, s and the cofactors u, v can be computed in polynomial time in t. The Legendre symbols $\left(\frac{u}{p}\right)$ can also be computed in polynomial time in $\text{size}(u, p)$ and thus in t.

If $p = 2$, there is a precise description [Voi21, Section 12.4.13] which yields a computation in polynomial time in the size of a, b. For example, when a, b are odd:

$$(a, b)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}. \tag{3}$$

Since the number of primes to check is less than $\text{size}(a) + \text{size}(b)$ and each check takes polynomial time, the entire algorithm runs in polynomial time in the size of a, b.

`RamifiedPrimes` $\implies$ `Factor`: Assume we have an oracle for `RamifiedPrimes` on inputs of size less than t. Let $N > 0$ be the integer to factor; we can assume N is odd and not a perfect square. The strategy is to construct a quaternion algebra of the form $B = \left(\frac{a,N}{\mathbb{Q}}\right)$ for a suitably chosen integer a.

First, we seek an odd prime p such that N is a quadratic non-residue modulo p, i.e., $\left(\frac{N}{p}\right) = -1$. By Assumption A, such a prime can be found deterministically in polynomial time in $\text{size}(N)$ by checking primes sequentially, and with $\text{size}(p) \leq \text{size}(N) \leq t$. Let $p^* = (-1)^{(p-1)/2}p$. Note that $p^* \equiv 1 \pmod 4$. We consider the algebra $B = \left(\frac{p^*,N}{\mathbb{Q}}\right)$, which satisfies the following:

- B is unramified at ∞ since not both p^* and N are negative.
- B is ramified at p because using formula (2), $(p^*, N)_p = \left(\frac{N}{p}\right) = -1$.
- B is unramified at 2 because p^* and N are odd, so by formula (3), $(p^*, N)_2 = 1$ since $p^* \equiv 1 \pmod 4$.

By Hilbert reciprocity [Voi21, Corollary 14.2.3] (in Voight's book $\text{Ram}(B)$ inlcude the place ∞), since B is not ramified at ∞ the number of ramified primes must of B must be even. Since B ramifies at p but not at 2, it must ramify at another finite prime $q \neq p$. The finite ramified primes of B must divide $2p^*N$, so this prime q must be a factor of N. Calling the oracle on (p^*, N) thus reveals a non-trivial factor of N. □

In particular during the first part of the proof we have shown in particular:

Theorem 3.4. *Let α, β, a, b be non-zero integers. Assuming their factorizations are known, we can compute their ramified primes in polynomial time in* $\text{size}(\alpha, \beta, a, b)$ *and hence we can decide if $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ are isomorphic in polynomial time in* $\text{size}(\alpha, \beta, a, b)$.

However, as far as I know, it is still an open question whether `DecideIsoQuatAlg` is equivalent to `Factor` in the same sense as `RamifiedPrimes`. That is, it is an open question whether `DecideIsoQuatAlg` is equivalent to `RamifiedPrimes`.

4. Orders in Quaternion Algebras

Let us fix a quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ over $\mathbb{Q}$.

A *lattice* L in B is a free sub-$\mathbb{Z}$-module of rank 4 of the form

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4,$$

where $\{e_1, e_2, e_3, e_4\}$ is a $\mathbb{Q}$-basis of B.

An *order* $\mathcal{O}$ in B is a lattice that is also a subring.

For a $\mathbb{Q}$-basis $\{e_1, e_2, e_3, e_4\}$ of B, we denote

$$T(e_1, e_2, e_3, e_4) = (\mathrm{trd}(e_i e_j))_{1 \le i,j \le 4}.$$

This is an invertible matrix in $\mathrm{GL}_4(\mathbb{Q})$ because the reduced trace form is non-degenerate.

If $\{e_i\}$ and $\{f_i\}$ are two $\mathbb{Q}$-bases of B, let M be the change of basis matrix such that $f_i = \sum_k M_{ki} e_k$ for all i. Then

$$T(f_1, f_2, f_3, f_4) = M^T T(e_1, e_2, e_3, e_4) M.$$

Definition 4.1. Let $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4$ be a lattice in B. The *discriminant* of L is

$$\mathrm{disc}(L) := |\det(T(e_1, e_2, e_3, e_4))| \in \mathbb{Q}_{>0},$$

which does not depend on the choice of the $\mathbb{Z}$-basis.

Proof. The change of basis matrix between any two $\mathbb{Z}$-bases of L is in $\mathrm{GL}_4(\mathbb{Z})$ and has determinant ± 1. □

Proposition 4.2. *Let $J \subset I$ be two lattices in B. The index of J in I, denoted $[I : J]$, as abelian groups is finite. If M is the matrix of a $\mathbb{Z}$-basis of J expressed in a $\mathbb{Z}$-basis of I, then*

$$[I : J] = |\det(M)|.$$

Proof. By choosing a basis for I, we can identify I with $\mathbb{Z}^4$ and J with $M\mathbb{Z}^4$. Note that $M \in M_4(\mathbb{Z}) \cap \mathrm{GL}_4(\mathbb{Q})$. We need to show that $|\mathbb{Z}^4/M\mathbb{Z}^4| = |\det(M)|$.

Let $f : M_4(\mathbb{Z}) \cap \mathrm{GL}_4(\mathbb{Q}) \to \mathbb{N}_{>0} \cup \{\infty\}, M \mapsto |\mathbb{Z}^4/M\mathbb{Z}^4|$. We claim that f is multiplicative. This follows from the isomorphism for all $M, N \in M_4(\mathbb{Z})$ with non-zero determinant:

$$(\mathbb{Z}^4/MN\mathbb{Z}^4)/(N\mathbb{Z}^4/MN\mathbb{Z}^4) \cong \mathbb{Z}^4/N\mathbb{Z}^4$$

Since N is invertible in $M_4(\mathbb{Q})$, we have $N\mathbb{Z}^4 \cong \mathbb{Z}^4$. Hence, $\frac{f(MN)}{f(M)} = f(N)$.

For a unimodular matrix U (i.e., $U \in M_4(\mathbb{Z})$ with $\det(U) = \pm 1$), the result is clear since $U\mathbb{Z}^4 = \mathbb{Z}^4$, so $|\mathbb{Z}^4/U\mathbb{Z}^4| = |\det(U)| = 1$. For a diagonal matrix $D = \mathrm{diag}(d_1, d_2, d_3, d_4)$ where $d_i \in \mathbb{Z}$, the result holds because

$$\mathbb{Z}^4/D\mathbb{Z}^4 \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}/d_3\mathbb{Z} \times \mathbb{Z}/d_4\mathbb{Z}.$$

The size of this quotient is $|\det(D)| = |d_1 d_2 d_3 d_4|$. Finally, it suffices to show that any matrix $M \in M_4(\mathbb{Z}) \cap \mathrm{GL}_4(\mathbb{Q})$ can be decomposed into a product of unimodular and diagonal matrices. This comes from the Smith Normal Form, where every such matrix M can be written as a product $M = UDV$ with U, V unimodular and D a diagonal matrix. By the multiplicativity of f and the fact that $|\det|$ is also multiplicative, the result holds for every matrix $M \in M_4(\mathbb{Z}) \cap \mathrm{GL}_4(\mathbb{Q})$. □

Proposition 4.3. *If $J \subset I$ are two lattices in B, then*

$$\mathrm{disc}(J) = [I : J]^2 \mathrm{disc}(I).$$

Proof. This is an immediate consequence of the previous definitions and discussion. □

Proposition 4.4. *Every element of an order $\mathcal{O}$ is integral over $\mathbb{Z}$. Hence, the reduced trace takes integral values on $\mathcal{O}$, and thus*

$$\mathrm{disc}(\mathcal{O}) \in \mathbb{Z}_{>0}.$$

Proof. Let $x \in \mathcal{O}$, the left-multiplication by x is a $\mathbb{Z}$-linear endomorphism of $\mathcal{O}$, $m_x : \mathcal{O} \to \mathcal{O}$. By choosing a $\mathbb{Z}$ basis of $\mathcal{O}$ the matrix of m_x has integral coefficient. Hence its caracteristic polynomial χ is monic and has integral coefficient and $\chi(m_x) = 0$ i.e. $\chi(x) = 0$. So x is integral. Then apply general properties of the reduced trace form from Appendix A. □

It follows from Proposition 4.3 applied to orders that if $\mathcal{O}_1 \subset \mathcal{O}_2$ are two orders, then $\mathrm{disc}(\mathcal{O}_2)$ divides $\mathrm{disc}(\mathcal{O}_1)$ in $\mathbb{Z}$. The equality $\mathrm{disc}(\mathcal{O}_1) = \mathrm{disc}(\mathcal{O}_2)$ holds if and only if $\mathcal{O}_1 = \mathcal{O}_2$.

An order is *maximal* if it is maximal for inclusion among the orders of B.

Theorem 4.5 (Discriminant of Maximal Orders In Quaternion Algebra)**.** *Let B a quaternion algebra. An order $\mathcal{O}$ in B is maximal if and only if*

$$\mathrm{disc}(\mathcal{O}) = \left(\prod_{p \text{ ramified in } B} p \right)^2.$$

Proof. See [Voi21, Theorem 15.5.5] for a complete proof. □

Since the isomorphism class of B is determined by its discriminant, the knowledge of a maximal order in B characterizes the isomorphism class of B via its own discriminant. In particular:

Proposition 4.6. *Given two quaternion algebras A and B with maximal orders $\mathcal{O}_A$ and $\mathcal{O}_B$ provided by some bases, the problem* `DecideIsoQuatAlg` *becomes immediate (solvable in polynomial time in the size of the coefficients of the bases of $\mathcal{O}_A$ and $\mathcal{O}_B$).*

Proof. One just needs to compute $\mathrm{disc}(\mathcal{O}_A)$ and $\mathrm{disc}(\mathcal{O}_B)$ and check for equality. □

5. Computing Isomorphisms of Split Quaternion Algebras

We dedicate this section to computing an isomorphism between two split quaternion algebras. Let $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be two *split* quaternion algebras, i.e., $A \cong B \cong \mathrm{M}_2(\mathbb{Q})$. It suffices to compute an isomorphism $B \to \mathrm{M}_2(\mathbb{Q})$.

Proposition 5.1. *Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a split quaternion algebra. Given a non-zero solution to $-aX^2 - bY^2 + abZ^2 = 0$, we can compute an equivalence of quadratic forms $-aX^2 - bY^2 + abZ^2 \sim -X^2 - Y^2 + Z^2$ in polynomial time and hence an isomorphism $B \to \left(\frac{1,1}{\mathbb{Q}}\right)$ in polynomial time in* $\mathrm{size}(a, b)$.

Proof. See [Voi12, Algorithm 4.3] for a proof with algebra. We give a proof based on quadratic reduction.

Denote by $S = \mathrm{diag}(-a, -b, ab)$ and $q(x) = x^T S x$ the associated symmetric matrix and quadratic form. Assume we are given $u \in \mathbb{Q}^3$ non-zero such that $q(u) = u^T S u = 0$. Since S is invertible, $u^T S \neq 0$ and we can compute $v \in \mathbb{Q}^3$ such that $u^T S v \neq 0$; by rescaling we can assume $u^T S v = 1$. Let $e_2 = v - q(v)u/2$. So that $u^T S e_2 = 1$ and $q(e_2) = 0$. Then $e_1 = u$ and e_2 are linearly independent. Let $N = (e_1|e_2)$ be the 3×2 matrix. Then $N^T S$ has a kernel of rank 1. Let $w \neq 0 \in \mathbb{Q}^3$ such that $N^T S w = 0$. Then $M' = (e_1|e_2|w)$ is invertible and satisfies

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

where $\alpha = q(w)$. Since the discriminant is a square, $-\alpha$ is a square, say $-\alpha = r^2$. Taking $e_3 = \frac{1}{r} w$ and letting $M = (e_1|e_2|e_3)$, M is a 3×3 invertible rational matrix and

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

Finally, we can easily deduce an equivalence with

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The correspondence with isomorphisms of quaternion algebras comes from Theorem 2.1. □

Theorem 5.2 (Denis Simon, 2005)**.** *Let a, b, c be non-zero integers. Assuming their factorization is known, there is an algorithm to find an isotropic rational vector for $aX^2 + bY^2 + cZ^2 = 0$ which runs in polynomial time in* size(a, b, c).

Proof. See [Sim05b], combining Theorems 1.3, 2.1 and Algorithm 3.1. □

Proposition 5.3. *Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a split quaternion algebra. Assuming the factorizations of a, b are known, we can compute an isomorphism between B and $\mathrm{M}_2(\mathbb{Q})$ in polynomial time in* size(a, b).

Proof. This follows immediately from Simon's Theorem 5.2 applied to $-aX^2 - bY^2 + abZ^2 = 0$ and Proposition 5.1. □

Remark 5.4. Simon's algorithm of Theorem 5.2 is designed only for use over $\mathbb{Q}$. If we work over a number field K rather than $\mathbb{Q}$, we have to work as follows. Let a, b, c be non-zero elements in K. We seek a non-zero solution to $aX^2 + bY^2 + cZ^2 = 0$ with unknowns $X, Y, Z \in K$. Multiplying by a, rescaling X, and changing the sign and notation, this is equivalent to finding a non-zero solution to $X^2 - dY^2 = eZ^2$. So far we have two cases. If d is a square in K, let's write $d = r^2$ with $r \in K$ (this is easy to do computationally). Then we get $(X - rY)(X + rY) = eZ^2$, which can be solved by the linear system $X - rY = 1$ and $X + rY = e$. If d is not a square in K, we can consider the quadratic extension $K(\sqrt{d})$. Since any non-trivial solution must satisfy $Z \neq 0$, the equation $x^2 - dy^2 = e$ has a solution in K. This last equation can also be written as $\mathcal{N}_{K(\sqrt{d})/K}(x + y\sqrt{d}) = e$, where $\mathcal{N}_{K(\sqrt{d})/K}$ is the norm of $K(\sqrt{d})$ over K. This last kind of equation is called a *(quadratic) norm equation* over number fields. Algorithms for solving norm equations have been known since another article by Denis Simon [Sim02]. However, those algorithms are expensive in time, and the complexity is hard to determine precisely. Even though these algorithms are implemented in Magma and PARI/GP and work pretty fast for small-degree number fields, over $\mathbb{Q}$ it is preferable to use the special rational algorithm of Denis Simon [Sim05b].

5.1. Using Maximal Orders. As mentioned in Proposition 4.6, maximal orders can help solve the decision problem. They can also help in the constructive problem.

Theorem 5.5. *Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a split algebra. Given a maximal order $\mathcal{O} \subset B$ by a basis, there is an algorithm to compute an isomorphism $B \to \mathrm{M}_2(\mathbb{Q})$ that runs in polynomial time in the size of the parameters a, b and the size of the basis coefficients of $\mathcal{O}$ (max of the size of the coefficients of the basis vectors in terms of $1, i, j, ij$).*

Proof. This was shown by Ivanyos in [IS96, Theorem 3] (the size of structure constant in basis $1, i, j, ij$ are polynomial in the size of paramters a, b). We present another idea. Let $S = \mathrm{diag}(2a, 2b, -2ab)$. We have to find an isotropic vector for S. For that, we make use of the maximal order to first reduce S with an equivalence. Write $\mathcal{O} = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4$. Then $\mathrm{trd} : \mathcal{O} \to \mathbb{Z}$ is a non-zero $\mathbb{Z}$-linear map. Its kernel $\mathcal{O}_0$ has rank 3 as a $\mathbb{Z}$-module: $\mathcal{O}_0 = \mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \oplus \mathbb{Z}f_3$. Hence $\{f_1, f_2, f_3\}$ is another $\mathbb{Q}$-basis of B_0. Let M be the matrix of $\{f_1, f_2, f_3\}$ in the basis $\{i, j, ij\}$. We have

$$M^T S M = (\mathrm{trd}(f_i f_j))_{1 \leq i,j \leq 3}.$$

We borrow a lemma from the future 8.7 that the determinant of this matrix is

$$\det((\mathrm{trd}(f_i f_j))_{1 \leq i,j \leq 3}) = -2 \left(\prod_{p \text{ ramified in } B} p \right)^2 = -2.$$

Then we can apply the algorithm of Denis Simon to find an isotropic vector for $M^T S M$. This runs in polynomial time since we know the factorization of its determinant. Then we deduce an isotropic vector for S and thus an isomorphism as wanted. Overall, the algorithm is polynomial time in the size of the inputs. □

6. Method 1: Isomorphism via Solving Quadratic Forms

In this section, we present what is perhaps the most natural approach to explicitly compute an isomorphism between two quaternion algebras $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, where a, b, α, β are integers. We assume A, B are non-split.

To seek an isomorphism $f : A \to B$, the image of i_A must be a pure quaternion $\mu \in B_0$ such that $\mu^2 = \alpha$. Then we claim:

Lemma 6.1. *There exists a pure quaternion $\nu \in B_0$ such that $\mu\nu = -\nu\mu$ and $\nu^2 = \beta$.*

Proof. Using the Skolem-Noether theorem: Since A and B are isomorphic central simple algebras, by a version of the Skolem-Noether theorem [Voi21, Corollary 7.7.3], and since μ and $f(i_A)$ have the same minimal polynomial $X^2 - \alpha$, they are conjugate. Let i_B, j_B be the standard generators of B. The map $g : \mathbb{Q}(i_A) \to B$ given by $g(i_A) = \mu$ is an algebra homomorphism. Since $A \cong B$, there exists an isomorphism $f : A \to B$. Then f extends g up to conjugation. That is, there is an invertible $u \in B$ such that $f(x) = ug(x)u^{-1}$ for all $x \in \mathbb{Q}(i_A)$. Then $\nu = f(j_A)$ works. □

Thanks to this lemma, the following method is guaranteed to succeed.

Find μ such that $\mu^2 = \alpha$. First, we want to find a pure quaternion $\mu \in B_0$ such that $\mu^2 = \alpha$.

Writing $\mu = Xi_B + Yj_B + Z(i_Bj_B)$, we must solve the quadratic equation over $\mathbb{Q}$: $aX^2+bY^2-abZ^2 = -\alpha$. As the quadratic form on the left is anisotropic (since B is non-split), this is equivalent to finding a non-trivial solution to $aX^2+bY^2-abZ^2+\alpha W^2 = 0$. For this, one can use the algorithm from [Sim05a]. This requires factoring the integer $ab\alpha$, but apart from this, the algorithm appears to be polynomial in the number of digits of a, b, α.

Adapting the final basis. Next, we find a pure quaternion $\nu \in B_0$ that is orthogonal to μ with respect to the trace pairing (which is equivalent to $\mu\nu = -\nu\mu$). This amounts to solving a system of linear equations for the coefficients of ν. Let its square be $\nu^2 = \gamma$.

So far, we have a basis $\{1, \mu, \nu, \mu\nu\}$ for B with $\mu^2 = \alpha$ and $\nu^2 = \gamma$. Since $A \cong B$, the element β/γ must be a norm from the extension $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$. We can therefore find $x, y \in \mathbb{Q}$ by solving the norm equation $x^2 - \alpha y^2 = \beta/\gamma$. This is equivalent to finding an isotropic vector for the quadratic form $X^2 - \alpha Y^2 - (\beta/\gamma)Z^2 = 0$. For this, we

use the algorithm from [Sim05b], specialized for dimension 3 over $\mathbb{Q}$. Any non-trivial solution will have $Z \neq 0$, so we can scale it to get a solution with $Z = 1$.

Finally, we define $\nu' = (x + y\mu)\nu$. This new element ν' still anticommutes with μ, and its square is $(\nu')^2 = (x + y\mu)\nu(x + y\mu)\nu = (x + y\mu)(x - y\mu)\nu^2 = (x^2 - \alpha y^2)\gamma = (\beta/\gamma)\gamma = \beta$. The isomorphism $f : A \to B$ is then given by $f(i_A) = \mu$ and $f(j_A) = \nu'$.

Conclusion. Overall, to compute the isomorphism $f : A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right) \to B = \left(\frac{a,b}{\mathbb{Q}}\right)$, we have to solve:

1. $aX^2 + bY^2 - abZ^2 + \alpha W^2 = 0$ over $\mathbb{Q}$.
2. $X^2 - \alpha Y^2 - (\beta/\gamma)Z^2 = 0$ over $\mathbb{Q}$.

It seems preferable to solve equations entirely over $\mathbb{Q}$ using the two algorithms of D. Simon, [Sim05b] and [Sim05a]. We can easily work with forms with integer coefficients. In these algorithms, the most computationally expensive step is factoring the determinant of the form. Thus, we only need to be able to factor the integers a, b, α, β, and the numerator and denominator of γ.

Remark 6.2 (Generalization over a number field)**.** Over a number field K, the only known algorithm can solve quadratic equations of dimension 3 and not 4. This is based on solving norm equations ([Sim02]). Hence we have to reduce to only equations of the form

$$aX^2 + bY^2 + cZ^2 = 0. \qquad (X, Y, Z \in K)$$

The computer algebra system Magma has implemented this method (even over $\mathbb{Q}$, which is not optimal).

Let $L = K(\sqrt{\alpha})$. Since $A \cong B$, their extensions of scalars A_L and B_L are also isomorphic. The algebra A_L is split, so $B_L = \left(\frac{a,b}{L}\right)$ must also be split. This implies we can find an isotropic vector for the quadratic form of dimension 3 over L: $U^2 - aV^2 - bW^2 = 0$, with $U, V, W \in L$. We can be sure that $W \neq 0$; otherwise, a would be a square in L.

Scaling the solution allows us to assume $W = 1$, so we find $U, V \in L$ such that $U^2 - aV^2 = b$. This means the element $\zeta = U + Vi_B + j_B \in B_L$ has reduced norm $\mathrm{nrd}(\zeta) = U^2 - aV^2 - b = 0$. Now, write $U = u_1 + u_2\sqrt{\alpha}$ and $V = v_1 + v_2\sqrt{\alpha}$ for $u_i, v_i \in K$. We can express ζ as $\zeta_1 + \zeta_2\sqrt{\alpha}$, where $\zeta_1 = u_1 + v_1 i_B + j_B$ and $\zeta_2 = u_2 + v_2 i_B$ are elements of B. The element ζ_2 must be invertible; otherwise, we would have $U, V \in K$, which implies B is split over K, a contradiction. The condition $\mathrm{nrd}(\zeta) = 0$ implies $\mathrm{nrd}(\zeta_1\zeta_2^{-1} + \sqrt{\alpha}) = 0$. Let $\mu = \zeta_1\zeta_2^{-1}$. One can check from $U^2 - aV^2 = b$ that μ is a pure quaternion, and the norm condition becomes $\mathrm{nrd}(\mu) + \alpha = 0$, which simplifies to $-\mu^2 + \alpha = 0$. Thus, $\mu^2 = \alpha$, as desired.

Overall, this method solves $U^2 - aV^2 - bW^2 = 0$ over $L = K(\sqrt{\alpha})$. The algorithm for this first reduces the form and then solves a norm equation over a quadratic extension of L as presented in Remark 5.4, using the algorithm from [Sim02].

7. Method 2: Isomorphism via Splitting Matrix Algebras

In this section, we present a conceptual approach to explicitly computing an isomorphism between two quaternion algebras, $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. As presented in [Csa+22, Proposition 4.1], this method can make use of the knowledge of maximal orders in A and B.

Proposition 7.1. *Let A and B be two quaternion algebras over $\mathbb{Q}$. Then*

$$A \cong B \iff A \otimes_{\mathbb{Q}} B^{\mathrm{op}} \cong \mathrm{M}_4(\mathbb{Q}).$$

Moreover, this equivalence is explicit: given an isomorphism $\Phi : A \otimes_{\mathbb{Q}} B^{\mathrm{op}} \to \mathrm{M}_4(\mathbb{Q})$, we can deduce an isomorphism $f : A \to B$ in polynomial time.

Proof. The theoretical claim is shown in Appendix A and the computational claim is in Appendix **??**. □

To consider $C := A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$ computationally and frame the problem in a standard form, we introduce the notion of an algebra given by *structure constants*.

Definition 7.2. An algebra C over $\mathbb{Q}$ is given by **structure constants** if it is defined by a basis $\{e_1, \ldots, e_N\}$ and rational numbers c_{ijk} for $i, j, k \in \{1, \ldots, N\}$ such that, for all i, j, the product is given by

$$e_i e_j = \sum_{k=1}^{N} c_{ijk} e_k.$$

Given the quaternion algebras $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, we can easily compute the structure constants for $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$. We use the basis $\{e_1, \ldots, e_{16}\}$ formed by the tensor product of the standard bases $\{1_A, i_A, j_A, k_A\}$ of A and $\{1_B, i_B, j_B, k_B\}$ of B^{op}. The structure constants c_{ijk} of C in this basis are expressed in terms of α, β, a, b, and many of them are zero.

This leads us to the following general problem:

Problem `SplittingMatrixAlgebraDegree4`(c_{ijk}) : Let C be an algebra over $\mathbb{Q}$ given by structure constants c_{ijk}, and assume $C \cong \mathrm{M}_4(\mathbb{Q})$. Compute an explicit isomorphism $\varphi : C \to \mathrm{M}_4(\mathbb{Q})$. That is, output 16 matrices in $\mathrm{M}_4(\mathbb{Q})$ representing the images of the basis elements of C under φ.

This problem, which can be generalized to any dimension, is also referred to as the "splitting matrix algebra problem" or the "explicit isomorphism problem". It is well-studied in the literature, and the remainder of this report is dedicated to it.

7.1. Splitting Matrix Algebras. The central problem can be stated as follows:

Problem `SplittingMatrixAlgebra`(c_{ijk}) : Let C be an algebra over $\mathbb{Q}$ given by structure constants c_{ijk}, and assume $C \cong \mathrm{M}_n(\mathbb{Q})$ for some $n > 0$. Compute an explicit isomorphism $\varphi : C \to \mathrm{M}_n(\mathbb{Q})$. That is, output n^2 matrices in $\mathrm{M}_n(\mathbb{Q})$ representing the images of the basis elements of C under φ.

This problem can be reduced to finding a special kind of element in the algebra.

One can define the *rank* of an element $x \in A$ as follows. For every isomorphism $\varphi : A \to \mathrm{M}_n(\mathbb{Q})$, we have

$$n \cdot \mathrm{rank}(\varphi(x)) = \dim_{\mathbb{Q}}(\mathrm{M}_n(\mathbb{Q})\varphi(x)) = \dim_{\mathbb{Q}}(\varphi(Ax)) = \dim_{\mathbb{Q}}(Ax).$$

Hence we define the *rank* of an element $x \in A$ by

$$\mathrm{rank}_A(x) := \frac{1}{n}\dim_{\mathbb{Q}}(Ax) = \mathrm{rank}(\varphi(x)) \quad \text{(for any isomorphism } \varphi : A \to \mathrm{M}_n(\mathbb{Q})).$$

Problem `RankOneMatrixAlgebra`(c_{ijk}) : Let C be an algebra over $\mathbb{Q}$ given by structure constants c_{ijk}, and assume $C \cong \mathrm{M}_n(\mathbb{Q})$ for some $n > 0$. Compute a rank-one element in C.

Lemma 7.3. *Problems `SplittingMatrixAlgebra` and `RankOneMatrixAlgebra` are polynomial-time equivalent in the size of the structure constants.*

Proof. Let $C \cong \mathrm{M}_n(\mathbb{Q})$ be given by structure constants. Given an isomorphism $C \to \mathrm{M}_n(\mathbb{Q})$, we can compute a rank-one element immediately. Given a rank-one element $x \in C$. The map $\Phi : C \to \mathrm{End}_{\mathbb{Q}}(Cx); c \mapsto [z \mapsto cz]$ is $\mathbb{Q}$-linear and a ring homomorphism. Since C is a simple ring and Φ is non-zero, Φ is injective, and hence bijective by a dimension argument. Then, by computing a $\mathbb{Q}$-basis of Cx, we deduce an isomorphism $C \to \mathrm{M}_n(\mathbb{Q})$. □

Currently, the best-known algorithm to solve Problem `RankOneMatrixAlgebra` and therefore `SplittingMatrixAlgebra` is the following. This requires the definition of a *maximal order*, which we define in the next subsection.

Theorem 7.4 (Ivanyos, Rónyai, & Schicho, 2018)**.** *Let $\Lambda = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_{16} \cong \mathrm{M}_4(\mathbb{Z})$ be a maximal order in $C \cong \mathrm{M}_4(\mathbb{Q})$. There is a polynomial-time algorithm to compute a rank-one element in Λ.*

Proof. [IRS12], Theorem 1. □

7.2. Orders in a Matrix Ring. Let C be a $\mathbb{Q}$-algebra such that $C \cong \mathrm{M}_n(\mathbb{Q})$. Denote $N = n^2$.

An $\mathbb{Z}$-*order* in C is a subring $\Lambda \subset C$ such that:

- Λ is a full $\mathbb{Z}$-lattice in C; that is, there exists a $\mathbb{Q}$-basis $e_1, \ldots, e_N$ of C such that $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$.
- Λ is a subring of C; in particular, $1 \in \Lambda$.

An order is *maximal* if it is maximal regarding inclusion among orders.

Lemma 7.5. *If Λ is a $\mathbb{Z}$-order in C, then for all $\alpha \in \Lambda$, α is integral over $\mathbb{Z}$; hence* $\mathrm{trd}(\alpha) \in \mathbb{Z}$.

Proof. Same as 4.4. □

The notion of the *discriminant* of an order is intended to measure inclusion relations between orders.

Definition 7.6. Let $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$ be an order in C. The *discriminant* of Λ is:

$$\mathrm{disc}(\Lambda) := |\det((\mathrm{trd}(e_i e_j))_{i,j})| \in \mathbb{Z}_{>0}.$$

Recall that trd on C is defined for a central simple algebra in Appendix A. For the same reason as for orders in quaternion algebras, this does not depend on the choice of the basis of Λ. And is an integer by Lemma 7.5.

Proposition 7.7. *The discriminant is strictly decreasing regarding inclusion and divisibility on $\mathbb{Z}_{>0}$. That is, for all orders Λ, Γ in C:*

$$\begin{aligned} \Lambda \subset \Gamma \quad &\implies \quad \mathrm{disc}(\Gamma) \mid \mathrm{disc}(\Lambda) \\ \Lambda = \Gamma \quad &\iff \Lambda \subset \Gamma \quad \textit{and} \quad \mathrm{disc}(\Lambda) = \mathrm{disc}(\Gamma) \end{aligned}$$

An important consequence is the following: if

$$\Lambda_1 \subset \Lambda_2 \subset \cdots \subset \Lambda_r$$

is a chain of strictly increasing orders, then the corresponding sequence of discriminants

$$d_r \mid d_{r-1} \mid \cdots \mid d_1$$

is a strictly decreasing sequence (with respect to divisibility) of elements in $\mathbb{Z}$. In particular, if

$$d_1 = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$$

is the factorization of d_1 into primes, then $r \leq \alpha_1 + \cdots + \alpha_s$.

This shows that there exists a maximal order containing Λ_1, since $\mathbb{Z}$ cannot have an infinite strictly descending chain with respect to divisibility.

We have seen in Theorem 4.5 that in quaternion algebras, maximal orders are characterized by their discriminant. For orders in a matrix ring, the characterization is easier.

Theorem 7.8. *Recall $C \cong \mathrm{M}_n(\mathbb{Q})$. In this case, an order is maximal if and only if its discriminant is* 1.

Proof. See [Voi21], 10.5.5 and exercise 10.6. □

Computing Maximal Orders

Theorem 7.9 (Ivanyos & Rónyai, 1993)**.** *Given a non-maximal order $\Lambda \subset C$ and a prime p dividing* $\mathrm{disc}(\Lambda)$*, one can compute in polynomial time a strictly larger order $\Gamma \supset \Lambda$.*

Proof. See [IR93, Theorem 5.1]. □

Starting with an initial order Λ_0 and the **prime factorization** of $\mathrm{disc}(\Lambda_0)$, we can compute a strictly increasing sequence of orders:

$$\Lambda_0 \subsetneq \Lambda_1 \subsetneq \cdots \subsetneq \Lambda_r.$$

$$\mathrm{disc}(\Lambda_r) \mid \cdots \mid \mathrm{disc}(\Lambda_1) \mid \mathrm{disc}(\Lambda_0)$$

This process terminates at a maximal order $\Gamma = \Lambda_r$ in polynomial time.

7.3. Use of Maximal Orders in Each Quaternion Algebra. We explain here how the knowledge of maximal orders $\mathcal{O}_A \subset A$ and $\mathcal{O}_B \subset B$ in two quaternion algebras A and B can be used to find a rank-one element and thus an explicit isomorphism between A and B.

In the algorithm of Ivanyos and Rónyai, we take as a starting order Λ_0 in $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$:

$$\Lambda_0 := \mathcal{O}_A \otimes_{\mathbb{Z}} \mathcal{O}_B^{\mathrm{op}}.$$

To be concrete, write $\mathcal{O}_A = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4$ and $\mathcal{O}_B = \mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \oplus \mathbb{Z}f_3 \oplus \mathbb{Z}f_4$. Then

$$\Lambda_0 = \bigoplus_{i,j=1}^{4} \mathbb{Z}(e_i \otimes f_j).$$

It is easily checked that Λ_0 is an order in $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$. This order has a discriminant related to the discriminants of the orders in A and B as follows.

Lemma 7.10. *We have* $\mathrm{disc}(\Lambda_0) = (\mathrm{disc}(\mathcal{O}_A)\,\mathrm{disc}(\mathcal{O}_B))^4$.

Proof. Let us denote $C = A \otimes_{\mathbb{Q}} B^{\mathrm{op}}$. We use the characterization of the reduced trace in terms of the global trace. Let trd denote the reduced trace and Tr the global trace.

Let $M = (\mathrm{trd}_A(e_i e_j))_{1 \le i,j \le 4}$ and $N = (\mathrm{trd}_B(f_i f_j))_{1 \le i,j \le 4}$ be the 4×4 trace matrices with integer entries. Let $T = (\mathrm{trd}_C((e_i \otimes f_s)(e_j \otimes f_r)))_{1 \le i,j,s,r \le 4}$ be the corresponding 16×16 trace matrix for Λ_0. By definition of the discriminant, we have to show that $\det(T) = (\det(M)\det(N))^4$. This follows from the properties of the Kronecker product of matrices.

It suffices to show that the entry of T at row (i,s) and column (j,r) is $T_{(i,s),(j,r)} = M_{ij}N_{sr}$. We write:

$$\begin{aligned}
T_{(i,s),(j,r)} &= \mathrm{trd}_C((e_i \otimes f_s)(e_j \otimes f_r)) \\
&= \mathrm{trd}_C(e_i e_j \otimes f_s f_r) \\
&= \frac{1}{4}\,\mathrm{Tr}_{C/\mathbb{Q}}(e_i e_j \otimes f_s f_r) \\
&= \frac{1}{4}\,\mathrm{Tr}_{A/\mathbb{Q}}(e_i e_j)\,\mathrm{Tr}_{B/\mathbb{Q}}(f_s f_r) \\
&= \left(\frac{1}{2}\,\mathrm{Tr}_{A/\mathbb{Q}}(e_i e_j)\right)\left(\frac{1}{2}\,\mathrm{Tr}_{B/\mathbb{Q}}(f_s f_r)\right) \\
&= \mathrm{trd}_A(e_i e_j)\,\mathrm{trd}_B(f_s f_r) \\
&= M_{ij}N_{sr}
\end{aligned}$$

We used the general property of the trace with respect to the tensor product: $\mathrm{Tr}_{A\otimes B/\mathbb{Q}}(u \otimes v) = \mathrm{Tr}_{A/\mathbb{Q}}(u)\,\mathrm{Tr}_{B/\mathbb{Q}}(v)$. □

7.4. Final Outline and Catch. With known maximal orders $\mathcal{O}_A$ and $\mathcal{O}_B$ and known ramified primes, we have a polynomial-time algorithm:

1. Construct the initial order $\Lambda_0 = \mathcal{O}_A \otimes_{\mathbb{Z}} \mathcal{O}_B^{\mathrm{op}}$.

2. Compute a maximal order $\Lambda \supset \Lambda_0$ using the known prime factors of $\mathrm{disc}(\Lambda_0)$. (Ivanyos & Rónyai, 1993)

3. Find a rank-one element within the maximal order $\Lambda \cong \mathrm{M}_4(\mathbb{Z})$. (Ivanyos, Rónyai, & Schicho, 2018)

Theorem 7.11. *Given a maximal order in each algebra and their ramified primes, we can compute an explicit isomorphism in polynomial time in size of the inputs.*

The Catch While the algorithm is polynomial-time in theory, it seems impractical.

The algorithm of Ivanyos & Rónyai (1993) for computing a maximal order is actually efficient; it's implemented in Magma, and we provide a full implementation in Sage.

However, the algorithm of Ivanyos, Rónyai, & Schicho (2018) for finding a rank-one element in a matrix ring, given a maximal order, seems more theoretical. The idea in their paper is to embed the maximal order Γ into $M_n(\mathbb{R})$, which isn't too difficult. They then view Γ as a lattice to find a shorter element in Γ that must have rank one. To do this, Ivanyos, Rónyai, & Schicho construct a basis for Γ such that the coefficients of the shorter vector in this basis are integers bounded by an absolute constant, given explicitly for the matrix ring $M_4(\mathbb{Q})$ by:

Theorem 7.12. *A four dimensional algebra over a field F of characteristic not 2 is a quaternion algebra if an only if it is a central simple algebra.*

Proof. See [Voi21, p. 7.6.1] □

$$c_{16} := (\gamma_{16})^{\frac{16}{2}} \left(\frac{3}{2}\right)^{16} 2^{\frac{16(16-1)}{2}}$$

where γ_{16} is the Hermite constant for lattices. Even though γ_{16} isn't exactly known, under a conjecture by Mächler and Naccache (2022), we obtain $\gamma_{16}^{16} = 2^{24}$, which leads to $c_{16} = 2^{116} \cdot 3^{16}$. This means the search space for the shorter vector is of size $(2 \cdot c_{16} + 1)^{16}$, which is computationally impossible.

We tried to implement this algorithm, and at the end, to search "randomly" in this space starting with small values, but it was not successful. As far as we know, this algorithm seems impossible to implement in this manner, even if it is polynomial time in theory.

8. Method 3: Isomorphism via Equivalence of Quadratic Forms

Let $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ with α, β, a, b integers. Assume that A and B are isomorphic and non-split, that is, not isomorphic to $\mathrm{M}_2(\mathbb{Q})$. As seen in Theorem 2.1, computing an explicit isomorphism $f : A \to B$ is equivalent to computing an explicit equivalence between their corresponding quadratic forms. That is, very explicitly, to compute a matrix $M \in \mathrm{GL}_3(\mathbb{Q})$ such that

$$M^T \begin{pmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{pmatrix} M = \begin{pmatrix} -\alpha & 0 & 0 \\ 0 & -\beta & 0 \\ 0 & 0 & \alpha\beta \end{pmatrix}.$$

For this, we use a method from Mark Watkins [Wat06, Paragraph 2.7]. This requires introducing the notion of a *maximal isotropic subspace*.

8.1. Maximal isotropic subspace.

Definition 8.1. Let $n > 0$ be an integer and $S \in \mathrm{M}_n(\mathbb{Q})$ be a symmetric matrix viewed as a quadratic form. A *(totally) isotropic subspace* of S is a subspace $H \subset \mathbb{Q}^n$ such that for all $x \in H$, $x^T S x = 0$. Equivalently, for all $x, y \in H$, $x^T S y = 0$.

An isotropic subspace H is *maximal* if it is of maximal dimension among all isotropic subspaces of S.

Concretely, vectors $U_1, \ldots, U_r \in \mathbb{Q}^n$ form a basis of some isotropic subspace of S if and only if they are all isotropic for S and orthogonal to each other with respect to S, that is:

$$\begin{pmatrix} U_1^T \\ \vdots \\ U_r^T \end{pmatrix} S \begin{pmatrix} U_1 & \ldots & U_r \end{pmatrix} = 0.$$

Also, when $\det(S) \neq 0$, we have that the dimension of a maximal isotropic subspace is at most $n/2$. This follows because...

In his article [Sim05a], Denis Simon extends his work on quadratic forms of dimension 3 [Sim05b] to quadratic forms of dimension 4, 5, and higher. In particular, he develops algorithms to find an isotropic vector of a matrix $S \in \mathrm{M}_n(\mathbb{Z})$. These algorithms require factoring $\det(S)$ and are then believed to run in polynomial time in the size of the entries of S (apart from the factorization step, which is not known to be polynomial). He also gave an algorithm which computes a "large" isotropic subspace of a matrix $S \in \mathrm{M}_n(\mathbb{Z})$. This algorithm also requires one factorization of

$\det(S)$ and is then believed to run in polynomial time in the entries of S. However, it is not guaranteed to output a maximal isotropic subspace. Specifically:

- When $\det(S) = 1$, the output is maximal [Sim05a, Algorithm 2].
- When n is odd, the output is maximal [Sim05a, Algorithm 6].
- When n is even, the output may not be maximal [Sim05a, Algorithm 7].

All of these algorithms are currently implemented in Magma under `IsotropicSubspace`. In our experiments, this implementation seems to be always correct (for dimension 6) and runs in polynomial time, except for the factorization. Hence, we are led to make the following mathematical assumption:

Assumption B. Given $n > 0$, a matrix $S \in \mathrm{M}_n(\mathbb{Z})$ and the factorization of $\det(S)$, there exists a polynomial-time algorithm in the size of the entries of S which outputs a basis of a maximal isotropic subspace of S. Perhaps the algorithm of Simon, or a modification of it, works.

8.2. Equivalence of quadratic forms. We now present the idea of [Wat06, Paragraph 2.7]. Let $S_1, S_2 \in \mathrm{M}_n(\mathbb{Z})$ be two symmetric matrices with integer entries, assumed to be equivalent over $\mathbb{Q}$ and anisotropic. We want to compute an equivalence from S_1 to S_2, that is, a matrix $M \in \mathrm{GL}_n(\mathbb{Q})$ such that $M^T S_1 M = S_2$.

Let T be the block symmetric matrix which defines a quadratic form of dimension $2n$:

$$T = \begin{pmatrix} S_1 & 0 \\ 0 & -S_2 \end{pmatrix}.$$

The dimension of a maximal isotropic subspace of an invertible symmetric matrix of dimension $2n$ is n. Assuming the factorization of $\det(T) = \det(S_1)\det(S_2)$ is known, and using the algorithm of Assumption B, we can compute a basis of an isotropic subspace of dimension n, say $U_1, \ldots, U_n$, for T. This means $U_1, \ldots, U_n$ are linearly independent and

$$\begin{pmatrix} U_1 & \ldots & U_n \end{pmatrix}^T T \begin{pmatrix} U_1 & \ldots & U_n \end{pmatrix} = 0.$$

Then, writing the $2n \times n$ matrix as

$$\begin{pmatrix} U_1 & \ldots & U_n \end{pmatrix} = \begin{pmatrix} R \\ S \end{pmatrix},$$

with R, S being two $n \times n$ matrices, it follows that

$$R^T S_1 R - S^T S_2 S = 0. \tag{4}$$

Since S_1, S_2 are assumed anisotropic, this implies R and S are invertible: if x is a non-zero vector in the kernel of R, since the matrix $\begin{pmatrix} R \\ S \end{pmatrix}$ has rank n (because

$U_1, \ldots, U_n$ are linearly independent), then x is not in the kernel of S. It follows that Sx is a non-zero isotropic vector for S_2, a contradiction. So the kernel of R is trivial, and similarly for S, so they are invertible.

We deduce from (4) that $M := RS^{-1}$ is an invertible matrix such that $M^T S_1 M = S_2$. We have thus shown:

Theorem 8.2 (Watkins)**.** *Under Assumption B, given two symmetric matrices $S_1, S_2 \in \mathrm{M}_n(\mathbb{Z})$, assumed equivalent and anisotropic when viewed as quadratic forms, if we know the factorization of $\det(S_1)$ and $\det(S_2)$, then there is a polynomial-time algorithm in the entries of S_1, S_2 which computes an equivalence $M \in \mathrm{GL}_n(\mathbb{Q})$ between S_1 and S_2.*

8.3. Application to quaternion algebra isomorphism. As said in the beginning of the section, given $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ with α, β, a, b integers, being isomorphic and non-split quaternion algebras, an isomorphism from A to B is exactly a matrix $M \in \mathrm{GL}_3(\mathbb{Q})$ such that

$$M^T \begin{pmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{pmatrix} M = \begin{pmatrix} -\alpha & 0 & 0 \\ 0 & -\beta & 0 \\ 0 & 0 & \alpha\beta \end{pmatrix}.$$

The two diagonal matrices are anisotropic (since the algebras are non-split), and by Theorem 8.2, we only need to factor their determinants.

Theorem 8.3. *Under Assumption B, let $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ with α, β, a, b integers be isomorphic and non-split quaternion algebras. Assuming the factorization of α, β, a, b is given, then there is a polynomial-time algorithm in the size of α, β, a, b to compute an isomorphism from A to B.*

Proof. Use Theorem 2.1 and Theorem 8.2 applied to $S_1 = \mathrm{diag}(-\alpha, -\beta, \alpha\beta)$ and $S_2 = \mathrm{diag}(-a, -b, ab)$ with their determinant factorizations known. □

Remark 8.4. As far as we know, this is the best-known algorithm for this problem. Surprisingly, the decision isomorphism problem `DecideIsoQuatAlg` (see Theorem 3.4) requires the same factorization and is then polynomial-time, like the explicit isomorphism problem `ExplicitIsoQuatAlg` (under Assumption B).

It is an open question to justify or infirm Assumption B, even if it seems valid thanks to the implementation in Magma.

It is also an open question to determine if `DecideIsoQuatAlg` and `ExplicitIsoQuatAlg` are theoretically polynomial-time equivalent, and also equivalent to `Factor`, in a precise sense.

8.4. Use of maximal orders. We now study how the difficulty can change when we are given maximal orders $\mathcal{O}_A \subset A$ and $\mathcal{O}_B \subset B$ and the ramified primes of A and B. The idea is that the knowledge of a maximal order, for example $\mathcal{O}_B \subset B$, gives us an equivalence between the quadratic form $-aX^2 - bY^2 + abZ^2$ and a quadratic form with a simpler determinant, in the sense that it is easy to factorize. That is, the matrix

$$M^T \begin{pmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{pmatrix} M$$

has integer entries and a determinant that is easy to factorize. To this purpose, we introduce the notion of the *trace zero subspace*.

Definition 8.5. Let $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a quaternion algebra and $\mathcal{O} \subset B$ be an order. The *trace zero subspace* of $\mathcal{O}$ is

$$\mathcal{O}_0 := \{x \in \mathcal{O} \mid \mathrm{trd}(x) = 0\}.$$

Lemma 8.6. *Let $\mathcal{O}$ be a maximal order in a quaternion algebra. There exists an element in $\mathcal{O}$ of odd reduced trace.*

Proof. Write $\mathcal{O} = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4$. Assume for the purpose of contradiction that $\mathrm{trd}(x)$ is even for all $x \in \mathcal{O}$. Then the discriminant $\mathrm{disc}(\mathcal{O}) = \det(\mathrm{trd}(e_i e_j)_{1 \leq i,j \leq 4})$ must be divisible by 16. But since $\mathcal{O}$ is maximal,

$$\mathrm{disc}(\mathcal{O}) = \left(\prod_{p \text{ ramified in } B} p \right)^2,$$

which cannot be divisible by 16. This is a contradiction. □

Lemma 8.7. *Let $\mathcal{O}$ be a maximal order in a quaternion algebra B. The trace zero subspace $\mathcal{O}_0$ has rank 3 as a $\mathbb{Z}$-module. If we write $\mathcal{O}_0 = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$, then the Gram matrix of the reduced trace bilinear form on this basis has determinant:*

$$\det(\mathrm{trd}(e_i e_j)_{1 \leq i,j \leq 3}) = -2 \left(\prod_{p \text{ ramified in } B} p \right)^2.$$

Proof. The trace zero subspace $\mathcal{O}_0$ is the kernel of the non-zero $\mathbb{Z}$-linear form $\mathrm{trd} : \mathcal{O} \to \mathbb{Z}$, so it has rank 3 as a $\mathbb{Z}$-module. Assume $\mathcal{O}_0 = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$. Let us denote

$$L := \mathbb{Z} \oplus \mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3.$$

L is a sublattice of $\mathcal{O}$. More precisely, L is the kernel of the map $\pi \circ \mathrm{trd} : \mathcal{O} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Indeed, any element of L has an even trace. Conversely, if $x \in \mathcal{O}$

has an even trace $\mathrm{trd}(x) = 2k$, then $x - k$ has trace 0, so $x - k \in \mathcal{O}_0$. Hence $x = k + (x - k) \in \mathbb{Z} + \mathcal{O}_0 = L$.

By Lemma 8.6, the map $\pi \circ \mathrm{trd}$ is surjective. So it follows that $[\mathcal{O} : L] = |\mathcal{O}/L| = |\mathbb{Z}/2\mathbb{Z}| = 2$. Hence, using Proposition 4.3, on one hand,

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

On the other hand, by definition of the discriminant (with $e_0 := 1$),

$$\mathrm{disc}(L) = |\det(\mathrm{trd}(e_i e_j)_{0\le i,j\le 3})| = \left|\det \begin{pmatrix} 2 & 0 \\ 0 & (\mathrm{trd}(e_i e_j))_{1\le i,j\le 3} \end{pmatrix}\right| = 2\,|\det(\mathrm{trd}(e_i e_j)_{1\le i,j\le 3})|\,.$$

Overall, using Theorem 4.5, we deduce

$$\det(\mathrm{trd}(e_i e_j)_{1\le i,j\le 3}) = -2\,\mathrm{disc}(\mathcal{O}) = -2\left(\prod_{p \text{ ramified in } B} p\right)^2.$$

The negative sign comes from the determinant of the quadratic form on B_0 with the basis i, j, ij (if $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ the matrix of trd in i, j, ij is $\mathrm{diag}(2a, 2b, -2ab)$ with determinant $-4(ab)^2 < 0$.) □

So, given a quaternion algebra B and a maximal order $\mathcal{O}$ with a $\mathbb{Z}$-basis, we can compute a basis e_1, e_2, e_3 of the kernel $\mathcal{O}_0$ in polynomial time. Let M_B be the change-of-basis matrix from the basis $\{e_1, e_2, e_3\}$ to the canonical basis $\{i, j, k\}$ of B_0. The Gram matrix of the trace form in the canonical basis is $D_B = \mathrm{diag}(2a, 2b, -2ab)$, while in the basis $\{e_i\}$ it is $S_B = (\mathrm{trd}(e_i e_j))$. These are related by $S_B = M_B^T D_B M_B$. The determinant of S_B has a known factorization by the lemma 8.7 if we know the ramified primes. This allows us to construct an equivalence from the natural quadratic form of B to an equivalent one whose determinant has a known prime factorization. We deduce the following algorithm.

Algorithm 1: Explicit Isomorphism of Quaternion Algebras with Maximal Orders

Input: $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right), B = \left(\frac{a,b}{\mathbb{Q}}\right)$ isomorphic quaternion algebras, $\mathcal{O}_A, \mathcal{O}_B$ maximal orders, and the set of ramified primes.

Output: An isomorphism from A to B.

1. Compute bases of $(\mathcal{O}_A)_0$ and $(\mathcal{O}_B)_0$.
2. Compute the Gram matrices S_A and S_B for these bases, and the change-of-basis matrices M_A, M_B to the canonical bases.
3. Call the algorithm from Theorem 8.2 on S_A and S_B to find M_W such that $M_W^T S_B M_W = S_A$. The required determinant factorization is known from Lemma 8.7.
4. Output the isomorphism matrix $M_{iso} = M_B M_W M_A^{-1}$.

With the notation $D_B = \mathrm{diag}(2a, 2b, -2ab)$ and $D_A = \mathrm{diag}(2\alpha, 2\beta, -2\alpha\beta)$, the step 3 give $M_W^T S_B M_W = S_A$ so $M_W^T M_B^T D_B M_B M_W = M_A^T D_A M_A$. The output matrix satisfy

$$M_{iso}^T \mathrm{diag}(a, b, -ab) M_{iso} = \mathrm{diag}(\alpha, \beta, -\alpha\beta),$$

hence an isomorphism $f : A \to B$ is given by $f(i)$ has coordinates the first column of M_{iso} and $f(j)$ has coordinates the second column of M_{iso}. We have proved the following theorem.

Theorem 8.8. *Under Assumption B, Algorithm 1 runs in polynomial time in the size of the inputs (sizes of a, b, α, β and coefficients of the basis elements of $\mathcal{O}_A$ and $\mathcal{O}_B$) and outputs an isomorphism from A to B.*

Remark 8.9. This algorithm runs with the same theoretical complexity as the algorithm of Method 2 7: given a maximal order in each quaternion algebra and the common set of ramified primes, the algorithm is in polynomial time in the size of the input. However, the algorithm of Method 2 seems impractical, as mentioned in paragraph 7.4. But our new algorithm is really practical, and we provide an implementation in Magma that relies on the native function `IsotropicSubspace`. This assumes that this function satisfies Assumption B, which seems true in experiments.

A. Central Simple Algebras

All algebras B over a field F are assumed to be unitary and associative, so that we can view $F \subset B$. We recall that the center of B is the set $Z(B)$ of elements $b \in B$ that commute with every $x \in B$. It is a sub-F-algebra of B.

An algebra is a *division algebra* if every non-zero element has a two-sided inverse. Note that the center of a division algebra is a field, and every division algebra has the structure of an algebra over its center.

An algebra B, or more generally a ring, is *simple* if its only two-sided ideals are $\{0\}$ and B. This is equivalent to saying that for any non-zero ring R, every ring homomorphism $B \to R$ is injective. Now we define an important class of algebras.

Definition A.1. Let F be a field. A *central simple algebra* over F is a finite-dimensional algebra over F whose center is exactly F and which has no non-trivial two-sided ideals.

The standard example of a central simple algebra is $B = \mathrm{M}_n(F)$, called the *split* central simple algebra of dimension n^2. The goal of this section is to show that, by extending the base field, every central simple algebra becomes isomorphic to a split one.

First, as simple algebras, central simple algebras enjoy the following strong structure theorem.

Wedderburn-Artin Theorem and Consequences.

Theorem A.2 (Wedderburn-Artin Theorem, weak version)**.** *Let B be a finite-dimensional simple algebra over F. Then there exists a division algebra D over F and an integer $n \geq 1$ such that B is isomorphic to $\mathrm{M}_n(D)$. Moreover, D is unique up to F-algebra isomorphism.*

The proof follows [GS06, Section 2.1] by Philippe Gille and Tamás Szamuely.

Proof. Let I be a minimal non-zero left ideal of B. Such an ideal exists because a left ideal is an F-subspace, so we can choose one of minimal positive dimension. Define the ring D to be the ring of B-linear endomorphisms of I:

$$D := \mathrm{End}_B(I) = \{f : I \to I \mid f \text{ is a group homomorphism and } f(bx) = bf(x) \text{ for all } x \in I, b \in B\}.$$

This is a sub-F-algebra of $\mathrm{End}_F(I)$, and we claim that it is a division algebra. Indeed, if $f : I \to I$ is a non-zero B-linear map, then its kernel and image are left ideals of B contained in I. Since $f \neq 0$, $\ker(f) \neq I$ and $\mathrm{im}(f) \neq \{0\}$. By the minimality of I, we must have $\ker(f) = \{0\}$ and $\mathrm{im}(f) = I$. Therefore, f is an isomorphism and thus has an inverse in D.

Now, we consider the ring of D-linear endomorphisms of I:

$$\mathrm{End}_D(I) = \{f : I \to I \mid f \text{ is a group homomorphism and } f \circ g = g \circ f \text{ for all } g \in D\}.$$

It is also a sub-F-algebra of $\mathrm{End}_F(I)$.

For any $b \in B$, the map of left multiplication by b is in $\mathrm{End}_D(I)$. This allows us to define a map:

$$\Phi : B \to \mathrm{End}_D(I); \quad b \mapsto (x \mapsto bx).$$

It is immediate that Φ is an F-algebra homomorphism. Furthermore, $\ker(\Phi)$ is a two-sided ideal of B. Since Φ is non-zero (e.g., $\Phi(1) = \mathrm{id}_I$), its kernel cannot be all of B. By the simplicity of B, $\ker(\Phi) = \{0\}$, so Φ is injective. Let us show surjectivity. First, note that the set

$$IB := \left\{ \sum_{i=1}^{r} x_i b_i \mid r \in \mathbb{Z}_{\geq 0}, x_i \in I, b_i \in B \right\}$$

is a non-zero two-sided ideal of B, and thus $IB = B$ by simplicity. Hence, we can write $1 = \sum_{i=1}^{r} x_i b_i$ for some integer $r > 0$. Now let $f \in \mathrm{End}_D(I)$. We have:

$$f = f\Phi(1) = \sum_{i=1}^{r} f \circ \Phi(x_i) \circ \Phi(b_i).$$

For $i = 1, \ldots, r$, and $z \in I$, since $\mathrm{id}_I \cdot z$ is in $\mathrm{End}_D(I)$, by definition f commutes with $\mathrm{id}_I \cdot z$. This yields

$$f \circ \Phi(x_i)(z) = f(x_i z) = f(x_i)z = \Phi(f(x_i))(z),$$

hence $f \circ \Phi(x_i) = \Phi(f(x_i))$.

And finally,

$$f = \Phi\left(\sum f(x_i)b_i\right).$$

This concludes the proof of surjectivity. Thus, Φ realizes an F-algebra isomorphism between B and $\mathrm{End}_D(I)$.

Finally, by the theory of modules over a division ring, I is a free D-module of some rank n, i.e., $I \cong D^n$. It follows that

$$\mathrm{End}_D(I) \cong \mathrm{End}_D(D^n) \cong \mathrm{M}_n(D^{op}) \cong \mathrm{M}_n(D)$$

as rings, and therefore as F-algebras. This completes the proof. □

It follows that if K is an algebraically closed field, then every central simple algebra over K is isomorphic to some matrix algebra $\mathrm{M}_n(K)$. Indeed if D is a division algebra over K then $D = K$: for all $x \in D$ the minimal polynomial of x over K is irreducible (because D is a domain) and so is of degree 1, hence $x \in K$.

Lemma A.3. *Let B be a finite dimensional algebra over F and K/F be a field extension. Then B is a central simple algebra over F if and only if $B \otimes_F K$ is a central simple algebra over K.*

Proof. See Philippe Gille and Tamás Szamuely [GS06, Lemma 2.2.2.]. □

Proposition A.4. *Let B be a finite dimensional algebra over F. Then there exists a field extension K/F such that $B \otimes_F K \cong \mathrm{M}_n(K)$ as a K-algebra, for some integer n.*

Proof. It follows from taking K to be the algebraic closure of F in the previous lemma and the previous remark. □

Reduced trace. Let F be a field and let B be a central simple algebra over F. Let K be an algebraic closure of F so that $B \otimes_F K \cong \mathrm{M}_n(K)$. Hence, we can embed B into $\mathrm{M}_n(K)$ via

$$\varphi : B \to \mathrm{M}_n(K), \quad b \mapsto b \otimes 1.$$

We define the *reduced trace* of $b \in B$ by

$$\mathrm{trd}(b) := \mathrm{trace}(\varphi(b)) \in K.$$

Proposition A.5. *Assume that F is of characteristic 0. The reduced trace of b does not depend on the choice of the isomorphism. It satisfies the following properties:*

1. *For all $b \in B$, we have*

$$\mathrm{trd}(b) = \frac{1}{n}\mathrm{trace}_F(B \to B,\ x \mapsto bx),$$

   hence $\mathrm{trd}(b) \in F$, and $\mathrm{trd} : B \to F$ is an F-linear form.

2. *The map $B \times B \to F,\ (x, y) \mapsto \mathrm{trd}(xy)$ is a non-degenerate F-bilinear form.*

3. *If $F = \mathrm{Frac}(R)$ for some principal ideal domain R, and if $x \in B$ is integral over R, then $\mathrm{trd}(x) \in R$.*

Lemma A.6 (Skolem-Noether Theorem for matrix rings)**.** *Let K be a field. Every K-algebra automorphism of $\mathrm{M}_n(K)$ is inner, that is, of the form $M \mapsto PMP^{-1}$ for some $P \in \mathrm{GL}_n(K)$.*

Proof of Lemma A.6. Let $\phi : \mathrm{M}_n(K) \to \mathrm{M}_n(K)$ be a K-algebra automorphism. Let $I \subset \mathrm{M}_n(K)$ be the left ideal of matrices with only the first column nonzero. Fix a nonzero $u_0 \in K^n$. Since ϕ is an automorphism, $\phi((u_0 \mid 0 \mid \cdots \mid 0)) \neq 0$. Thus, we can choose $x_0 \in K^n$ such that

$$\phi((u_0 \mid 0 \mid \cdots \mid 0))x_0 \neq 0.$$

Define the K-linear endomorphism

$$P : K^n \to K^n, \quad u \mapsto \phi((u \mid 0 \mid \cdots \mid 0))x_0.$$

For any $M \in \mathrm{M}_n(K)$ and any $u \in K^n$, we have $PMu = \phi(M)Pu$, so $PM = \phi(M)P$. The kernel of P is stable under left multiplication by any matrix in $\mathrm{M}_n(K)$. Since $Pu_0 \neq 0$, the kernel is not all of K^n, and since the only ideals of $\mathrm{M}_n(K)$ are $\{0\}$ and $\mathrm{M}_n(K)$, the kernel must be zero. Hence, P is an isomorphism, and

$$\phi(M) = PMP^{-1}.$$

□

Proof of Proposition A.5. The well-definedness follows directly from Lemma A.6. For any field K of characteristic 0 and any matrix $M \in \mathrm{M}_n(K)$, we have

$$\mathrm{trace}(M) = \frac{1}{n}\mathrm{trace}_F(\mathrm{M}_n(K) \to \mathrm{M}_n(K),\ Z \mapsto MZ).$$

Hence,

$$\mathrm{trd}(b) = \mathrm{trace}_F(\mathrm{M}_n(K) \to \mathrm{M}_n(K),\ Z \mapsto \varphi(b\otimes 1)Z) = \mathrm{trace}_F(B\otimes_F K \to B\otimes_F K,\ z \mapsto (b\otimes 1)z).$$

Since we can choose a K-basis of $B \otimes_F K$ of the form $e_1 \otimes 1, \dots, e_N \otimes 1$, where $e_1, \dots, e_N$ is an F-basis of B, this trace equals that of the map $B \to B,\ z \mapsto bz$. This proves the first point, as F-linearity is evident.

Now let $x \in B$, and assume that $\mathrm{trd}(xy) = 0$ for all $y \in B$. Then

$$\mathrm{trace}(\varphi(xy \otimes 1)) = 0 \quad \text{for all } y \in B.$$

Hence,

$$\mathrm{trace}(\varphi(x \otimes 1)\varphi(y \otimes 1)) = 0 \quad \text{for all } y \in B.$$

Since the set $\{y \otimes 1 \mid y \in B\}$ spans $B_K = B \otimes_F K$ over K, it follows that $\varphi(x \otimes 1)$ is orthogonal to all matrices in $\mathrm{M}_n(K)$ under the trace pairing, and thus must be zero. Hence, $x \otimes 1 = 0$, and therefore $x = 0$. This proves the second point.

Finally, suppose that $x \in B$ is integral over R. Then the matrix $A := \varphi(x \otimes 1)$ is integral over R, so its eigenvalues lie in $K = F^{\mathrm{alg}}$ and are integral over R. Therefore, the trace of A, being the sum of its eigenvalues, is also integral over R. But since we have already seen that $\mathrm{trd}(x) = \mathrm{trace}(A) \in F$, and R is integrally closed in F, it follows that $\mathrm{trd}(x) \in R$. This proves the third point. □

Theorem A.7. *A four-dimensional algebra over a field F of characteristic not 2 is a quaternion algebra if and only if it is a central simple algebra.*

Proof. See [Voi21, p. 7.6.1]. □

B. Implementation and Algorithms

The source code for this project is publicly available on GitHub at https://github.com/TommyChakroun/quat_alg_project. The repository contains the following main folders:

- **iso_isotropicsubspace**: This folder contains the Magma implementation for Method 3 8, which uses an isotropic subspace to solve quadratic equivalence.
- **iso_solving_quadratics**: Here you will find the implementations for Method 1 6, which focuses on solving quadratic forms.
- **iso_splitting_algebra**: This folder holds the reduction steps for Method 2 7, which involves splitting matrix rings. It also contains functions for computing maximal orders in semi-simple algebras.
- **quaternion_recognition**: This folder includes functions to identify a quaternion algebra, identify its standard involution, and normalize a quadratic form.

This appendix provides a detailed mathematical overview of some key algorithms, particularly those in the `iso_splitting_algebra` folder for computing maximal orders in semi-simple algebras.

B.1. Reduction $\varphi : A \otimes_{\mathbb{Q}} B^{op} \to \mathrm{M}_4(\mathbb{Q})$ to $f : A \to B$. Let A, B be two central simple algebras of same dimension n. In Proposition 7.1 we showed the equivalence

$$A \cong B \iff A \otimes_{\mathbb{Q}} B \cong M_{n^2}(\mathbb{Q}).$$

The proof of the direct implication was already explicit and efficient, but for the converse we had argued theoretically with the Wedderburn decomposition. Here we present an efficient but randomized algorithm to show this converse implication.

Suppose we have $\varphi : A \otimes_{\mathbb{Q}} B^{op} \to M_4(\mathbb{Q})$ an isomorphism. Fix us $e_1, \dots, e_N$ a basis of A and $f_1, \dots, f_n$ a basis of B. Denote $N = n^2$ and $V = \mathbb{Q}^N$. For each $v \in V$ we consider:

$$\lambda_v : A \to V, \quad a \mapsto \varphi(a \otimes 1)v$$
$$\mu_v : B \to V, \quad b \mapsto \varphi(1 \otimes b)v.$$

Both λ_v and μ_v are $\mathbb{Q}$-linear maps.

First we claim that if we find $v \in V$ such that both λ_v and μ_v are $\mathbb{Q}$-linear isomorphisms, then $f : A \to B$, $a \mapsto \mu_v^{-1}(\lambda_v(a))$ is a $\mathbb{Q}$-algebra isomorphism. Indeed f

is a $\mathbb{Q}$-linear isomorphism, $\mu_v(1) = v = \lambda_v(1)$ so f maps 1_A to 1_B. For the preservation of the product: let $a, a' \in A$ and $b = f(a)$, $b' = f(a')$ in B. Then

$$\begin{aligned}
\mu_v(f(aa')) &= \varphi(aa' \otimes 1)v \\
&= \varphi(a \otimes 1)\varphi(a' \otimes 1)v \\
&= \varphi(a \otimes 1)\varphi(1 \otimes b')v \\
&= \varphi(1 \otimes b')\varphi(a \otimes 1)v \\
&= \varphi(1 \otimes b')\varphi(1 \otimes b)v \\
&= \varphi(1 \otimes bb')v \\
&= \mu_v(bb')
\end{aligned}$$

This shows $f(aa') = f(a)f(a')$.

Hence it suffices to show the existence of a suitable $v \in V$. We do this for λ. This comes from the theoretical existence of an isomorphism from A to B as follows. Choose $f : A \to B$ an isomorphism and denote $\varphi_f : A \otimes_{\mathbb{Q}} B^{op} \to M_N(\mathbb{Q})$ the other isomorphism obtained. By Lemma A.6 there exists some invertible matrix $P \in M_N(\mathbb{Q})$ such that:

$$\forall c \in A \otimes_{\mathbb{Q}} B^{op}, \quad \varphi(c) = P\varphi_f(c)P^{-1}.$$

Then for $v \in V$ and $a \in A$ we have

$$P\lambda_{P^{-1}v}(a) = P\varphi(a \otimes 1)P^{-1}v = \varphi_f(a \otimes 1)v = \mathrm{Mat}(b \mapsto f(a)b)v.$$

Hence if we take v to be the coordinates of 1_B in the basis of B we obtain:

$$P\lambda_{P^{-1}v} : A \to V, \quad a \mapsto \mathrm{Mat}(f(a), B)$$

so it is an isomorphism.

Now from the existence of a suitable v we are going to deduce that almost all $v \in V$ satisfy this condition in the following sense.

Fix a basis $e_1, \ldots, e_N$ of A, and let $M_i = \varphi(e_i \otimes 1) \in M_N(\mathbb{Q})$. For all $v = (v_1, \ldots, v_N) \in V$:

The matrix of λ_v in the basis $e_1, \ldots, e_N$ of A and the canonical basis of $V = \mathbb{Q}^N$ is, by columns:

$$\begin{pmatrix} M_1 v & \cdots & M_N v \end{pmatrix}.$$

Expanding, we have:

$$\begin{pmatrix} \sum_{j=1}^N m_{1j}^{(1)} v_j & \cdots & \sum_{j=1}^N m_{1j}^{(N)} v_j \\ \sum_{j=1}^N m_{2j}^{(1)} v_j & \cdots & \sum_{j=1}^N m_{2j}^{(N)} v_j \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^N m_{Nj}^{(1)} v_j & \cdots & \sum_{j=1}^N m_{Nj}^{(N)} v_j \end{pmatrix}$$

where $M_i = (m_{kj}^{(i)})_{1\leq k,j\leq N} \in M_N(\mathbb{Q})$.

So the determinant is of the form $P_A(v_1, \ldots, v_N)$ for some $P_A \in \mathbb{Q}[T_1, \ldots, T_N]$.

The fact that we found one suitable v proves that P_A is not identically zero. Then by the Schwartz-Zippel lemma for all finite subset $S \subset \mathbb{Q}$ we have $\mathrm{Card}(Z(P_A) \cap S^N) \leq N\,\mathrm{Card}(S)^{N-1}$.

Similarly for P_B associated to B and μ, $\mathrm{Card}(Z(P_B) \cap S^N) \leq N\,\mathrm{Card}(S)^{N-1}$.

Then a $v \in V$ satisfies both λ_v and μ_v are isomorphisms if and only if v is not a zero of P_A neither P_B. By taking $S \subset \mathbb{Q}$ sufficiently large such that $2N\,\mathrm{Card}(S)^{N-1} < \mathrm{Card}(S)^N$ this is possible. This concludes the proof and we deduce the following algorithm.

Algorithm 2: Isomorphism $f : A \to B$ from $\varphi : A \otimes B^{op} \to M_N(\mathbb{Q})$

Input: A, B two central simple algebras of dimension n and
$\varphi : A \otimes B^{op} \to M_N(\mathbb{Q})$ an isomorphism given in a basis $e_i \otimes f_j$ which is the tensor product of a basis of A and a basis of B

Output: $f : A \to B$ an isomorphism

1. Choose a finite subset $S \subset \mathbb{Q}$ such that $2N\mathrm{Card}(S)^{N-1} < \mathrm{Card}(S)^N$

foreach $v \in S^N$ **do**

2. Compute U the matrix of $A \to V$, $a \mapsto \varphi(a \otimes 1)v$ in the basis of A and the canonical basis of V
3. Compute M the matrix of $B \to V$, $b \mapsto \varphi(1 \otimes b)v$ in the basis of B and the canonical basis of V
4. **if** *M and U are invertible* **then**
5. Compute M^{-1}
6. **return** *$f : A \to B$ given in the basis of A by:*

$$f(e_i) = \sum_{j=1}^{N} M^{-1}_{j,i} U_{j,i} f_j$$

end

end

B.2. Solution to a System $AX \equiv 0 \pmod{d}$ for Integral Matrices.

Algorithm 3: ModularMatrixKernel

Input: $A \in M_{m\times n}(\mathbb{Z})$, $d \in \mathbb{Z}_{>0}$

Output: $X_1, \dots, X_k \in \mathbb{Z}^n$ a $\mathbb{Z}$-basis of the $\mathbb{Z}$-submodule $\{X \in \mathbb{Z}^n \mid AX \equiv 0 \pmod d\}$

1. Compute the Smith normal form of A: $U \in \mathrm{GL}_m(\mathbb{Z})$, $V \in \mathrm{GL}_n(\mathbb{Z})$ such that $UAV = D$ is in diagonal form
2. If $t = \min(n, m)$, let $Y_1, \dots, Y_t$ be defined by $Y_i = (0, \dots, 0, \frac{d}{\gcd(d, D_{i,i})}, 0, \dots, 0)$
3. If $n > m$, complete with $Y_j = (0, \dots, 0, 1, 0, \dots, 0)$ for $t < j \leq n$
4. **return** $VY_1, \dots, VY_k$

Implementation. The function `kernel_mod(A,d)` is available at `src/iso_splitting_algebra/explicit_iso_quat_alg.sage`

B.3. Computation of Left Order. Let B be a finite dimensional algebra over $\mathbb{Q}$ of dimension N. Let

$$I = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$$

be a $\mathbb{Z}$-(full) lattice in B. The *left order* of I is the set

$$O_L(I) := \{\alpha \in B \mid \alpha I \subset I\}.$$

We claim that $O_L(I)$ is indeed an order. Indeed $O_L(I)$ is a $\mathbb{Z}$-submodule of B, is stable under multiplication, contains 1. It remains to show that $O_L(I)$ contains a $\mathbb{Q}$-basis of B. Starting from $b_1, \dots, b_N$ any basis of B, then for all i there exists $t_i \in \mathbb{Z}_{>0}$ such that $t_i b_i \in O_L(I)$.

Now we want to compute explicitly a $\mathbb{Z}$-basis $f_1, \dots, f_N$ of $O_L(I)$. First note that there exists $s \in \mathbb{Z}_{>0}$ such that $s \cdot 1_B \in I$. Hence $O_L(I) \cdot s \subset I$ so $O_L(I) \subset s^{-1}I$. After, for $\alpha \in s^{-1}I$ that we write $\alpha = s^{-1}(x_1e_1 + \cdots + x_Ne_N)$ with $x_i \in \mathbb{Z}$:

$$\alpha \in O_L(I) \iff \forall j, \alpha e_j \in I \iff \forall j, s^{-1}(x_1e_1e_j + \cdots + x_Ne_Ne_j) \in \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$$

Let's write the *structure constants* of the basis $e_1, \dots, e_N$, that is:

$$e_ie_j = \sum_{k=1}^{N} c_{ijk}e_k \quad ((1 \leq i, j \leq N),\ c_{ijk} \in \mathbb{Q}).$$

Then

$$\alpha \in O_L(I) \iff \forall j, k, \sum_{i=1}^{N} s^{-1}c_{ijk}x_i \in \mathbb{Z}$$

or equivalently by denoting $X = (x_1, \ldots, x_N) \in \mathbb{Z}^N$ and $T = (s^{-1}c_{ijk})$ the rational matrix with N^2 rows and N columns:

$$\alpha \in O_L(I) \iff TX \in \mathbb{Z}^{N^2}.$$

Finally by multiplying both sides by the least common multiple of the denominators of T this yields solving $AX \equiv 0 \pmod{d}$ for some integer matrix A of size $N^2 \times N$. Hence together with the previous algorithm we deduce a method to compute the left order of I.

Algorithm 4: LeftOrder

Input: B a finite dimensional algebra over $\mathbb{Q}$; $e_1, \ldots, e_N$ a $\mathbb{Q}$-basis of B representing $I = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$

Output: A $\mathbb{Z}$-basis of the left order $O_L(I)$

1. Write $1_B = r_1e_1 + \cdots + r_Ne_N$ with $r_i \in \mathbb{Q}$
2. Let $s \in \mathbb{Z}_{>0}$ be the least common multiple of the denominators of r_i
3. Compute $c_{i,j,k}$ the structure constants of the basis $e_1, \ldots, e_N$, that is $e_ie_j = \sum c_{i,j,k}e_k$
4. Let d be the lcm of the denominators of the $s \cdot c_{i,j,k}$ and let $A = (d \cdot s \cdot c_{i,j,k})_{1 \le i \le N; 1 \le j,k \le N} \in M_{N^2,N}(\mathbb{Z})$
5. Let $X_1, \ldots, X_\ell \in \mathbb{Z}^N$ be a $\mathbb{Z}$-basis of solutions of $AX \equiv 0 \pmod{d}$
6. **return** $f_1, \ldots, f_\ell \in B$ *where* $f_i = \frac{1}{s}(X_{i,1}e_1 + \cdots + X_{i,N}e_N)$

Implementation. The function `left_order(B,Zbasis_I)` is available at `src/_iso_splitting_algebra/_maximal_orders/_maximal_orders_utilities.sage`.

Remark B.1. If we suppose in addition that B is a division algebra or even just that every element of the $\mathbb{Z}$-basis $e_1, \ldots, e_N$ of the lattice $I = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_N$ are invertible in B, then we can use a more efficient algorithm as follows. Let $\alpha \in B$, we have

$$\alpha \in O_L(I) \iff \forall j, \alpha e_j \in I \iff \forall j, \alpha \in e_j^{-1}I = \mathbb{Z}e_j^{-1}e_1 \oplus \cdots \oplus \mathbb{Z}e_j^{-1}e_N$$

The last direct sum holds because $(e_j^{-1}e_1, \ldots, e_j^{-1}e_N)$ is still a $\mathbb{Q}$-basis of B since $z \mapsto e_j^{-1}z$ is a $\mathbb{Q}$-linear automorphism of B.

Hence to compute the left order it suffices to compute an intersection of lattices. There are efficient algorithms for this based on the Hermite normal form. This is the method used in SageMath for the case of division quaternion algebras.

B.4. Randomized Computation of Central Idempotents over a Finite Field.

We begin with some general notions about rings. Let R be an arbitrary (unital) ring. There is a correspondence between:

1. The decomposition of R into ideals: $R = I_1 \oplus \cdots \oplus I_r$,

2. The decomposition of 1_R into *central orthogonal idempotents* $1_R = e_1 + \cdots + e_r$, where $e_i \in Z(R)$, $e_i^2 = e_i$, and $e_i e_j = 0$ if $i \neq j$.

Now we turn to algebras over finite fields. Fix a finite field $F = \mathbb{F}_p$. If A is a *semisimple algebra* (i.e., an algebra isomorphic to a direct product of simple algebras), then by the Wedderburn–Artin theorem, there exist integers $n_1, \ldots, n_r$ and division algebras $D_1, \ldots, D_r$ over F such that

$$A \cong \mathrm{M}_{n_1}(D_1) \times \cdots \times \mathrm{M}_{n_r}(D_r).$$

Lemma B.2. *Consequently, A has exactly r minimal nonzero two-sided ideals $I_1, \ldots, I_r$, which satisfy $A = I_1 \oplus \cdots \oplus I_r$. Moreover, writing $1 = e_1 + \cdots + e_r$ for the corresponding decomposition of the identity, the elements $e_1, \ldots, e_r$ are central orthogonal idempotents, and e_i is the identity of I_i.*

Proof. Let us fix an isomorphism as above. The image of $\mathrm{M}_{n_i}(D_i)$ in A is simple, so its image I_i is a minimal nonzero two-sided ideal of A, and $A = I_1 \oplus \cdots \oplus I_r$. By the correspondence above, we obtain a decomposition of 1 into central orthogonal idempotents e_i, each acting as the identity on I_i.

Suppose J is another minimal nonzero two-sided ideal of A. Choose $x \in J$, $x \neq 0$, and write $x = x_1 + \cdots + x_r$ with $x_i \in I_i$. Since $x \neq 0$, assume $x_1 \neq 0$. Then $e_1 x = x_1 \neq 0$, so $I_1 \cap J \neq 0$. But both I_1 and J are minimal two-sided ideals, so $I_1 = J$. Hence, any minimal two-sided ideal must be one of the I_i. □

Lemma B.3. *Conversely, if $e_1, \ldots, e_r$ are central orthogonal idempotents summing to 1, then the ideals Ae_i are exactly the minimal nonzero two-sided ideals of A, up to permutation.*

Finding central orthogonal idempotents $e_1, \ldots, e_r$ summing to 1 in A reduces to finding them in the center $Z(A)$. We have:

$$Z(A) \cong Z(D_1) \times \cdots \times Z(D_r) \cong K_1 \times \cdots \times K_r,$$

where each K_i/F is a finite field extension.

So we are reduced to the following problem: let Z be a finite F-algebra isomorphic to a product

$$Z \cong K_1 \times \cdots \times K_r,$$

of finite field extensions of F. Find a maximal family $e_1, \ldots, e_r$ of central orthogonal idempotents in Z.

To solve this, we study the structure of F-algebras isomorphic to such a product. Let $a = (a_1, \ldots, a_r) \in K_1 \times \cdots \times K_r$. The minimal polynomial of a over F is

$$\pi_a = \operatorname{lcm}(\pi_{a_1}, \ldots, \pi_{a_r}),$$

which is square-free and can be written as $\pi_a = \pi_1 \ldots \pi_s$, with $\{\pi_1, \ldots, \pi_s\} = \{\pi_{a_1}, \ldots, \pi_{a_r}\}$.

If $s \geq 2$, by the Chinese Remainder Theorem, there exist polynomials $h_1, \ldots, h_s$ such that

$$h_i \equiv 1 \pmod{\pi_i}, \quad h_i \equiv 0 \pmod{\pi_j} \text{ for } j \neq i.$$

Then for each i, $h_i(a)$ has the form:

$$w_i = h_i(a) = (h_i(a_1), \ldots, h_i(a_r)) = (0, 0, \ldots, 0, 1, 0, \ldots, 0),$$

which gives a central orthogonal idempotent.

If $s = r$, then the w_i are exactly the elementary idempotents $(0, \ldots, 0, 1, 0, \ldots, 0)$, which form a maximal list of central orthogonal idempotents in $K_1 \times \cdots \times K_r$.

This procedure can be applied in A since minimal polynomials and their factorization are abstract notions that can be computed from structure constants. So we randomly choose $a \in A$, compute its minimal polynomial π_a, factor it as $\pi_a = \pi_1 \ldots \pi_s$, and attempt the construction above.

If $s \geq 2$, then

$$A = A\omega_1 \oplus \cdots \oplus A\omega_s,$$

where each $A\omega_i$ is a unital subalgebra with identity $\omega_i = h_i(a)$. We can then recurse within each $A\omega_i$.

Note that the case $s = r$ may not occur when the prime p is small and r is large; for example, when $A \cong \mathbb{F}_p^r$.

Still, if $r \geq 2$, then $s \geq 2$ occurs for most $a \in A$, so a randomized approach works: pick random elements of A until the minimal polynomial splits. If no such element is found, then A is a field and we return 1_A.

We deduce a deterministic algorithm in theory, but the reasonable complexity is randomized.

Algorithm 5: CentralIdempotentsCommutativeSplit

Input: Z Semisimple commutative algebra over a finite field $\mathbb{F}_p$ given by structure constants

Output: Primitive central idempotents $e_1, e_2, \ldots, e_r \in A$

foreach *a in Z* **do**

1. Compute the minimal polynomial $\pi_a \in \mathbb{F}_p[T]$ of a.
2. Factor $\pi_a = \pi_1 \ldots \pi_s$ in $\mathbb{F}_p[T]$.
3. **if** $s \geq 2$ **then**
   4. By the Chinese remainder theorem, compute $h_1, \ldots, h_s \in \mathbb{F}_p[T]$ such that $h_i \equiv 1 \pmod{\pi_i}$, $\quad h_i \equiv 0 \pmod{\pi_j}$ for $j \neq i$.
   5. Compute $\omega_i := h_i(a) \neq 0$ for $i = 1, \ldots, s$.
   6. Compute a basis BA_i of $A_i := A\omega_i$.
   7. Compute the structure constants of A_i in BA_i and build the abstract version of A_i.
   8. $Res = []$. ;
   9. **foreach** $i = 1, \ldots, s$ **do**
      10. Compute recursively $e_1, \ldots, e_k = \text{CentralIdempotentsCommutative}(A_i)$.
      11. Lift $e_1, \ldots, e_k$ in Z and add it to res.
   end
   12. **return** *Res*

end

13. **return** *the list* 1_A

Implementation. The function `central_idempotent_commutative_split` is available at `src/_iso_splitting_algebra/_minimal_ideals/_minimal_ideals_manually.sage`.

Comments. The algorithm is deterministic in theory with complexity at worst $\text{Card}(Z) = p^n$. It really depends on the size of the prime p and the dimension n. If both are relatively small we can easily iterate on Z. Otherwise if p is a very large prime around 100 bits then we can't reasonably iterate on Z so we prefer to pick a finite random number of elements of Z. Luckily when p is large and n small it happens that the probability that a is *decomposable* that is $s \geq 2$ in the algorithm is very high. Actually when p is very large in comparison to n we can use an easier algorithm. For example in our purpose of computing a maximal order containing an order O in the matrix ring $\text{M}_4(\mathbb{Q})$, for each prime dividing $\text{disc}\, O$ we compute a finite dimensional algebra $\mathcal{A}$ over $\mathbb{F}_p$ of dimension 16 then we quotient $\mathcal{A}$ by its radical so $\mathcal{A}/\text{Rad}(A)$ has dimension less than 16 over $\mathbb{F}_p$ and consequently its center Z has

dimension at most 16 over $\mathbb{F}_p$. It is in this final algebra Z that we run our algorithm. Hence provided that all prime factors of $\operatorname{disc} O$ are much bigger than 16, the following algorithm may give the correct answer with a high probability and less computation time.

Precise evaluation of the probabilities. The success and complexity of the previous algorithm depend directly on the proportion of elements of Z satisfying good algebraic properties. To compute this proportion, we can as well work directly on

$$Z = K_1 \times \cdots \times K_r$$

where $K_i/\mathbb{F}_p$ are finite field extensions. Let us denote $s_i = [K_i : \mathbb{F}_p]$, so that $K_i \cong \mathbb{F}_{p^{s_i}}$. We denote also n the $\mathbb{F}_p$-dimension of Z, that is:

$$n = \sum_{i=1}^{r} s_i = [K_1 : \mathbb{F}_p] + \cdots + [K_r : \mathbb{F}_p]$$

The total number of elements in the algebra is thus $\operatorname{Card} Z = p^n$.

Since we will not know a priori the value of r when running the algorithm, n is the only reasonable bound that we can put on r (as $s_i \geq 1$, we have $r \leq n$).

Now let us define the subsets of Z:

$$S_0 := \{a = (a_1, \ldots, a_r) \in Z \mid \pi_{a_1} = \cdots = \pi_{a_r}\}$$

where π_x denotes the minimal polynomial of x over $\mathbb{F}_p$ and let us denote $d_0 = \frac{\operatorname{Card} S_0}{\operatorname{Card} Z}$ its densities.

Then the success of the algorithm `CentralIdempotentsCommutativeSplit` depends on whether d_0 is near zero for the first split, and afterward we have to deal with the recursion.

Computation of the density d_0. Let $a = (a_1, \ldots, a_r) \in S_0$. By definition, all components a_i share the same minimal polynomial over $\mathbb{F}_p$, let's call it $P(X)$. Let $\deg(P) = d$. For $P(X)$ to be the minimal polynomial of $a_i \in K_i = \mathbb{F}_{p^{s_i}}$, its degree d must be a divisor of s_i. This must hold for all $i = 1, \ldots, r$. Therefore, the degree d of any such common minimal polynomial must divide $g = \gcd(s_1, \ldots, s_r)$.

Let $N_d(p)$ be the number of monic irreducible polynomials of degree d over $\mathbb{F}_p$. For a fixed such polynomial $P(X)$ of degree d, the number of its roots in any field extension K_i where $d \mid s_i$ is exactly d. To form an element of S_0 corresponding to this polynomial $P(X)$, we must choose one of its d roots for each component a_i. This gives d^r choices.

Summing over all possible polynomials, we get the cardinality of S_0:

$$\operatorname{Card} S_0 = \sum_{d|g} N_d(p) \cdot d^r$$

To show that this quantity is small compared to $\operatorname{Card} Z$, we can bound it. Since $d \leq g$ for any $d \mid g$, we have $d^r = d \cdot d^{r-1} \leq d \cdot g^{r-1}$.

$$\begin{aligned} \operatorname{Card} S_0 &\leq \sum_{d|g} N_d(p) \cdot (d \cdot g^{r-1}) \\ &= g^{r-1} \sum_{d|g} N_d(p) \cdot d \end{aligned}$$

Using the classical identity $\sum_{d|m} N_d(p) \cdot d = p^m$, we obtain:

$$\operatorname{Card} S_0 \leq g^{r-1} p^g$$

The density d_0 is therefore bounded by:

$$d_0 = \frac{\operatorname{Card} S_0}{\operatorname{Card} Z} \leq \frac{g^{r-1} p^g}{p^{\sum s_i}}$$

Since $g = \gcd(s_1, \ldots, s_r) \leq s_i$ for all i, we have $\sum s_i \geq r \cdot g$. This gives:

$$d_0 \leq \frac{g^{r-1} p^g}{p^{rg}} = \frac{g^{r-1}}{p^{g(r-1)}} = \left(\frac{g}{p^g}\right)^{r-1}$$

For the algorithm to be in a non-trivial case, we must have $r > 1$. Since $p \geq 2$ and $g \geq 1$, the term p^g grows much faster than g, ensuring that $\frac{g}{p^g} < 1$. For instance, if $p = 2$ and $g = 1$, the ratio is $1/2$. If $g \geq 2$, the ratio is even smaller. Thus, for $r > 1$, the density d_0 is very small, confirming that picking an element from S_0 at random is a low-probability event. For example, if we take the smallest possible values $p = 2, r = 2, g = 1$, we get $d_0 \leq 1/2$. If $r = 3$, $d_0 \leq 1/4$, and so on. The probability decreases exponentially with r.

C. Performance Analysis

This section presents the performance results of our implemented algorithms. The source code is publicly available on GitHub:

`https://github.com/TommyChakroun/quat_alg_project`

We implemented the algorithm from **Method 1** (Section 6), which is based on solving quadratic equations, and the algorithm for **Method 3** (Section 8). For **Method 2**, we only implemented the reduction steps, which are analogous to the algorithm of Ivanyos and Rónyai (Theorem 7.9).

Experimental Setup. The performance was evaluated using statistical tests on 100 randomly generated pairs of quaternion algebras, $A = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$ and $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. The bit lengths of the defining coefficients were scaled by a parameter t as follows:

- The bit lengths of a and b are approximately t.
- The bit length of α is approximately $2t$.
- The bit length of β is approximately $3t$.

Growth of γ in Method 1. A key factor in the practical complexity of Method 1 is the bit-size growth of intermediate values. Figure 1 plots the average bit length of the intermediate value γ against the input size parameter t.

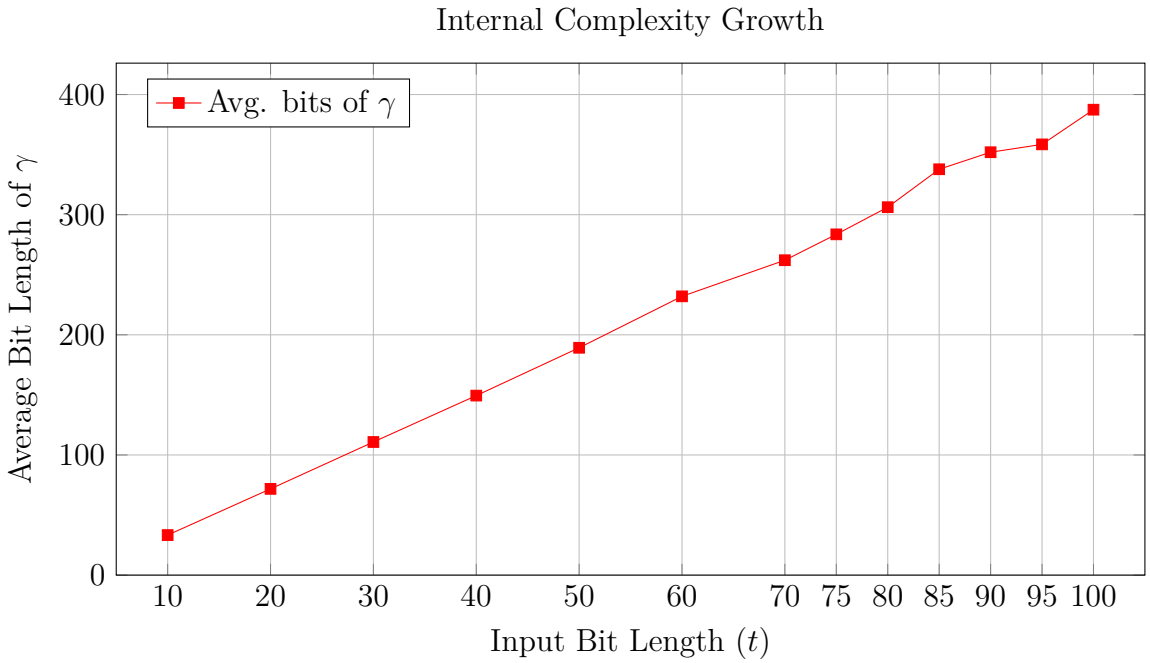

Figure 1: Average bit length of the intermediate value γ versus the input bit length t.

Runtime Comparison: Method 1 vs. Method 3. Figure 2 compares the average execution times of Method 1 and Method 3. The annotations for Method 1 indicate the number of instances (out of 100) that failed to complete within the time limit. Method 3 demonstrates significantly better stability and performance as the input size increases.

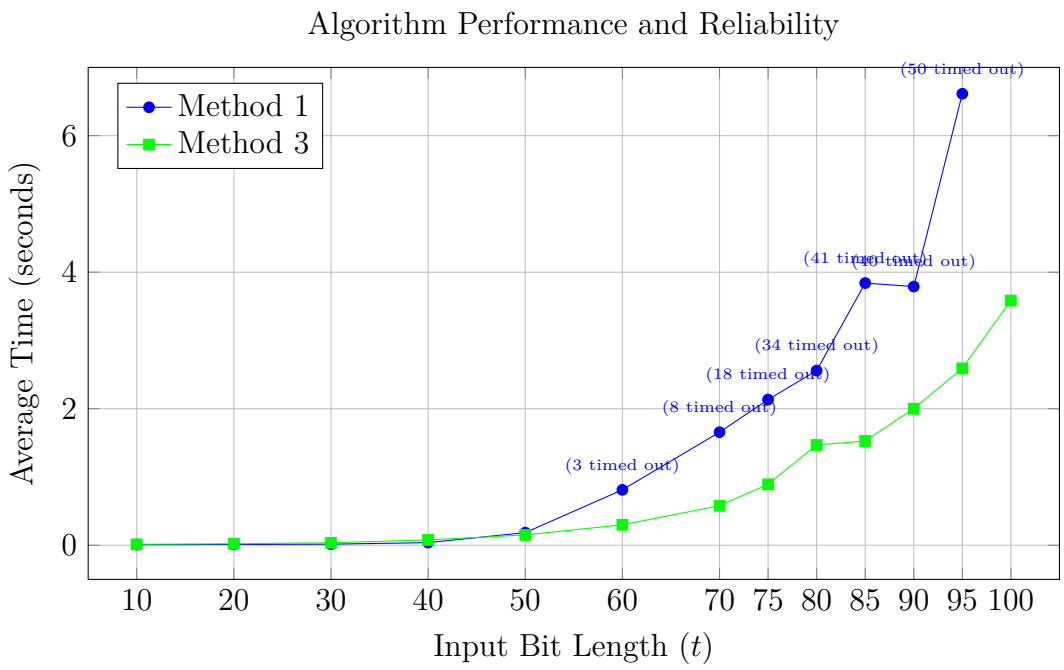

Figure 2: Average computation time of Method 1 (blue) and Method 3 (green) versus input bit length t.

Performance of Maximal Order Computation. This final test evaluates the performance of computing a maximal order in $A \otimes B^{\mathrm{op}}$ using a Sage implementation based on Ivanyos and Rónyai. This subroutine is a key component of Method 2. The test, shown in Figure 3, assumes that maximal orders in A and B are already known and that both algebras are ramified at the prime $p = 7$ and at ∞.

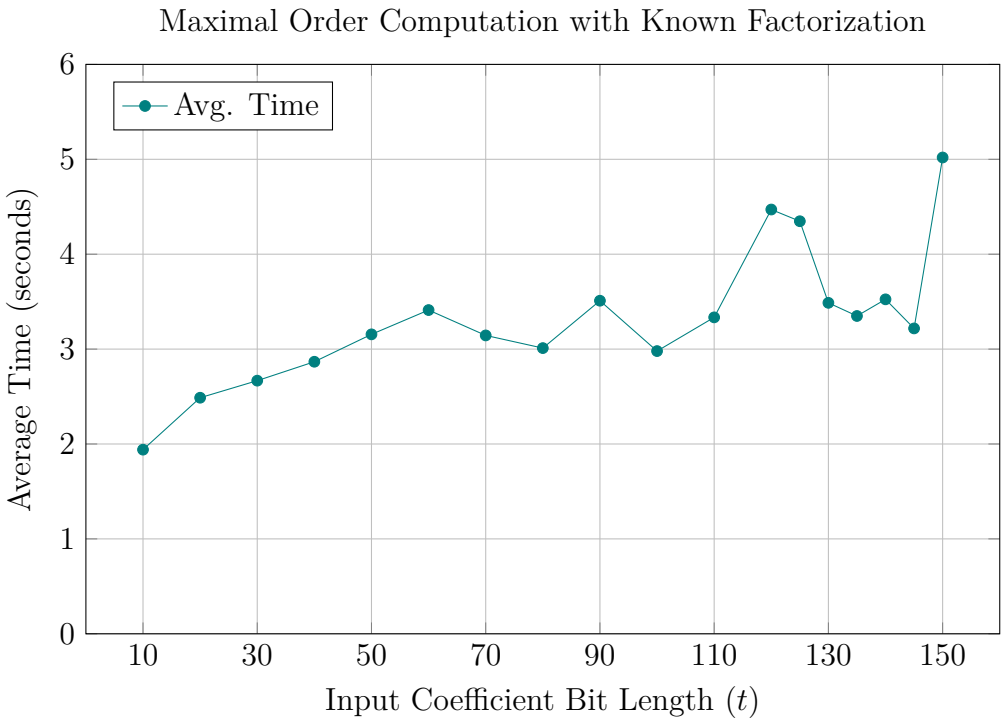

Figure 3: Time to compute the maximal order of $A \otimes B^{\mathrm{op}}$ given maximal orders of A and B, which are both ramified at $p = 7$ and ∞.

References

[Bac90] Eric Bach. "Explicit Bounds for Primality Testing and Related Problems". In: *Mathematics of Computation* 55.191 (1990), pp. 355–380. DOI: 10.1090/S0025-5718-1990-1023756-8.

[Csa+22] Tímea Csahók et al. *Explicit isomorphisms of quaternion algebras over quadratic global fields*. 2022. arXiv: 2007.06981 [math.NT]. URL: https://arxiv.org/abs/2007.06981.

[GS06] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. Vol. 101. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006. ISBN: 978-0-521-86103-8. DOI: 10.1017/CBO9780511607219.

[ILR12] Gábor Ivanyos, Ádám D. Lelkes, and Lajos Rónyai. *Improved algorithms for splitting full matrix algebras*. 2012. arXiv: 1211.1356 [math.RA]. URL: https://arxiv.org/abs/1211.1356.

[IR93] Gábor Ivanyos and Lajos Rónyai. "Finding maximal orders in semisimple algebras over Q". In: *Computational Complexity* 3 (1993), pp. 245–261. DOI: 10.1007/BF01271370. URL: https://link.springer.com/article/10.1007/BF01271370.

[IRS12] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho. "Splitting full matrix algebras over algebraic number fields". In: *Journal of Algebra* 354.1 (Mar. 2012), pp. 211–223. DOI: 10.1016/j.jalgebra.2012.01.008.

[IS96] Gábor Ivanyos and Ágnes Szántó. "Lattice basis reduction for indefinite forms and an application". In: *Discrete Mathematics* 153.1-3 (1996). Proceedings of the 5th Conference on Formal Power Series and Algebraic Combinatorics (Florence, 1993), pp. 177–188.

[Sim02] Denis Simon. "Solving norm equations in relative number fields using S-units". In: *Mathematics of Computation* 71.239 (2002), pp. 1301–1321. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-02-01309-1. URL: https://www.ams.org/journals/mcom/2002-71-239/S0025-5718-02-01309-1/S0025-5718-02-01309-1.pdf.

[Sim05a] Denis Simon. "Quadratic equations in dimensions 4, 5 and more." In: *LMNO - UMR 6139, Université de Caen – France* (2005). 11th May 2005. URL: mailto:simon@math.unicaen.fr.

[Sim05b] Denis Simon. "Solving quadratic equations using reduced unimodular quadratic forms". In: *Mathematics of Computation* 74.251 (2005), pp. 1531–1543.

[Voi12] John Voight. *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*. 2012. arXiv: 1004.0994 [math.NT]. URL: https://arxiv.org/abs/1004.0994.

[Voi21] John Voight. *Quaternion Algebras*. Vol. 288. Graduate Texts in Mathematics. Cham: Springer, 2021. ISBN: 978-3-030-56692-0. DOI: 10.1007/978-3-030-56694-4. URL: https://link.springer.com/book/10.1007/978-3-030-56694-4.

[Wat06] Mark Watkins. "Some comments about Indefinite LLL". In: *Magma Computer Algebra Group, School of Mathematics and Statistics, Carslaw Building F07, University of Sydney* (2006).