Improved algorithms for splitting full matrix algebras

Gábor Ivanyos
Computer and Automation Research Institute, Hungarian Acad. Sci.
Gabor.Ivanyos@sztaki.hu

Ádám D. Lelkes
Dept. of Algebra, Budapest Univ. of Technology and Economics
lelkesa@math.bme.hu

Lajos Rónyai
Computer and Automation Research Institute, Hungarian Acad. Sci.
Dept. of Algebra, Budapest Univ. of Technology and Economics
lajos@ilab.sztaki.hu

November 7, 2012

Abstract

Let $\mathbb{K}$ be an algebraic number field of degree d and discriminant Δ over $\mathbb{Q}$. Let $\mathcal{A}$ be an associative algebra over $\mathbb{K}$ given by structure constants such that $\mathcal{A} \cong M_n(\mathbb{K})$ holds for some positive integer n. Suppose that d, n and $|\Delta|$ are bounded. In a previous paper a polynomial time ff-algorithm was given to construct explicitly an isomorphism $\mathcal{A} \to M_n(\mathbb{K})$.

Here we simplify and improve this algorithm in the cases $n \leq 43$, $\mathbb{K} = \mathbb{Q}$, and $n = 2$, with $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. The improvements are based on work by Y. Kitaoka and R. Coulangeon on tensor products of lattices.

1 Introduction

The following *explicit isomorphism problem* is important in computational representation theory: let $\mathbb{K}$ be an algebraic number field, $\mathcal{A}$ an associative algebra over $\mathbb{K}$. Suppose that $\mathcal{A}$ is isomorphic to the full matrix algebra $M_n(\mathbb{K})$. Construct explicitly an isomorphism $\mathcal{A} \to M_n(\mathbb{K})$. Or, equivalently, give an irreducible $\mathcal{A}$ module.

The algebra $\mathcal{A}$ is considered to be given by a collection of *structure constants* $\gamma_{ijk} \in \mathbb{K}$. They form the multiplication table of $\mathcal{A}$ with respect to some $\mathbb{K}$ basis $a_1, \ldots, a_m$: the products $a_i a_j$ can be expressed as

$$a_i a_j = \gamma_{ij1} a_1 + \gamma_{ij2} a_2 + \cdots + \gamma_{ijm} a_m.$$

In [5] a polynomial time ff-algorithm was given for the case of the problem, when n and the degree and the discriminant of $\mathbb{K}$ are all bounded. Applications were also outlined there,

[0] *2010 Mathematics Subject Classification:* 16Z05, 11Y16, 68W30.
Key words and phrases: Central simple algebra, maximal order, real and complex embedding, lattice basis reduction, tensor product of lattices, Hermite constant, Bergé-Martinet constant.
Our work was supported in part by OTKA grants NK 105645, K77476, and K77778.

including some parametrization problems of algebraic geometry. The methods of [5] are based on theoretical and algorithmic results on lattices and eventually boil down to enumerating short vectors in some lattices in real Euclidean spaces.

In this paper we present considerable improvements of the methods of [5] in the case when the ground field $\mathbb{K}$ is the rationals, and $n \leq 43$. This is based on results of Kitaoka [6], [7] on tensor products of lattices, in particular we make use of the powerful result of Corollary 2. In Theorem 3 we prove a quantitative version, which allows further reduction in computing time. Some of Kitaoka's results have been extended by Coulangeon [3] from $\mathbb{Q}$ to imaginary quadratic fields. Using these we also obtain an improvement of the original algorithm when $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ (Gaussian rationals) or $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ (Eisenstein numbers) for the case $n = 2$. The new algorithms are simpler and faster than the original ones.

For the basic definitions and facts on lattices in real Euclidean spaces we refer to [2], [9], and [10].

2 Full matrix algebras over $\mathbb{Q}$

A *(full) lattice* $L \subset \mathbb{R}^n$ is the free Abelian group generated by n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$. Then $M = (\mathbf{b}_1|\mathbf{b}_2|\ldots|\mathbf{b}_n)$ is a matrix of L, and $|\det M|$ is called the *determinant* of L, and is denoted by $\det L$. We denote by $\lambda_1(L)$ the Euclidean length of the shortest nonzero vector from L. The nth *Hermite's constant* is

$$\gamma_n := \sup_L \left(\frac{\lambda_1(L)}{(\det L)^{1/n}} \right)^2,$$

where L is a full lattice in $\mathbb{R}^n$. Hermite proved that γ_n actually exists. The exact value of γ_n is known only for $n \in \{1, 2, \ldots, 8, 24\}$.

We briefly recall now the definition of the tensor product of lattices, for more information see section 1.10 of Martinet [9], and section 7 in Kitaoka [7]. Let L and M be two lattices in $\mathbb{R}^m$ and $\mathbb{R}^n$, respectively. The tensor product of $\mathbb{Z}$ modules $L \otimes_{\mathbb{Z}} M$ embeds in the straightforward way into $\mathbb{R}^m \otimes_{\mathbb{R}} \mathbb{R}^n$. This allows one to define $L \otimes M$ as the set of integral linear combinations of the tensors $\mathbf{x} \otimes \mathbf{y}$ from $\mathbb{R}^m \otimes_{\mathbb{R}} \mathbb{R}^n$ where $\mathbf{x} \in L$ and $\mathbf{y} \in M$.

Note that, in terms of coordinates, $L \otimes M$ can be viewed as the set (actually lattice) of m by n matrices over $\mathbb{R}$ which are integral linear combinations of dyads of the form $\mathbf{x}\mathbf{y}^T$, where $\mathbf{x} \in L$ and $\mathbf{y} \in M$. Note also that $\mathbb{R}^m \otimes \mathbb{R}^n$ is an Euclidean space with the law $\langle \mathbf{x}_1 \otimes \mathbf{y}_1, \mathbf{x}_2 \otimes \mathbf{y}_2 \rangle = \langle \mathbf{x}_1, \mathbf{x}_2 \rangle \langle \mathbf{y}_1, \mathbf{y}_2 \rangle$. In this setting the norm on the tensor product $\mathbb{R}^m \otimes \mathbb{R}^n$ is actually the Frobenius norm on the space of matrices $M_{m,n}(\mathbb{R})$.

Let L be a full lattice in $\mathbb{R}^m$. The *dual* L^* of L consists of those vectors $\mathbf{y} \in \mathbb{R}^m$ for which we have $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ holds for every $\mathbf{x} \in L$. The supremum γ'_n of $\lambda_1(L)\lambda_1(L^*)$ among full lattices $L \subset \mathbb{R}^n$ is the *Bergé-Martinet constant*, see [1], [9]. It is known that $\gamma'_n \leq \gamma_n$ for every n.

Following Y. Kitaoka [6] we say that a lattice L is of *E-type* if every minimal nonzero vector of $L \otimes M$ is of the form $\mathbf{x} \otimes \mathbf{y}$ ($\mathbf{x} \in L$, $\mathbf{y} \in M$) for any lattice M.

Kitaoka proved in [6], and in Theorem 7.1.1. of [7] the following.

Theorem 1 (Kitaoka)**.** *If L is a lattice of rank at most* 43*, then L is of E-type.*

We remark here that by a theorem of Steinberg (see [10], Chapter II, §9) for any integer $n \geq 292$ there exists a lattice L such that $\lambda_1(L \otimes L^*) < \lambda_1(L)\lambda_1(L^*)$. Thus, the conclusion of Kitaoka's theorem does not hold for larger values of n.

We can apply Kitaoka's theorem to maximal orders of the form $\Lambda = QM_n(\mathbb{Z})Q^{-1} \subset M_n(\mathbb{R})$, where $Q \in GL_n(\mathbb{R})$.

Corollary 2. *For any dimension $n \leq 43$ and subring $\Lambda \subset M_n(\mathbb{R})$ of the above form the nonzero matrices with the smallest Frobenius norm in Λ are of rank one.*

Proof. The order Λ is given by the transformation matrix Q. As in the proof of Theorem 1 of [5], we see that as a lattice $\Lambda \cong Q\mathbb{Z}^n \otimes (Q\mathbb{Z}^n)^*$. But $Q\mathbb{Z}^n$ is a rank n lattice, hence it is of E-type, giving that the matrices of minimal norm in Λ are dyadic products of vectors from $Q\mathbb{Z}^n$ and $(Q\mathbb{Z}^n)^*$, and hence have rank 1 as matrices from $M_n(\mathbb{R})$. □

Thus, when $n \leq 43$, then the smallest zero divisors in any Λ have rank one. In particular, no matrix from Λ of rank at least 2 can have minimal length. By using a modified variant of Kitaoka's original argument, we prove a slightly stronger, quantitative version of the latter statement.

Recall that the *rank* of a nonzero tensor $\mathbf{v} \in L \otimes M$ is the smallest positive integer r such that $\mathbf{v}$ can be written as

$$\mathbf{v} = \sum_{i=1}^{r} \mathbf{x}_i \otimes \mathbf{y}_i \tag{1}$$

for some $\mathbf{x}_1, \ldots, \mathbf{x}_r \in L$ and $\mathbf{y}_1, \ldots, \mathbf{y}_r \in M$.

Theorem 3. *Let L and M be lattices. Then for every tensor $\mathbf{v} \in L \otimes M$ of rank r we have*

$$\|\mathbf{v}\| \geq \sqrt{\frac{r}{\gamma_r^2}} \lambda_1(L \otimes M).$$

We remark that the above bound is meaningful when the dimension of L or M is at most 43. Then obviously $r \leq 43$, and by Lemma 7.1.2 from [7] for $2 \leq r \leq 43$ we have $1 < r/\gamma_r^2$. For r large the bound becomes trivial, because r/γ_r^2 tends to zero as r grows. We shall need Lemma 7.1.3 from [7]:

Lemma 4. *Let $A, B \in M_n(\mathbb{R})$ be positive definite real symmetric matrices. Then we have* $\mathrm{Tr}(AB) \geq n \sqrt[n]{\det A} \sqrt[n]{\det B}$.

Proof of Theorem 3. Let $\mathbf{v} \in L \otimes M$ be a tensor of rank r. Then $\mathbf{v}$ can be written in the form (1). Let L_1 be the lattice generated by $\{\mathbf{x}_1, \ldots, \mathbf{x}_r\}$, and similarly let M_1 be the lattice spanned by $\{\mathbf{y}_1, \ldots, \mathbf{y}_r\}$. By the minimality of representation (1) the rank of these sublattices is r. Noting that

$$\|\mathbf{v}\|^2 = \left\| \sum_{i=1}^{r} \mathbf{x}_i \otimes \mathbf{y}_i \right\|^2 = \sum_{i,j=1}^{r} \langle \mathbf{x}_i, \mathbf{x}_j \rangle \langle \mathbf{y}_i, \mathbf{y}_j \rangle = \mathrm{Tr}([\langle \mathbf{x}_i, \mathbf{x}_j \rangle]_{i,j=1}^{r} \cdot [\langle \mathbf{y}_i, \mathbf{y}_j \rangle]_{i,j=1}^{r}),$$

and by using Lemma 4 we obtain

$$\|\mathbf{v}\|^2 \geq r \left(\det[\langle \mathbf{x}_i, \mathbf{x}_j \rangle] \cdot \det[\langle \mathbf{y}_i, \mathbf{y}_j \rangle] \right)^{1/r}. \tag{2}$$

Now let us assume for contradiction that $\|\mathbf{v}\|^2 < (r/\gamma_r^2)\lambda_1(L \otimes M)^2$. It follows that

$$\|\mathbf{v}\|^2 < \frac{r}{\gamma_r^2} (\lambda_1(L)\lambda_1(M))^2 \leq \frac{r}{\gamma_r^2} (\lambda_1(L_1)\lambda_1(M_1))^2.$$

Combining this with (2) we obtain

$$r < \frac{r}{\gamma_r^2} \cdot \frac{\lambda_1(L_1)^2}{(\det[\langle \mathbf{x}_i, \mathbf{x}_j \rangle])^{1/r}} \cdot \frac{\lambda_1(M_1)^2}{(\det[\langle \mathbf{y}_i, \mathbf{y}_j \rangle])^{1/r}} \leq \frac{r}{\gamma_r^2} \gamma_r^2,$$

since $[\langle \mathbf{x}_i, \mathbf{x}_j \rangle]_{i,j=1}^r$ and $[\langle \mathbf{y}_i, \mathbf{y}_j \rangle]_{i,j=1}^r$ are Gram matrices for L_1 and M_1, respectively. The contradiction finishes the proof. $\square$

Using the known values of γ_r simple calculation gives that the minimal value of r/γ_2^2 for $2 \leq r \leq 8$ is $\frac{3}{2}$, which is attained at $r = 2$. We remark that the bound of Theorem 3 is sharp, at least for $r = 2$. This is demonstrated by the hexagonal lattice $A_2 \leq \mathbb{R}^2$ which is generated by the vectors

$$\begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

It is known that A_2 is attains the Hermite constant, moreover this holds also for the dual lattice A_2^* which is spanned by the vectors

$$\begin{pmatrix} 0 \\ \frac{2}{\sqrt{3}} \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -\frac{1}{\sqrt{3}} \end{pmatrix}.$$

Some calculation shows that the minimal norm among the rank two tensors in $A_2 \otimes A_2^*$ is $\sqrt{2} = \sqrt{\frac{3}{2}} \cdot \frac{2}{\sqrt{3}} = \sqrt{\frac{3}{2}} \lambda_1(A_2) \lambda_1(A_2^*)$.

In [5] it was shown that for the shortest nonzero matrix $\mathbf{v} \in \Lambda = QM_n(\mathbb{Z})Q^{-1}$ we have $\|\mathbf{v}\| \leq \gamma_n$, where γ_n is the Hermite constant. This can be strengthened as follows. Using again that $\Lambda \cong Q\mathbb{Z}^n \otimes (Q\mathbb{Z}^n)^*$, we obtain that

$$\|\mathbf{v}\| \leq \lambda_1(Q\mathbb{Z}^n) \lambda_1((Q\mathbb{Z}^n)^*) \leq \gamma_n', \tag{3}$$

where γ' is the Bergé-Martinet constant.

3 The modified IRS algorithm over $\mathbb{Q}$ for $n \leq 43$

The input of the algorithm is an associative algebra $\mathcal{A}$ over $\mathbb{Q}$ given by structure constants. It is known that $\mathcal{A}$ is isomorphic to the full matrix algebra $M_n(\mathbb{Q})$. The objective of the algorithm is to find an element $C \in \mathcal{A}$ which has rank one, when viewed as a matrix from $M_n(\mathbb{Q})$.

The first four steps of the algorithm below are identical to the first four steps of the corresponding algorithm from [5]. The last two steps of that method are replaced here by a new step 5:

1. Construct a maximal order Λ in $\mathcal{A}$.

2. Compute an embedding of $\mathcal{A}$ into $M_n(\mathbb{R})$. This way we have a Frobenius norm on $\mathcal{A}$. For $X \in \mathcal{A}$ we can set $\|X\| = \sqrt{Tr(X^T X)}$. Also, via this embedding Λ can be viewed as a full lattice in $\mathbb{R}^m$, where $m = n^2$. The length $\|\mathbf{v}\|$ of a lattice vector $\mathbf{v}$ is just the Frobenius norm of $\mathbf{v}$ as a matrix.

3. Compute a rational approximation A of our basis B of Λ with a suitable precision.

4. Obtain a reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_m$ of the lattice $\Lambda \subset \mathbb{R}^m$ by computing an LLL-reduced basis from A. The value c_m of reducedness is $(\gamma_m)^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}$.

5. Generate all integral linear combinations

$$C = \sum_{i=1}^{m} \alpha_i \mathbf{b}_i,$$

where α_i are integers, $|\alpha_i| \leq c_m$, until a C is found with $\operatorname{rank} C = 1$. Output this C.

Theorem 5. *This algorithm is correct when $n \leq 43$. Moreover, it runs in ff-polynomial time.*

Proof. For the details and timing of steps 1-4 we refer to the proof of Theorem 1 from [5]. As a result of these computations we obtain a basis $\mathbf{b}_1, \ldots, \mathbf{b}_m$ of the lattice Λ such that

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdots \|\mathbf{b}_m\| \leq c_m \cdot \det(\Lambda)$$

holds with

$$c_m = (\gamma_m)^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}.$$

We recall the following bound by H. W. Lenstra [8].

Lemma 6. *Let Γ be a full lattice in $\mathbb{R}^m$. Suppose that we have a basis $\mathbf{b}_1, \ldots, \mathbf{b}_m$ of Γ over $\mathbb{Z}$ such that*

$$\|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \cdots \|\mathbf{b}_m\| \leq c \cdot \det(\Gamma)$$

holds for a real number $c > 0$. Suppose that

$$\mathbf{v} = \sum_{i=1}^{m} \alpha_i \mathbf{b}_i \in \Gamma, \quad \alpha_i \in \mathbb{Z}.$$

Then we have $|\alpha_i| \leq c\frac{\|\mathbf{v}\|}{\|\mathbf{b}_i\|}$ for $i = 1, \ldots, m$.

Let $\mathbf{v} \in \Lambda$ be a nonzero vector with minimal length. Then, on one hand, by Corollary 2 $\mathbf{v}$ is a matrix of rank one. On the other hand, when $\mathbf{v}$ is expressed as an integer linear combination $\mathbf{v} = \sum_{i=1}^{m} \alpha_i \mathbf{b}_i$ then by Lemma 6 we have

$$|\alpha_i| \leq c_m \frac{\|\mathbf{v}\|}{\|\mathbf{b}_i\|} \leq c_m. \tag{4}$$

This implies that there is indeed a rank one matrix $C \in \Lambda$ among the linear combinations enumerated.

To obtain the timing bound, we observe that at step 5 we enumerate at most $(2c_m + 1)^m$ linear combinations, and this value is bounded by our assumption $n \leq 43$. □

We remark that the upper bound $|\alpha_i| \leq c_m$ which defines the domain to be searched at step 5 can be reduced. During the run of step 5 one may update the quantity d which is the actual minimum of the numbers $(\gamma_r^2/\sqrt{r})\|C\|$ over the matrices C enumerated so far (here r is the rank of C). From (4), Theorem 3, and (3) it follows that

$$|\alpha_i| \leq c_m \frac{\min\{d, \gamma'_n\}}{\|\mathbf{b}_i\|}. \tag{5}$$

4 Two by two matrices over imaginary quadratic fields

Here we consider possible extensions of the improvements obtained over $\mathbb{Q}$ to other number fields. In general not much is known about tensor products of lattices over general number fields. On the positive side, Coulangeon [3] extended some of Kitaoka's results to imaginary quadratic fields.

Let $\mathbb{K}$ denote an imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer. By $\mathcal{O}$ we denote the ring of algebraic integers in $\mathbb{K}$: $\mathcal{O} = \mathbb{Z}1 + \mathbb{Z}\sqrt{-d} + \mathbb{Z}\frac{1+\sqrt{-d}}{2}$ if $d \equiv -1$ modulo 4 and $\mathcal{O} = \mathbb{Z}1 + \mathbb{Z}\sqrt{-d}$ otherwise. In the next discussion we consider $\mathbb{K}$ (and hence $\mathcal{O}$) to be embedded into $\mathbb{C}$.

Let $\mathcal{A}$ be a central simple algebra of dimension 4 over $\mathbb{K}$ isomorphic to $M_2(\mathbb{K})$ and let Λ be a maximal order in $\mathcal{A}$. We assume that we are given an embedding ϕ of $\mathcal{A}$ into $M_2(\mathbb{C})$. From the theory of central simple algebras over number fields we know (see Corollary 27.6 in Reiner [11]) that there exists a matrix $B \in M_2(\mathbb{C})$ and a fractional ideal I of $\mathcal{O}$ such that

$$B\phi(\Lambda)B^{-1} = \begin{pmatrix} \mathcal{O} & I^{-1} \\ I & \mathcal{O} \end{pmatrix}.$$

In other words, there exists a full $\mathcal{O}$-lattice L in $\mathbb{C}^2$ (a finitely generated $\mathcal{O}$-submodule of $\mathbb{C}^2$ that spans $\mathbb{C}^2$ as a linear space over $\mathbb{C}$) such that

$$\Lambda = \{A \in M_2(\mathbb{C}) : AL \subseteq L\}.$$

In fact, for our specific Λ, we can take $L = B\begin{pmatrix} \mathcal{O} \\ I \end{pmatrix}$.

Let $\langle , \rangle$ stand for the standard Hermitian bilinear form on $\mathbb{C}^2$. The linear extension of the mapping $u \otimes v \mapsto A_{u,v}$ where $A_{u,v}w = \langle v, w\rangle u$ gives an identification of $M_2(\mathbb{C})$ with $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^2$. By this identification, the tensor square of the standard Euclidean norm of $\mathbb{C}^2$ becomes the Frobenius norm of matrices. Also, Λ is identified with $L \otimes_{\mathcal{O}} L^*$ where

$$L^* = \left\{u \in \mathbb{C}^2 : \langle u, v\rangle \in L \text{ for every } v \in L\right\}$$

and $L \otimes_{\mathcal{O}} L^*$ is just the additive subgroup of $\mathbb{C}^2 \otimes_{\mathbb{C}} C^2$ spanned by the tensors of the form $u \otimes v$ where $u \in L$ and $v \in L^*$.

Remark. We can speak about the rank of an element $\mathbf{x} \in L \otimes_{\mathcal{O}} L^*$ in two ways. One is the minimal positive integer r such that $\mathbf{x}$ can be written as

$$\mathbf{x} = \sum_{i=1}^{r} \mathbf{x}_i \otimes \mathbf{y}_i, \tag{6}$$

for some vectors $\mathbf{x}_i \in L$ and $\mathbf{y}_i \in L^*$. The other possible notion of rank is the rank of $\mathbf{x}$ as a matrix from $M_2(\mathbb{C})$. The two notions are not the same[1]. As an example[2], let $d = 5$, and $\Lambda = M_2(\mathcal{O})$ and consider the matrix

$$C = \begin{pmatrix} 3 & 1+\sqrt{-5} \\ 1-\sqrt{-5} & 2 \end{pmatrix}$$

[1]It is not hard to show that the two notions of rank coincide if $\mathcal{O}$ is a principal ideal ring.

[2]We thank Géza Kós for suggesting this example.

from Λ. We have $\det C = 0$, hence C has rank 1 as a matrix from $M_2(\mathbb{C})$. Moreover, using the fact that 3 and 2 are irreducible elements in $\mathcal{O}$, we see that C is not a decomposable tensor from $\mathcal{O}^2 \otimes_{\mathcal{O}} \mathcal{O}^2$.

We shall use the term *rank* in the former sense. We note also, that in the minimal representation (6) the vectors $\mathbf{x}_i$ and $\mathbf{y}_i$ are linearly independent over $\mathbb{K}$. For a proof we refer to Lemma 3.1 in [3].

Let M be an $\mathcal{O}$-submodule of $\mathbb{C}^2$ generated by two linearly independent vectors. The determinant of M is defined as the following Gram matrix

$$\det M = \det \begin{pmatrix} \langle \mathbf{v}_1, \mathbf{v}_1 \rangle & \langle \mathbf{v}_1, \mathbf{v}_2 \rangle \\ \langle \mathbf{v}_2, \mathbf{v}_1 \rangle & \langle \mathbf{v}_2, \mathbf{v}_2 \rangle \end{pmatrix},$$

where $\mathbf{v}_1, \mathbf{v}_2$ is any basis for M.

Following the notation of [3], we denote by $\gamma_h(M)$ the quantity

$$\|\mathbf{v}\|^2/(\det M)^{\frac{1}{2}},$$

where $\mathbf{v}$ is a shortest nonzero vector from M.

Let D be the discriminant of $\mathbb{K}$ (we have $D = d$ if $d \equiv 3$ modulo 4 and $D = 4d$ otherwise.) It is known (last paragraph of Subsection 2.1 in [3]) that $\gamma_h(M) = \gamma(M)\sqrt{D}/2$, and hence

$$\gamma_h(M) = \gamma(M)\sqrt{D}/2 \leq \gamma_4\sqrt{D}/2 = \sqrt{D/2}, \tag{7}$$

where $\gamma(M)$ is the ratio of $\|\mathbf{v}\|^2$ and the fourth root of the determinant of M, considered as a $\mathbb{Z}$-lattice of rank 4, and $\gamma_4 = \sqrt{2}$ is the Hermite constant.

Let us define $r(\Lambda)$ as the ratio between the squared length of the shortest rank 1 element of $\phi(\Lambda)$ and that of the shortest rank 2 element in $\phi(\Lambda)$.

Proposition 7. *We have*

$$r(\Lambda) \leq \frac{1}{2}\gamma_h(M)\gamma_h(M'),$$

where M is an $\mathcal{O}$-sublattice of L generated by two linearly independent vectors over $\mathbb{K}$ and and M' is an $\mathcal{O}$-sublattice of L^* generated by two linearly independent vectors over $\mathbb{K}$.

Proof. Indeed, let $\mathbf{v}$ and $\mathbf{w}$ be shortest nonzero vectors from L and L^*, respectively. Also, let ω be a shortest nonzero vector of rank 2 from $\Lambda \cong L \otimes_{\mathcal{O}} L^*$. We have then

$$r(\Lambda) = \frac{\|\mathbf{v}\|^2 \cdot |\mathbf{w}\|^2}{\|\omega\|^2}.$$

Similarly to the rational case (2) we obtain

$$\|\omega\|^2 \geq 2(\det M)^{1/2}(\det M')^{1/2}$$

for some sublattices $M \leq L$ and $M' \leq L^*$ which are spanned by two linearly independent vectors over $\mathbb{K}$ (see Proposition 3.2 from [3] for the details).

Let $\mathbf{v}'$ and $\mathbf{w}'$ be shortest nonzero vectors from M and M', respectively. Clearly we have $\|\mathbf{v}\| \leq \|\mathbf{v}'\|$, and $\|\mathbf{w}\| \leq \|\mathbf{w}'\|$. By putting all these together we obtain

$$r(\Lambda) = \frac{\|\mathbf{v}\|^2 \cdot |\mathbf{w}\|^2}{\|\omega\|^2} \leq \frac{\|\mathbf{v}'\|^2 \cdot |\mathbf{w}'\|^2}{2(\det M)^{1/2}(\det M')^{1/2}} = \frac{1}{2}\gamma_h(M)\gamma_h(M').$$

□

For $d = 1$ by (7) and Proposition 7 we have $r(\Lambda) \leq \frac{1}{2}\sqrt{2} \cdot \sqrt{2} = 1$. Similarly, for $d = 3$ we find that

$$r(\Lambda) \leq \frac{1}{2}\sqrt{\frac{3}{2}}\sqrt{\frac{3}{2}} = \frac{3}{4} < 1.$$

We have obtained the following:

Proposition 8. *For $d = 1$, at least one of the smallest element of $\phi(\Lambda)$ with respect to the Frobenius norm has rank one. For $d = 3$ every smallest element of $\phi(\Lambda)$ has rank one.* $\square$

The following example shows that over the Gaussian rationals it does indeed occur that a shortest nonzero element of Λ has rank 2. Let $d = 1$ let L be $\mathcal{O}$-submodule of $\mathbb{C}^2$ generated by $(1, 0)^T$ and $(\frac{1}{\sqrt{2}}, \frac{i}{\sqrt{2}})^T$ and let $\Lambda = \{A \in M_2(\mathbb{C}) : AL \subseteq L\}$. Then

$$\Lambda = \left\{ \frac{1+i}{2}\begin{pmatrix} a & b \\ c & e \end{pmatrix} : \begin{array}{c} a, b, c, e \in \mathcal{O}, \\ a + c \equiv a + b \equiv b + e \equiv c + e \equiv 0 \bmod (1+i), \\ a + b + c + e \equiv 0 \bmod 2 \end{array} \right\}$$

and the identity matrix is one of the elements of Λ having the smallest Frobenius norm.

Next we outline a direct, elementary proof of inequality (7). Let $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field, $\mathcal{O}$ be the maximal order of $\mathbb{K}$. Suppose further that $\mathcal{O}$ is a principal ideal ring.

Lemma 9. *Let z be any complex number. Then there exists an element $\alpha \in \mathcal{O}$ such that $|z - \alpha| \leq \kappa$, where*

$$\kappa = \begin{cases} \frac{d+1}{4\sqrt{d}} & d \equiv 3 \bmod 4, \\ \frac{\sqrt{d}+1}{2} & \text{otherwise.} \end{cases}$$

The proof is a simple argument from elementary geometry which we omit here. For $d = 1$, we have $\kappa = \frac{\sqrt{2}}{2}$, for $d = 2$, $\kappa = \frac{\sqrt{3}}{2}$, for $d = 3$, $\kappa = \frac{\sqrt{3}}{3}$, for $d = 7$, $\kappa = \frac{2\sqrt{7}}{7}$, for $d = 11$, $\kappa = \frac{3}{\sqrt{11}}$. In these cases $\kappa < 1$. For for $d = 5, 6, 10$ and for $d > 11$ we have $\kappa > 1$. Let us define $\tau = \lfloor \kappa + 1 \rfloor$. Then obviously we have $\kappa/\tau < 1$.

Proposition 10. *Suppose that $\kappa < 1$ holds, and let M be an $\mathcal{O}$-submodule of $\mathbb{C}^2$ generated by two linearly independent vectors over $\mathbb{K}$. Then*

$$\gamma_h(M) \leq \frac{\tau}{\sqrt{1 - \kappa^2}}.$$

Proof. Let $\mathbf{v}, \mathbf{w}$ be a basis of M such that $\mathbf{v}$ is a shortest nonzero vector from M. Such a basis exists because $\mathcal{O}$ is a principal ideal ring. Apply now the preceding lemma for $z = \tau\frac{\langle \mathbf{v}, \mathbf{w}\rangle}{\langle \mathbf{v}, \mathbf{v}\rangle}$. There exists an $\alpha \in \mathcal{O}$ be such that

$$\left| \frac{\langle \mathbf{v}, \mathbf{w}\rangle}{\langle \mathbf{v}, \mathbf{v}\rangle} - \frac{\alpha}{\tau} \right| \leq \frac{\kappa}{\tau}$$

and put $\mathbf{w}' = \mathbf{w} - \frac{\overline{\alpha}}{\tau}\mathbf{v}$. Then $\tau\mathbf{w}' \in M$ and hence $\|\mathbf{w}'\| \geq \frac{\|\mathbf{v}\|}{\tau}$. Furthermore,

$$|\langle \mathbf{v}, \mathbf{w}'\rangle| = \left| \langle \mathbf{v}, \mathbf{w} - \frac{\overline{\alpha}}{\tau}\mathbf{v}\rangle \right| = \left| \langle \mathbf{v}, \mathbf{w}\rangle - \frac{\alpha}{\tau}\langle \mathbf{v}, \mathbf{v}\rangle \right| \leq \frac{\kappa}{\tau}\langle \mathbf{v}, \mathbf{v}\rangle.$$

The Gram determinant does not change if we switch from the basis $\mathbf{v}, \mathbf{w}$ to $\mathbf{v}, \mathbf{w}'$, hence

$$\begin{aligned} \det M &= \det \begin{pmatrix} \langle \mathbf{v}, \mathbf{v} \rangle & \langle \mathbf{v}, \mathbf{w}' \rangle \\ \langle \mathbf{w}', \mathbf{v} \rangle & \langle \mathbf{w}', \mathbf{w}' \rangle \end{pmatrix} = \langle \mathbf{v}, \mathbf{v} \rangle \langle \mathbf{w}', \mathbf{w}' \rangle - |\langle \mathbf{v}, \mathbf{w}' \rangle|^2 \\ &\geq \left(\frac{1}{\tau^2} - \frac{\kappa^2}{\tau^2} \right) \|\mathbf{v}\|^4. \end{aligned}$$

□

For $d = 1$ the Proposition gives $\gamma_h(M) \leq \sqrt{2} = \sqrt{D/2}$. For $d = 2$ we obtain $\gamma_h(M) \leq 2 = \sqrt{D/2}$. For $d = 3$ our bound is $\gamma_h(M) \leq \frac{\sqrt{3}}{\sqrt{2}} = \sqrt{D/2}$. For $d = 7$ the proposition gives $\gamma_h(M) \leq \sqrt{\frac{7}{3}} < \sqrt{\frac{7}{2}} = \sqrt{\frac{D}{2}}$. For these values of d the ring $\mathcal{O}$ is a principal ideal ring, hence we have proved (7).

The improved algorithm when $d = 1$ or $d = 3$

We can achieve an improvement of the algorithm of Section 3 from [5] for $n = 2$ and $d = 1$ or $d = 3$, i.e. for the case of two by two matrices over the Gaussian rationals or over the Eisenstein rationals. These cases of the explicit isomorphism problem occur when one considers parametrization of Del Pezzo surfaces of degree 8, see Section 4 in [4]. Our method may present a viable alternative there to solving norm equations.

Our improvement over the method of [5] is very similar to that of the algorithm over $\mathbb{Q}$. Suppose therefore that $\mathbb{K}$ is either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, and we have as input an algebra $\mathcal{A}$ over $\mathbb{K}$ specified by structure constants. We assume that $\mathcal{A} \cong M_2(\mathbb{K})$. The first four steps of the method in [5] construct a maximal order Λ, an embedding $\phi : \Lambda \to M_2(\mathbb{C})$, a $\mathbb{Z}$ linear embedding Φ of Λ into $\mathbb{R}^8$ which maps an $y \in \Lambda$ to

$$\Phi(y) := (\Re\phi(y), \Im\phi(y)) \in \mathbb{R}^8.$$

The image $\Phi(\Lambda)$ is a full $\mathbb{Z}$ lattice in $\mathbb{R}^8$. Note that the (real) Euclidean norm $\|\Phi(y)\|$ is the same as the Frobenius norm $\|\phi(y)\|$ inherited from $M_2(\mathbb{C})$.

Moreover, the first four steps return a $\mathbb{Z}$ basis $\mathbf{b}_1, \ldots, \mathbf{b}_8$ of $\Phi(\Lambda)$ for which we have

$$\|\mathbf{b}_1\| \cdot |\mathbf{b}_2\| \cdots \|\mathbf{b}_8\| \leq c_8 \det \Phi(\Lambda).$$

From this point on we can simplify the search for a zero divisor. By Proposition 8 it suffices to enumerate[3] the elements of $\Phi(\Lambda)$ which have minimal norm until a zero divisor in Λ is found.

To this end, we generate all integral linear combinations

$$\mathbf{v} = \sum_{i=1}^{8} \alpha_i \mathbf{b}_i,$$

where α_i are integers, $|\alpha_i| \leq c_8$, until a $\mathbf{v}$ is found for which the matrix $y \in \Lambda$ with $\Phi(y) = \mathbf{v}$ is of rank one. The bound on the integers α_i follows from Lemma 6, like in the rational case.

Acknowledgment

We are grateful to Josef Schicho for discussions on the subject.

[3]For $d = 3$ it suffices to find just one element with minimal norm.

References

[1] A.M. Bergé, J. Martinet, Sur un problème de dualité lié aux sphères en géométrie des nombres, *J. of Number theory, 32(1989), 14–42.*

[2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups,* 2nd ed. Springer-Verlag, 1993.

[3] R. Coulangeon, Tensor products of hermitian lattices, *Acta Arithmetica 92 (2000), 115-129.*

[4] W. A. de Graaf, J. Pílniková, J. Schicho, Parametrizing Del Pezzo surfaces of degree 8 using Lie algebras, *Journal of Symbolic Computation 44 (2009), 1–14.*

[5] G. Ivanyos, L. Rónyai and J. Schicho, Splitting full matrix algebras over algebraic number fields, *Journal of Algebra, 354(2012), 211–223.*

[6] Y. Kitaoka, Scalar extensions of quadratic lattices II, *Nagoya Math. J. 67(1977), 159–164.*

[7] Y. Kitaoka, *Arithmetic of quadratic forms,* Cambridge University Press, 1993.

[8] H. W. Lenstra, Jr., Integer programming with a fixed number of variables, *Mathematics of Operations Research, 8(1983), 538–548.*

[9] J. Martinet, *Perfect lattices in Euclidean spaces,* Springer-Verlag, 2003.

[10] J. Milnor and D. Husemoller, *Symmetric bilinear forms,* Springer-Verlag 1973.

[11] I. Reiner, *Maximal orders*, Academic Press, 1975.