BSc Thesis

Small zero divisors in maximal orders of $M_n(\mathbb{Q})$

Ádám Dániel Lelkes

Supervisor: **Lajos Rónyai**
professor
Department of Algebra
Institute of Mathematics
Budapest University of Technology and Economics

2012

Contents

1 Introduction

Let $\mathcal{A}$ be an associative algebra over $\mathbb{Q}$ given by structure constants, which is isomorphic to the full matrix algebra $M_n(\mathbb{Q})$ for some positive integer n. A recent paper of G. Ivanyos, L. Rónyai and J. Schicho [14] focuses on the problem of finding an efficient algorithm which constructs explicitly an isomorphism $\mathcal{A} \to M_n(\mathbb{Q})$.

In order to construct such an isomorphism, we need to find a rank 1 matrix with a small Frobenius norm in a maximal $\mathbb{Z}$-order Λ in $\mathcal{A}$, where the Frobenius norm is inherited from an arbitrary embedding of $\mathcal{A}$ into $M_n(\mathbb{R})$. A maximal $\mathbb{Z}$-order in $\mathcal{A}$ is essentially $M_n(\mathbb{Z})$ transformed by an invertible real matrix. To establish a reasonable time bound for the algorithm, we need to find a tight upper bound for the minimal norm of rank one matrices.

Rónyai et al. proved that there exists a rank one matrix in Λ whose Frobenius norm is less than n. The upper bound for the norm we can obtain by slightly modifying the proof is in fact better: it is the Hermite constant γ_n. Thus a naturally arising question is whether this upper bound is optimal, i.e. if there is an invertible real matrix P such that the minimal Frobenius norm of PAP^{-1} for rank 1 matrices $A \in M_n(\mathbb{Z})$ is γ_n.

We use lattices in Euclidean spaces to examine this problem, thus establishing a firm link between the theory of lattices and the representation theory of algebras. Furthermore, to point out the significance of this problem, let us mention an article by Cremona et al. [8] in which the authors rely on an algorithm to compute an isomorphism of the above mentioned kind explicitly in order to study a group attached to elliptic curves over $\mathbb{Q}$ with the aim of representing the group's elements as genus one normal curves in $\mathbb{P}^{n-1}$. This representation in turn allows searching for rational points on these curves. Thus the topic of our paper is in connection with difficult problems in arithmetic geometry including the Birch and Swinnerton-Dyer conjecture. For the exact nature of this connection we refer the reader to the series articles of Cremona et al. [6], [7], [8]. For more information on the explicit isomorphism problem the reader is referred to [14], [10], [23], [24], [25].

The structure of this thesis is the following:

1. This is the first section. We have already given a brief summary of the problem investigated in this paper; more details are to be found below.

2. In the second section, we introduce the necessary definitions and theorems that we will use throughout this paper.

3. The third section deals with the general case of rank one matrices. In this section we prove that although Hermite's constant is a good upper bound for the norm of rank one matrices in maximal orders, the tight upper bound is the so-called Bergé-Martinet constant. We will see that the two constants are equal in dimension n if there is an autopolar Hermite-critical lattice of rank n.

4. These autopolar Hermite-critical lattices form the topic of the fourth section. There are four of them known so far: in 2, 4, 8 and 24 dimensions. We describe all of them.

5. In the fifth section we examine how fruit stands and checkerboards relate to the Bergé-Martinet-constant in 3 and 5 dimensions, recall the recently proved Kepler conjecture, and describe the 7-dimensional lattice attaining the Bergé-Martinet constant.

6. In the sixth section we consider the case of general singular matrices. We realize that we have been working with tensor products of lattices, and use the results of Steinberg and Kitaoka to decide whether the matrix with the smallest Frobenius norm in a maximal order always has rank one. The answer will be negative in general, but affirmative in small dimensions. We present a stronger version of Kitaoka's theorem in dimensions at most 8.

7. In the seventh section we present the original Ivanyos-Rónyai-Schicho algorithm.

8. The eighth section presents the main application of the results obtained in earlier sections: in small dimensions this presents a substantially improved version of the first algorithm of IRS. Our variant surpasses the

original method in two ways: it has a simpler control structure as it no longer involves jumps, moreover, a better bound is given for the size of the region to be searched.

9. In the ninth section we outline a possible generalization of the problem to algebras over other algebraic number fields.

The main new results of this paper are Theorem 3.2 in Section 3 which states the optimality of the Bergé-Martinet constant; Theorem 6.7 in Section 6 which improves Kitaoka's result in small dimensions; and the improved algorithm described in Section 7.

This thesis is based on the Students' Scientific Conference paper of the same title which was awarded the 1st Prize in the Discrete Mathematics Section and the Special Prize of the President.

2 Preliminaries

First let us explain the title of the paper.

Definition 2.1. *A* central simple algebra *over $\mathcal{A}$ over a field $\mathbb{K}$ is a finite dimensional associative algebra over $\mathbb{K}$ with center $\mathbb{K}$ and with no nontrivial two-sided ideals.*

Definition 2.2. *A ring is called (left, resp. right)* Artinian *if it satisfies the descending chain condition on (left, resp. right) ideals; i.e. if every descending chain of (left, resp. right) ideals eventually stabilizes.*

Theorem 2.3 (Artin and Wedderburn)**.** *Any Artinian semisimple ring R is isomorphic to a direct sum of finitely many full matrix rings over division rings (also called skew fields). In particular, any simple left or right Artinian ring is isomorphic to a full matrix ring over a division ring.*

It follows that every central simple algebra is isomorphic to a full matrix algebra over a division ring D with center $\mathbb{K}$.

Definition 2.4. *An* order *in a central simple algebra $\mathcal{A}$ of dimension n^2 over $\mathbb{Q}$ is a subring $\mathcal{O} \subset \mathcal{A}$ whose additive group is a free abelian group of rank n^2. A* maximal order *$\mathcal{O} \subset \mathcal{A}$ is an order that is not a proper subring of any other order in $\mathcal{A}$.*

It can be shown that every maximal order in $M_n(\mathbb{Q})$ is conjugate to $M_n(\mathbb{Z})$.

Now we introduce lattices and recall some of their important properties. For more details about lattices we refer the reader to [3], [18] and [20].

Definition 2.5. *We call a set $X \subset \mathbb{R}^n$ discrete if for evey $x \in X$ there exists $\varepsilon > 0$ such that $B_\varepsilon(x) \cap X = \{x\}$ (i.e. X has no limit point).*

Definition 2.6. *A* lattice *is a discrete subgroup of the additive group $(\mathbb{R}^n; +)$.*

The simplest example is the lattice of integers $\mathbb{Z}^n$ in $\mathbb{R}^n$.

Definition 2.7. *The* rank *of a lattice L is the dimension of* $\mathrm{Span}(L)$ *as a vector space.*

For example, the rank of $\mathbb{Z}^n$ is clearly n. Every lattice $L \subseteq \mathbb{R}^n$ is isomorphic as a group to $\mathbb{Z}^k$ for some $k \leq n$. If $k = n$, then we speak about *full lattices*.

Definition 2.8. *We call a subset $\mathcal{B}$ of a lattice L a* basis *if each lattice vector can be written uniquely as an integral linear combination of the elements of $\mathcal{B}$; i.e. only linear combinations with integer coefficients are allowed.*

It is easy to show that like vector spaces, every lattice has a basis.

Definition 2.9. *If $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$ is a basis of a full lattice L, then we use the notation $L = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$. Furthermore we call the matrix $M = (\mathbf{b}_1|\mathbf{b}_2|\ldots|\mathbf{b}_n)$ the* generator matrix *for L; we shall say that $|\det M|$ is the determinant of L which we will denote by* $\det L$.

The determinant is sometimes also called the *volume* of the lattice, since it is the volume of the parallelepiped spanned by an arbitrary basis. Note that there are many possible bases and generator matrices for the same lattice, which leads to the following definition:

Definition 2.10. *We say that two lattices are* equivalent*, if they can be transformed into each other by rotation, reflection and/or change of scale.*

We introduce another related matrix to lattices:

Definition 2.11. *The matrix $[\langle \mathbf{b}_i, \mathbf{b}_j \rangle]_{i,j=1}^n$ is the* Gram matrix *of $L = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n)$, its determinant is the* Gram determinant *which is equal to the square of the volume of the lattice.*

We associate a so-called *polar lattice* to every lattice:

Definition 2.12. *If L is a lattice, then $L^* := \{\mathbf{y} \in \mathrm{Span}_{\mathbb{R}}(L) : \forall \mathbf{x} \in L : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}$ is the* polar *(or* dual*) lattice of L. If $L = L^*$, then we say that the lattice L is* autopolar.

Autopolar lattices will play a crucial role in our investigation in 8 and 24 dimensions.

Definition 2.13. *The Euclidean norm of the shortest nonzero vector in a lattice L is called the* first minimum *of L, and is denoted by $\lambda_1(L)$.*

Now we are ready to define Hermite's constant.

Definition 2.14. *The nth* Hermite's constant *is* $\gamma_n := \sup_L \left(\frac{\lambda_1(L)}{(\det L)^{1/n}}\right)^2$, *where L is any lattice of rank n. Furthermore, a lattice L is called* Hermite critical *if* $\left(\frac{\lambda_1(L)}{(\det L)^{1/n}}\right)^2 = \gamma_n$.

Hermite proved that γ_n actually exists. The exact value of γ_n is only known for $n \in \{1, 2, \dots, 8, 24\}$, see the table below.

n	1	2	3	4	5	6	7	8	24
γ_n	1	$\frac{2}{\sqrt{3}}$	$\sqrt[3]{2}$	$\sqrt{2}$	$\sqrt[5]{8}$	$\sqrt[6]{\frac{64}{3}}$	$\sqrt[7]{64}$	2	4

Definition 2.15. *For each positive integer n, let $\omega_n = \pi^{\frac{n}{2}}/\Gamma(1+\frac{n}{2})$ denote the volume of the unit ball in $\mathbb{R}^n$, and let $k(n)$ denote the closest integer to $\frac{5}{3}(\omega_n^{-1})^{\frac{2}{n}}$.*

In order to avoid problems due to scaling, we introduce the following quantity for lattices:

Definition 2.16. $\lambda(L) := \frac{\lambda_1(L)}{(\det L)^{1/n}}$

Thus $\gamma_n = \sup_L(\lambda(L))^2$. As a lower bound of γ_n we have the following theorem.

Theorem 2.17 (Conway and Thompson)**.** *For any dimension n there exists a rank n autopolar lattice L_n such that $\lambda(L_n)^2 \geq k(n)$.*

Corollary 2.18. *For each positive integer n, there exists a rank n autopolar lattice L_n such that*

$$\lambda(L_n)^2 \geq \frac{n}{2\pi e}(1+o(1)) \qquad \text{as } n \to \infty$$

This is also the best known asymptotic lower bound for γ_n; for the proof, see [19], Theorem 9.5.

Now we introduce a quantity similar to Hermite's constant:

Definition 2.19. *We call the supremum of $\lambda(L)\lambda(L^*)$ among rank n lattices the nth* Bergé-Martinet constant*, which is denoted by γ_n'.*

It is probably not surprising that this constant was introduced by Bergé and Martinet [1]. They calculated the exact value of γ'_n for $1 \leq n \leq 4$. For $5 \leq n \leq 7$, the value of γ'_n was determined by C. Poor and D. S. Yuen [22].

After these definitions the reader will understand the theorem from which our question arises:

Theorem 2.20 (Rónyai et al.)**.** *Let* Λ *be a maximal* $\mathbb{Z}$*-order in* $\mathcal{A} = M_n(\mathbb{Q})$*. Then there exists an element* $C \in \Lambda$ *which has rank* 1 *as a matrix, and whose Frobenius norm* $\|C\|$ *is less than* n*.*

A maximal $\mathbb{Z}$-order is essentially $M_n(\mathbb{Z})$ transformed by an invertible real matrix P; i.e. $\Lambda = PM_n(\mathbb{Z})P^{-1}$. In the next section we shall see that in fact the proof of this theorem shows that the theorem holds even if we choose the Hermite constant γ_n instead of n as the upper bound.

Now there is only one step left before we can focus on our actual topic: as the last theorem in this section, we recall Minkowski's convex body theorem.

Theorem 2.21 (Minkowski)**.** *Let* L *be an* n*-rank lattice and* K *a convex subset in* $\mathbb{R}^n$ *which is symmetric around* 0*. If the Lebesgue measure of* K *is at least* 2^n *times greater than* $\det L$*, then* K *contains at least one nonzero lattice point from* L*.*

The proof can be found in [19], Chapter II, §1.

3 The general case

Here we include the full proof of theorem 2.20.

Proof. Let Λ' denote the standard maximal order $M_n(\mathbb{Z})$ in $\mathcal{A}$. The theory of maximal orders in central simple algebras over $\mathbb{Q}$ implies that there exists an invertible real matrix $P \in M_n(\mathbb{R})$ such that it gives us Λ from Λ':

$$\Lambda = P\Lambda' P^{-1}.$$

Set $Q = P/(|\det P|)^{1/n}$. Clearly $Q \in M_n(\mathbb{R})$, $\det Q$ is ± 1 and $QXQ^{-1} = PXP^{-1}$ holds for any $X \in M_n(\mathbb{Q})$. Let ρ denote the left ideal of Λ' consisting of all integer matrices which have 0 everywhere except in the first column. Clearly ρ is a lattice of determinant 1 in the linear space S of all real matrices having nonzeros only in the first column. Now the lattice $L = Q\rho$ will be a sublattice of S, with determinant 1.

We can apply Minkowski's theorem on lattice points in convex bodies to L in S, and to the ball of radius $\sqrt{n}$ in S centered at the zero matrix (we refer here to the Euclidean distance, that is, the Frobenius norm on $M_n(\mathbb{R})$). The volume (calculated in S) of the ball is more than 2^n, as it contains 2^n internally disjoint copies of the n-dimensional unit cube, and more. We infer that there exists an element $B \in \rho$ such that QB is a nonzero matrix whose length is less than $\sqrt{n}$. Clearly B and hence QB is a rank 1 matrix.

Next consider the "transpose" of this argument with Q^{-1} in the place of Q: there exists a nonzero integer matrix B', which is zero everywhere except in the first row, such that $B'Q^{-1}$ is nonzero, and has Euclidean length less than $\sqrt{n}$.

Now

$$C = PBB'P^{-1} = QBB'Q^{-1}$$

meets the requirements of the statement. Indeed, it is in Λ because $BB' \in M_n(\mathbb{Z})$. It has length less than n because the Frobenius norm is submultiplicative:

$$\|C\| = \|(QB)(B'Q^{-1})\| \leq \|QB\| \cdot \|B'Q^{-1}\| < (\sqrt{n})^2 = n.$$

Obviously, C has rank at most 1, as B and B' are of rank 1. Finally, from the shape of B and B' we see, that $BB' \neq 0$, hence $\operatorname{rank} BB' = \operatorname{rank} C = 1$. This finishes the proof. □

First let us observe that we do not actually need Minkowski's convex body theorem for the proof, in fact we can prove a stricter upper bound with a slightly different reasoning.

Theorem 3.1. *Theorem 2.20 holds even with γ_n as an upper bound instead of n.*

Proof. Our task is to find a rank one matrix $C \in QM_n(\mathbb{Z})Q^{-1}$ such that $\|C\| \leq \gamma_n$. The lattice $Q\rho$ has rank n and determinant 1, therefore the shortest nonzero vector must have length less than or equal to $\sqrt{\gamma_n}$. Let v_1 be such a vector. The same holds for $(Q^{-1})^T$: let us denote a vector not longer than $\sqrt{\gamma_n}$ in $(Q^{-1})^T\rho$ by v_2. It follows that the dyadic product of v_1 and v_2 is a rank one matrix whose Frobenius norm is at most γ_n. □

Here Q is to be seen as the generator matrix for the full rank lattice L in $\mathbb{R}^n$; clearly the upper bound can only be optimal if L is Hermite critical. Since the generating matrix of L^* is the transpose of Q^{-1}, it follows that L^* has to be Hermite critical as well. Should there exist a rank n Hermite critical lattice which is autopolar, it is clear that the upper bound is optimal in n dimensions.

We will see that such a matrix does not always exist. This implies that Hermite's constant is not always the optimal upper bound; we can formulate an even stronger version of the above using the Bergé-Martinet constant:

Theorem 3.2. *Let us assume that $\mathcal{A} = M_n(\mathbb{Q})$. Then for every maximal $\mathbb{Z}$-order Λ in $\mathcal{A}$ the minimal Frobenius norm of the rank 1 matrices in Λ is less than or equal to γ'_n. Furthermore, this is the optimal upper bound; i.e.*

$$\sup_{\Lambda \subset \mathcal{A} \text{ max. order}} \min_{C \in \Lambda,\ \operatorname{rank} C = 1} \|C\| = \gamma'_n$$

and there is an invertible real matrix $\hat{Q} \in GL_n(\mathbb{R})$ such that

$$\min_{B \in M_n(\mathbb{Z}),\ \operatorname{rank} B = 1} \|\hat{Q}B\hat{Q}^{-1}\| = \gamma'_n$$

Proof. $\Lambda = QM_n(\mathbb{Z})Q^{-1}$ for some invertible rational matrix Q. After possibly multiplying by a real constant we can assume that $\det Q = \pm 1$, $Q \in M_n(\mathbb{R})$. Every rank one matrix in $M_n(\mathbb{Z})$ is the dyadic product of two vectors $w_1 \in \mathbb{Z}^n$ and $w_2^T \in (\mathbb{Z}^n)^T$. Thus every rank one C matrix in Λ can be written in the form $C = Qw_1 \cdot ((Q^{-1})^T w_2)^T$. Obviously $\|C\| = \|Qw_1\| \cdot \|((Q^{-1})^T w_2)^T\|$.

Again, let ρ denote the left ideal of $M_n(\mathbb{Z})$ consisting of all integer matrices which have 0 everywhere except in the first column. Consider the lattice $L \cong Q\rho$. Then $(Q^{-1})^T$ is the generator matrix for $L^* \cong (Q^{-1})^T\rho$. $\min\limits_{C\in\Lambda}\|C\| = \min\limits_{w_1\in\mathbb{Z}^n}\|Qw_1\| \cdot \min\limits_{w_2\in\mathbb{Z}^n}\|((Q^{-1})^T w_2)^T\|$ is attained by the shortest nonzero vectors in L and L^*, so $\min\limits_{C\in\Lambda}\|C\| = \lambda(Q\rho)\cdot\lambda((Q\rho)^*)$. Therefore

$$\sup_{\Lambda\subset\mathcal{A} \text{ max. order}} \min_{C\in\Lambda,\ \operatorname{rank} C=1}\|C\| \le \sup_{Q\in M_n(\mathbb{R})} \lambda(Q\rho)\cdot\lambda((Q\rho)^*) = \gamma_n'.$$

Moreover, there is a sequence Q_m of invertible rational matrices such that

$$\lim_{m\to\infty} \min_{B\in M_n(\mathbb{Z}),\ \operatorname{rank} B=1}\|Q_m B Q_m^{-1}\| = \gamma_n'.$$

This shows that in general there is no better bound than γ_n'. Also, by multiplying each Q_m by an appropriate real constant, we can assume that $\forall m \in \mathbb{N} : \|Q_m\| = 1$; thus according to the Bolzano-Weierstrass theorem there is a subsequence Q_{m_k} such that $\lim\limits_{k\to\infty} Q_{m_k} = \hat{Q}$ exists. Since matrix multiplication and inverse are continuous as well as the Frobenius norm, it is clear that $\hat{Q}$ is an invertible real matrix and $\min\limits_{B\in M_n(\mathbb{Z}),\ \operatorname{rank} B=1}\|\hat{Q}B\hat{Q}^{-1}\| = \gamma_n'$. □

We remark that this bound remains valid if Q is a real (and not necessarily rational) matrix.

See the table below for the exact value of γ_n' in $1, 2, 3, 4, 5, 6, 7, 8$ and 24 dimensions.

n	1	2	3	4	5	6	7	8	24
γ_n'	1	$\frac{2}{\sqrt{3}}$	$\sqrt{\frac{3}{2}}$	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{\frac{8}{3}}$	$\sqrt{3}$	2	4

The following table contains the differences $\gamma_n - \gamma_n'$ rounded to four decimals:

n	1	2	3	4	5	6	7	8	24
$\gamma_n - \gamma_n'$	0	0	0.0352	0	0.1015	0.0324	0.0794	0	0

In general we have $\gamma'_n \leq \gamma_n$. The Conway-Thompson theorem gives the asymptotic lower bound

$$\frac{n}{2\pi e}(1 + o(1)) \leq \gamma'_n, \qquad \text{as } n \to \infty$$

This appears to be the best lower bound to date on γ_n as well. It is also known that

$$\gamma_n \leq \frac{1.744n}{2\pi e}(1 + o(1)), \qquad \text{as } n \to \infty$$

For the proof, see [3], Chapter 9.

4 Autopolar Hermite critical lattices

In this section we deal with the simplest cases, when there is an autopolar Hermite critical lattice. This is the case in 2, 4, 8 and 24 dimensions. For detailed descriptions of the lattices mentioned in this section and the following sections, see the book of Conway and Sloane [3]; the definitions used for most of the lattices mentioned in this paper are from this excellent book.

In 2 dimension our lattice is the *hexagonal lattice* A_2 in which three nearby points form an equilateral triangle. It has generator matrix

$$M = \begin{pmatrix} \frac{1}{2} & 1 \\ \frac{\sqrt{3}}{2} & 0 \end{pmatrix}$$

Obviously $\lambda(A_2)^2 = \frac{2}{\sqrt{3}}$, and it is easy to see that every two dimensional Hermite critical lattice is equivalent to A_2. Fortunately A_2 is autopolar as well. Furthermore,

$$M^{-1} = \begin{pmatrix} 0 & \frac{2}{\sqrt{3}} \\ 1 & -\frac{1}{\sqrt{3}} \end{pmatrix}$$

Thus we obtain that

$$M \begin{pmatrix} a & b \\ c & d \end{pmatrix} M^{-1} = \begin{pmatrix} \frac{b}{2} + d & \frac{1}{\sqrt{3}}\left(a - \frac{b}{2} + 2c - d\right) \\ \frac{\sqrt{3}}{2} b & a - \frac{b}{2} \end{pmatrix}$$

This matrix has Frobenius norm

$$\left\| M \begin{pmatrix} a & b \\ c & d \end{pmatrix} M^{-1} \right\| = \sqrt{\left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2 + \left(\frac{b}{2} + d\right)^2 + \frac{1}{3}\left(a - \frac{b}{2} + 2c - d\right)^2}$$

Obviously this expression is minimal among $(a, b, c, d) \in \mathbb{Z}^2 \setminus \{(0, 0, 0, 0)\}$ when one element is 1, and the others are 0. So it is easy to see using elementary techniques that γ_2 is an optimal upper bound for the Frobenius norm of MCM^{-1} for arbitrary (not only rank one) $0 \neq C \in M_2(\mathbb{Z})$. Now let us move on to eight dimensions; we will deal with the four dimensional case in the next section.

The 8 dimensional lattice E_8 consists of the points which have the following two properties: (1) every coordinate is in $\frac{1}{2}\mathbb{Z}$ and (2) the sum of the coordinates is an even integer. A generator matrix for E_8 is

$$M = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \end{pmatrix},$$

$\det E_8 = 1$ and $\lambda(E_8)^2 = 2$ which is exactly the Hermite constant γ_8. Furthermore it is not difficult to see that E_8 is autopolar, thus it follows that the upper bound is optimal in 8 dimensions.

The 24 dimensional autopolar Hermite critical lattice was discovered by John Leech in 1965, thus it is called the Leech lattice, and is denoted by Λ_{24}. Its construction is somewhat more complicated than that of E_8; Conway and Sloane describe more than 30 different constructions in [3].

Here we briefly describe one of these constructions which is based on an intuitive idea about lattice packings of spheres. Sphere packings are arrangements of non-overlapping identical spheres; the goal is to find the densest such packing. A natural way to arrange the spheres is to choose lattice points as centers of the spheres; these packings are called lattice packings. The problem of densest sphere packings is still unsolved even in 4 dimensions. In 2 dimensions the hexagonal lattice packing is known to be the densest. In 3 dimensions the problem has recently been solved by Thomas Hales, whose proof involved checking a tremendous amount of individual cases using a computer: the proof is more than a hundred pages long with additional gigabytes of data [12].

An intuitive way to construct lattice packings is to build up the packings in layers (much like stacking oranges) starting from the one-point lattice Λ_0. Then for all $n \geq 1$ let us take all n dimensional lattices with $\lambda_1 = 2$ that have at least one sublattice Λ_{n-1}, and select those of minimal determinant. Any

such lattice is denoted by Λ_n. In some higher dimensional spaces there are several such lattices; in lower dimensions that we are interested in, they are unique.

These lattices are the so-called *laminated lattices*. Λ_1 is the integer lattice $\mathbb{Z}$, $\Lambda_2 \cong A_2$ is the hexagonal lattice which we already know, and Λ_{24} is the Leech lattice.

It can be shown that the Leech lattice is autopolar, $\det \Lambda_{24} = 1$ and $\lambda_1(\Lambda_{24})^2 = 4 = \gamma_{24}$.

5 Pyramids of oranges and checkerboards

We have already seen the generalization of the way greengrocers stack oranges to arbitrary dimensions. As mentioned without proof in the last section, it happens that the lattice 24 dimensional greengrocers would use is Hermite critical and autopolar at the same time. In this section we will stick to lower dimensions.

The laminated lattice Λ_3 is called the *face-centered cubic lattice*. Hales proved that this sphere packing found in the pyramids of oranges on every fruit stand has the greatest density that can be attained. Notwithstanding Hales' proof, this fact is still known as the Kepler conjecture, named after the German astronomer and mathematician who first stated it in 1611 [16].

Here we will use another definition of this lattice that is simpler than the construction of laminated lattices. The *checkerboard lattice* D_n ($n \geq 3$) is a sublattice of $\mathbb{Z}^n$ consisting of the points for which the sum of the coordinates is even; that is, the lattice we obtain by coloring the points of $\mathbb{Z}^n$ alternately red and blue, and taking the red points. A generator matrix for D_n is

$$M = \begin{pmatrix} -1 & 1 & 0 & \cdots & 0 \\ -1 & -1 & 1 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}$$

For $n \in \{3, 4, 5\}$ the checkerboard lattices are equivalent to the laminated lattices Λ_3, Λ_4 and Λ_5, respectively, and they are Hermite critical. A generator matrix for D_n^* is

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1/2 \\ 0 & 1 & \cdots & 0 & 1/2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1/2 \\ 0 & 0 & \cdots & 0 & 1/2 \end{pmatrix}$$

It happens that $D_4 \cong D_4^*$, so the upper bound γ_4 is optimal in four dimensions. In general $\det D_n = 4$, $\lambda_1(D_n) = \sqrt{2}$, $\det D_n^* = \frac{1}{4}$, and $\lambda_1(D_n^*) = 1$ for $n \geq 4$.

Now let us consider the case of our three dimensional world. Here the polar lattice D_3^* is the *body-centered cubic lattice*. A simple definition of this lattice is that it consists of the points with all even or all odd coordinates, yielding the generator matrix

$$M = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

The body-centered cubic lattice is the solution for the *covering problem* in 3 dimensions. The covering problem asks for the most economical way to cover $\mathbb{R}^n$ with identical overlapping spheres. We do not need the exact definition here, we refer again the curious reader to [3]. In addition, body-centered cubic lattices are very common in the crystal structure of metals such as iron, chromium or sodium.

The problem is that although D_3 is Hermite critical, D_3^* is not: $\lambda(D_3*) = \sqrt{3}$, so the smallest norm we obtain for a rank one matrix using D_3 is $\sqrt{\frac{3}{2}}$. $\sqrt{\frac{3}{2}} \approx 1.22474$, $\gamma_3 = \sqrt[3]{2} \approx 1.25992$.

One intuitive idea that comes to mind is that we should try to move D_3 closer to its dual by constructing a lattice that is "between" D_3 and D_3^*. In fact, Conway and Sloane managed to construct such a lattice [4]. This lattice is called the *central centered-cuboidal lattice*, and it is the autopolar lattice in 3 dimensions for which $\lambda(L)^2$ is maximal. Unfortunately this maximum is $\frac{1}{2} + \sqrt{\frac{1}{2}} \approx 1.20711$, so from our viewpoint this lattice is weaker than D_3.

We have seen that the optimal upper bound is the Bergé-Martinet constant, which is equal to Hermite's constant if there is an autopolar Hermite critcal lattice. It turns out that in three dimensions D_3 attains the Bergé-Martinet constant, as does D_5 in five dimensions. The value of the constant for 3 and 5 dimensions is $\sqrt{\frac{3}{2}}$ and $\sqrt{2}$, respectively. More generally, $\forall n > 3$: $\lambda(D_n)\lambda(D_n^*) = \sqrt{2}$.

In six and seven dimensions, the optimal lattices are E_6 and E_7. These are both sublattices of the already familiar E_8: E_7 consists of the vectors in E_8 that are perpendicular to any minimal vector $v \in E_8$, whereas the vectors in E_6 are those that are perpendicular to any A_2-sublattice V in E_8. $\gamma_6' = \sqrt{\frac{8}{3}}$ and $\gamma_7' = \sqrt{3}$.

After enumerating all these cases, we can summarize the results as follows.

Theorem 5.1. *The lowest upper bound for the minimal norm of rank one matrices in maximal orders of $M_n(\mathbb{Q})$ for $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 24\}$ and the corresponding lattices attaining the bound are the following:*

n	1	2	3	4	5	6	7	8	24
bound	*1*	$\frac{2}{\sqrt{3}}$	$\sqrt{\frac{3}{2}}$	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{\frac{8}{3}}$	$\sqrt{3}$	2	4
lattice	$\mathbb{Z}$	A_2	D_3	D_4	D_5	E_6	E_7	E_8	Λ_{24}

6 General singular matrices

So far we have only treated rank one matrices. However, it is natural to ask whether a singular matrix with minimal norm in Λ has always rank one. Furthermore, if we consider all the singular matrices, will the lattices attaining the maximum of minimal norms remain the same? In the simple case of two dimensions, we have already seen that the hexagonal lattice is optimal not only for rank one matrices.

In order to answer this question, we have to understand the structure of the lattice QAQ^{-1}, where Q is a nonsigular rational (or more generally real) matrix, and A runs over the elements of $M_n(\mathbb{Z})$. The key observation is that this lattice is in fact the tensor product of the lattice generated by Q and its polar lattice.

Let L and M be two lattices in $\mathbb{R}^m$ and $\mathbb{R}^n$, respectively. Then $L \otimes_{\mathbb{Z}} M$ embeds naturally in $\mathbb{R}^m \otimes_{\mathbb{R}} \mathbb{R}^n$. This allows us 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 is the same as the Frobenius norm on $M_{m,n}(\mathbb{R})$.

Thus our question is whether $\lambda(L \otimes L^*) = \lambda(L)\lambda(L^*)$ holds. (Obviously $\lambda(L \otimes L^*) \leq \lambda(L)\lambda(L^*)$.) The following theorem is a direct application of the Conway-Thompson theorem, which answers our question in general.

Theorem 6.1 (Steinberg)**.** *For any dimension $n \geq 292$ there exists a lattice L so that $\lambda(L \otimes L^*) < \lambda(L)\lambda(L^*)$.*

A proof for this theorem can be found in [19], Chapter II, §9; here we include a slightly modified version of this proof which is more in accordance with our terminology.

Proof. $L \otimes L^* \cong \mathrm{Hom}(L, L) \cong \{QAQ^{-1} : A \in M_n(\mathbb{Z})\}$, where Q is the gen-

erator matrix for L. Let us choose $A = I$ (I denotes the identity matrix). $\|QIQ^{-1}\| = \sqrt{n}$, hence $\lambda_1(L \otimes L^*) \leq \sqrt{n}$.

Now let us apply the theorem of Conway and Thompson. For each positive integer n, there is a rank n autopolar lattice L_n such that $\lambda(L_n)^2 \geq \frac{n}{2\pi e}(1+o(1))$ as $n \to \infty$, which is greater than $\sqrt{n}$ for sufficiently large n.

More precisely, for $n \geq \lceil (2\pi e)^2 \rceil = 292$, computation shows that $k(n) > \sqrt{n}$. In this case $\lambda(L \otimes L^*) \leq \sqrt{n} < k(n) \leq \lambda(L)\lambda(L^*)$. □

We have obtained that in general rank one matrices are not optimal. However, in small dimensions, the smallest zero divisors have rank one. The following definitions were introduced by Y. Kitaoka [17].

Definition 6.2. *We say that a lattice L is of* E-type *if every minimal 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.*

Definition 6.3. $\kappa := \max\{k \in \mathbb{N} : ((\gamma_r \geq \sqrt{r}) \wedge (r \leq k)) \implies r = 1\}$.

Kitaoka proved that $\kappa \geq 42$ ([17], §1, Lemma 2). Theorem 1 of the same section has interesting consequences.

Theorem 6.4 (Kitaoka)**.** *If L is a lattice of rank at most κ, then L is of E-type.*

Corollary 6.5. *In any dimension $n \leq 42$ and any maximal order $\Lambda \subset M_n(\mathbb{Q})$ the matrices with the smallest Frobenius norm in Λ are of rank one.*

Proof. Let Λ be given by the transformation matrix Q. $Q\rho$ is a rank n lattice (ρ as in the proof of Theorem 2.20), hence it is of E-type. Since $\Lambda \cong Q\rho \otimes (Q\rho)^*$, the matrices of minimal norm in Λ are dyadic products of vectors in $Q\rho$ and $(Q\rho)^*$. □

After obtaining that in at most 42 dimensions the smallest zero divisors in any maximal order Λ have rank one, we might wonder if there is a positive constant C such that every singular matrix of rank at least two has Frobenius norm at least C times the minimal norm in Λ. In order to obtain such a constant C, we use a modified version of Kitaoka's proof for Theorem 6.4.

Lemma 6.6 (Kitaoka)**.** *Let A, B be positive definite real symmetric matrices of degree n; then we have* $\mathrm{Tr}(AB) \geq n \sqrt[n]{\det A} \sqrt[n]{\det B}$.

Proof. Put $B = P^T DP$, where D is diagonal and P is orthogonal. Let $a_1, \ldots, a_n$ and $d_1, \ldots, d_n$ be diagonals of PAP^T and D, respectively. Then

$$\mathrm{Tr}(AB) = \mathrm{Tr}(AP^T DP) = \mathrm{Tr}(PAP^T D) = \sum_{i=1}^{n} a_i d_i$$

The arithmetic-geometric mean inequality implies that

$$\sum_{i=1}^{n} a_i d_i \geq n \sqrt[n]{\prod_{i=1}^{n} (a_i d_i)} = n \sqrt[n]{\det B} \sqrt[n]{\prod_{i=1}^{n} a_i}$$

By using Hadamard's inequality for positive definite matrices we obtain that

$$n \sqrt[n]{\det B} \sqrt[n]{\prod_{i=1}^{n} a_i} \geq n \sqrt[n]{\det B} \sqrt[n]{\det(PAP^T)} = n \sqrt[n]{\det A} \sqrt[n]{\det B}.$$

□

Theorem 6.7. *Let L be a lattice of rank at most* 8*. Then for any lattice M, every tensor of rank at least two in $L \otimes M$ has norm at least $\sqrt{\frac{3}{2}} \lambda_1(L \otimes M)$.*

Proof. Let $\mathbf{v}$ be a tensor in $L \otimes M$. Then $\mathbf{v} = \sum_{i=1}^{r} \mathbf{x}_i \otimes \mathbf{y}_i$, where $2 \leq r \leq 8$, and $\mathbf{x}_i \in L$, $\mathbf{y}_i \in L^*$ for every $i \in \{1, 2, \ldots, r\}$. In these representations of $\mathbf{v}$ we take one with minimal r. Then $\{\mathbf{x}_1, \ldots, \mathbf{x}_r\}$ and $\{\mathbf{y}_1, \ldots, \mathbf{y}_r\}$ are linearly independent sets in L and M, respectively. Noting

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

and using Lemma 6.6 we get $\|\mathbf{v}\|^2 \geq r \left(\det[\langle \mathbf{x}_i, \mathbf{x}_j \rangle] \cdot \det[\langle \mathbf{y}_i, \mathbf{y}_j \rangle]\right)^{1/r}$.

Now let us assume that $\|\mathbf{v}\|^2 < \frac{3}{2} \lambda_1(L \otimes M)^2$. It follows that $\|\mathbf{v}\|^2 < \frac{3}{2} (\lambda_1(L) \lambda_1(M))^2 \leq \frac{3}{2} (\lambda_1(\mathcal{L}(\mathbf{x}_1, \ldots, \mathbf{x}_r)) \lambda_1(\mathcal{L}(\mathbf{y}_1, \ldots, \mathbf{y}_r)))^2$. Therefore

$$r < \frac{3}{2} \cdot \frac{(\lambda_1(\mathcal{L}(\mathbf{x}_1, \ldots, \mathbf{x}_r)))^2}{(\det[\langle \mathbf{x}_i, \mathbf{x}_j \rangle])^{1/r}} \cdot \frac{(\lambda_1(\mathcal{L}(\mathbf{y}_1, \ldots, \mathbf{y}_r)))^2}{(\det[\langle \mathbf{y}_i, \mathbf{y}_j \rangle])^{1/r}} \leq \frac{3}{2} \gamma_r^2,$$

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 the Gram matrices for $\mathcal{L}(\mathbf{x}_1, \ldots, \mathbf{x}_r)$ and $\mathcal{L}(\mathbf{y}_1, \ldots, \mathbf{y}_r)$, respectively. On the other hand, $\min_{2 \leq r \leq 8} r/\gamma_r^2 = \frac{3}{2}$, hence we have $r = 1$. □

By choosing $M = L^*$ we obtain that the constant C we were looking for is at least $\sqrt{\frac{3}{2}}$. In fact, even though we did not assume in the proof that $M = L^*$, $C = \sqrt{\frac{3}{2}}$ is tight in the following sense: there exists a lattice L with $\operatorname{rank} L \leq 8$ such that the minimal norm among tensors of rank at least two in $L \otimes L^*$ is exactly $C\lambda_1(L \otimes L^*)$. This lattice is the hexagonal lattice which attains the Hermite constant $\gamma_2 = \frac{2}{\sqrt{3}}$. Computation shows that the minimal norm among rank two tensors in $A_2 \otimes A_2^*$ is $\sqrt{2} = \sqrt{\frac{3}{2}} \cdot \frac{2}{\sqrt{3}}$.

We remark that a little bit better C value is possible in the practically interesting range $3 \leq r \leq 8$.

7 The original IRS algorithm

Now we describe the original Ivanyos-Rónyai-Schicho algorithm from [14]. For the proofs of the preceding lemmas we refer the reader to [14].

Lemma 7.1. *Let $X \in M_n(\mathbb{C})$ be a matrix such that $\det X$ is an integer, and $\|X\| < \sqrt{n}$. Then X is a singular matrix.*

Lemma 7.2. *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*

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

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

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

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

The input of the algorithm is an associative algebra $\mathcal{A}$ given by structure constants, which is isomorphic to $M_n(\mathbb{Q})$. We intend to find a rank one element.

1. Use the Ivanyos-Rónyai algorithm [15] to construct a maximal order Λ in $\mathcal{A}$. This is a polynomial time ff-algorithm[1].

2. Compute an embedding of $\mathcal{A}$ into $M_n(\mathbb{R})$. One uses here the the deterministic polynomial time algorithm obtained via the derandomization by de Graaf and Ivanyos [11] of the Las Vegas algorithm of Eberly [9]. 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.

[1]For the definiton of ff-algorithms we refer the reader to [14]. It performs well if the integers to be factored are not very big. The method has been implemented in Magma by de Graaf.

3. Compute a rational approximation A of our basis B of Λ with precision $q_0(B, \frac{1}{2}, 2^{\frac{m-1}{2}})$ (see Section 2 in [2] for the definition of the precision parameter q_0). One can use here the Algorithm of Schönhage[2] [26].

4. Compute a reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_m$ of the lattice $\Lambda \subset \mathbb{R}^m$ by applying the LLL algorithm to A. The value of c_m is $(\gamma_m)^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}$ from the approximate version of the LLL algorithm developed by Buchmann, see Corollary 4 of [2].

5. If some of the basis elements $\mathbf{b}_i$ is a zero divisor in $\mathcal{A}$, then there are two cases. If $\operatorname{rank} \mathbf{b}_i = 1$, then we are done and stop with the output $C := \mathbf{b}_i$. Otherwise, if $1 < \operatorname{rank} \mathbf{b}_i < n$, then we compute the the right identity element e of the left ideal $\mathcal{A}\mathbf{b}_i$ by solving the straightforward system of linear equations, set $\mathcal{A} := e\mathcal{A}e$ and go back to Step 1.

6. At this point we know that $|\mathbf{b}_i| \geq \sqrt{n}$ holds for every i. Generate all integral linear combinations $C' = \sum_{i=1}^{m} \gamma_i \mathbf{b}_i$, where the γ_i are integers, $|\gamma_i| \leq c_m \frac{n}{|\mathbf{b}_i|} \leq c_m \sqrt{n}$ until a C is found with $\operatorname{rank} C = 1$. Output this C.

This algorithm is correct and runs in ff-polynomial time, the proof can be found in [14]. Nevertheless, the jumps in Step 5 make the algorithm somewhat complicated; we shall see in the next section that these jumps can be avoided in small dimensions.

[2]For a more recent method see [21].

8 The IRS algorithm in small dimensions

In this section we describe the improved Ivanyos-Rónyai-Schicho algorithm in small dimensions.

The improved IRS algorithm consists of the following steps:

1. Use the Ivanyos-Rónyai algorithm [15] to construct a maximal order Λ in $\mathcal{A}$. This is a polynomial time ff-algorithm.

2. Compute an embedding of $\mathcal{A}$ into $M_n(\mathbb{R})$. One uses here the deterministic polynomial time algorithm obtained via the derandomization by de Graaf and Ivanyos [11] of the Las Vegas algorithm of Eberly [9]. 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 precision $q_0(B, \frac{1}{2}, 2^{\frac{m-1}{2}})$ (see Section 2 in [2] for the definition of the precision parameter q_0). One can use here the algorithm of Schönhage [26].

4. Compute a reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_m$ of the lattice $\Lambda \subset \mathbb{R}^m$ by applying the LLL algorithm to A. The value of c_m is $(\gamma_m)^{\frac{m}{2}} \left(\frac{3}{2}\right)^m 2^{\frac{m(m-1)}{2}}$ from the approximate version of the LLL algorithm developed by Buchmann, see Corollary 4 of [2].

5. Let us assume that $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \ldots \|\mathbf{b}_n\|$. Generate all integral linear combinations $C' = \sum_{i=1}^m \alpha_i \mathbf{b}_i$, where α_i are integers, $|\alpha_i| \leq c_m \frac{\min\{\gamma'_n, \|\mathbf{b}_1\|\}}{\|\mathbf{b}_i\|}$ until a C is found with $\operatorname{rank} C = 1$. Output this C.

Theorem 8.1. *This algorithm is correct in dimensions $n \leq 42$. Moreover, the algorithm runs in ff-polynomial time.*

Proof. The original IRS algorithm includes an extra step between Steps 4 and 5: if there is a zero divisor $\mathbf{b}_i$ among the basis elements, and $\operatorname{rank} \mathbf{b}_i > 1$, then we compute the right identity element e of the left ideal $\mathcal{A}\mathbf{b}_i$ by solving the

straightforward system of linear equations, set $\mathcal{A} := e\mathcal{A}e$ and go back to Step 1.

The reason we have to jump back possibly several times in Step 5 is that we need to have a lower bound for the norm of the vectors $\mathbf{b}_i$ in order to obtain a good upper bound for the coefficients α_i. (We obtain that $\|\mathbf{b}_i\| \geq \sqrt{n}$ holds for every i in Step 5 according to Lemma 7.1.)

However, according to the results of Kitaoka we know that in at most 42 dimensions if there is a matrix $\mathbf{b}_i$ of rank at least two in the maximal order Λ, then there must be a rank one matrix with norm less than $\|\mathbf{b}_i\|$. Thus for the vector $\mathbf{v}$ in Lemma 7.2 we have the bound $\|\mathbf{v}\| < \|\mathbf{b}_i\|$; hence by using Theorem 3.2 as well we have $|\alpha_i| \leq c_m \frac{\min\{\gamma'_n, \|\mathbf{b}_1\|\}}{\|\mathbf{b}_i\|} \leq c_m$.

This means that using the results of the previous sections, we obtain that for $n \leq 42$ there is no need for this extra step, and the upper bound for $|\alpha_i|$ is $c_m \frac{\min\{\gamma'_n, \|\mathbf{b}_1\|\}}{\|\mathbf{b}_i\|}$. □

Furthermore, Theorem 6.7 implies that whenever we have a matrix $\mathbf{b}_i$ of rank r where $2 \leq r \leq 8$ it follows that there exists a rank one matrix with Frobenius norm at most $\sqrt{\frac{\gamma_r^2}{r}}\|\mathbf{b}_i\|$. For small $\|\mathbf{b}_i\|$ this further reduces the size of the region to be searched.

For $n > 42$, we know that $|\alpha_i| \leq c_m \frac{\gamma'_n}{\|\mathbf{b}_i\|} \leq c_m \frac{\gamma'_n}{\sqrt{n}}$. It follows that as $n \to \infty$,

$$|\alpha_i| \leq c_m \frac{\frac{n}{\pi e}(1 + o(1))}{\sqrt{n}} = c_m \frac{\sqrt{n}}{\pi e}(1 + o(1))$$

9 Hermitian lattices

In the original article of Ivanyos, Rónyai and Schicho the IRS algorithm was extended to the general case of algebraic number fields. In this section, based on [5], we try to generalize our results as well. First, some definitions.

Definition 9.1. *An* algebraic number field *is a finite field extension of* $\mathbb{Q}$.

Definition 9.2. *An algebraic number field of degree* 2 *over* $\mathbb{Q}$ *is called a* quadratic field.

It is easy to show that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

Definition 9.3. *The quadratic field* $\mathbb{Q}(\sqrt{d})$ *is called a* real quadratic field *if* $d > 0$*; for* $d < 0$ *it is called an* imaginary quadratic field.

It can be shown that there is a unique maximal order in a number field, the ring of algebraic integers contained in the field. Let $\mathcal{O}_{\mathbb{K}}$ denote this maximal order of the algebraic number field $\mathbb{K}$. $\mathcal{O}_{\mathbb{K}}$ is a free $\mathbb{Z}$-module, and thus it has a basis as a $\mathbb{Z}$-module, which we call an *integral basis*.

Definition 9.4. *Let* $\mathbb{K}$ *be an algebraic number field and let* $\mathcal{O}_{\mathbb{K}}$ *denote its maximal order. Let* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *be an integral basis of* $\mathcal{O}_{\mathbb{K}}$ *and let* $\sigma_1, \ldots, \sigma_n$ *be the distinct* $\mathbb{Q}$*-homomorphisms from* $\mathbb{K}$ *to* $\mathbb{C}$*. The* discriminant *of* $\mathbb{K}/\mathbb{Q}$ *is* $\Delta_{\mathbb{K}} := (\det[\sigma_i(\mathbf{b}_j)])^2$.

Theorem 9.5. *The discriminant of a quadratic number field* $\mathbb{Q}(\sqrt{d})$ *is* d *if* $d \equiv 1 \pmod 4$*,* $4d$ *otherwise. [13]*

Definition 9.6. *Let* V *be a finite dimensional vector space over* $\mathbb{K}$ *endowed with a positive definite Hermitian form* $\langle \cdot, \cdot \rangle$*. A* Hermitian lattice *in* V *is a finitely generated* $\mathcal{O}_{\mathbb{K}}$*-submodule of* V *containing a* $\mathbb{K}$*-basis of* V.

Definition 9.7. *The* Hermitian dual *of a Hermitian lattice* L *is* $L^* := \{\mathbf{y} \in V : \forall x \in V : \langle x, y \rangle \in \mathcal{O}_{\mathbb{K}}\}$.

Definition 9.8. *Let R be an integral domain and let F be its field of fractions (i.e. the smallest field in which it can be embedded). A* fractional ideal *of R is an R-submodule $\mathfrak{f}$ of F for which there is an element $b \in R$ such that $b\mathfrak{f}$ is an ideal in R.*

Let $\bar{}$ denote the non-trivial Galois-automorphism of the imaginary quadratic field $\mathbb{K}$. Once we have an embedding of $\mathbb{K}$ into $\mathbb{C}$, this corresponds to the complex conjugation.

Definition 9.9. *Let $L = \mathfrak{a}_1\mathbf{e}_1 \oplus \ldots \mathfrak{a}_n\mathbf{e}_n$, where $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a $\mathbb{K}$-basis of V, $n = \dim V$, and $\mathfrak{a}_i$s are fractional ideals in $\mathbb{K}$. The principial ideal $\delta_L := \det[\langle \mathbf{e}_i, \mathbf{e}_j \rangle] \prod_{i=1}^{n} \mathfrak{a}_i\bar{\mathfrak{a}}_i$ is the* discriminant *of L. d_L denotes δ_L's unique non-negative generator in $\mathbb{Q}$.*

Hermitian lattices of rank n over a quadratic number field can be considered as $\mathbb{Z}$-lattices of rank $2n$ by setting $\langle \mathbf{x}, \mathbf{y} \rangle_{\mathbb{Z}} := \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\langle \mathbf{x}, \mathbf{y} \rangle)$. Then $\det L = |\Delta_{\mathbb{K}}|^n (d_L)^2$ holds.

We can introduce these definitions in the case of quaternion algebras as well.

Definition 9.10. *A* quaternion algebra *over a field $\mathbb{K}$ is a central simple algebra H of dimension 4 over $\mathbb{K}$.*

Let H denote a quaternion algebra over $\mathbb{Q}$. The conjugation in H is denoted by $\bar{}$. Let $\mathcal{M}$ denote a maximal order in H.

Definition 9.11. *Let V be a free left H-module of finite rank endowed with a positive definite Hermitian form $\langle \cdot, \cdot \rangle$. A* left $\mathcal{M}$-lattice *in V is a finitely generated $\mathcal{M}$-submodule of V containing a H-basis of V.*

Definition 9.12. *The* Hermitian dual *of a left $\mathcal{M}$-lattice L is $L^* := \{\mathbf{y} \in V : \forall x \in V : \langle x, y \rangle \in \mathcal{M}\}$.*

Now we will define the first minimum and the related invariants for Hermitian lattices.

Definition 9.13. $\lambda_1(L) := \min_{\mathbf{x} \in L \setminus \{\mathbf{0}\}} \langle \mathbf{x}, \mathbf{x} \rangle$ *is the* first minimum *of L.*

Definition 9.14. $\lambda(L) := \frac{\lambda_1(L)}{d_L^{1/n}}$. $\gamma_n := \sup_{L \subset V} (\lambda(L))^2$.

In the quadratic case we have $\lambda(L) = \frac{1}{2}\sqrt{\Delta_{\mathbb{K}}}\lambda_{\mathbb{Z}}(L)$.

In the case of imaginary quadratic fields, the definition of the tensor product of two Hermitian lattices is essentially the same as in the case of $\mathbb{Q}$. In contrast, the quaternionic case is more complicated.

Definition 9.15. *Let W be a free left H-module. $\langle \cdot, \cdot \rangle_W$ is called a* left sesquilinear form *if*

$$\langle \alpha \mathbf{x} + \beta \mathbf{y}, \mathbf{z} \rangle_W = \alpha \langle \mathbf{x}, \mathbf{z} \rangle_W + \beta \langle \mathbf{y}, \mathbf{z} \rangle_H$$

and

$$\langle \mathbf{x}, \alpha \mathbf{y} + \beta \mathbf{z}, \rangle_W = \langle \mathbf{x}, \mathbf{y} \rangle_W \bar{\alpha} + \langle \mathbf{x}, \mathbf{z} \rangle_H \bar{\beta}$$

holds. Right sesquilinear forms for free right H-modules can be defined in an analogous way.

If V is a free right H-module endowed with a right sesquilinear form and W is a free left H-module endowed with a left sesquilinear form then the tensor product $V \otimes_H W$ is well defined. However, because H is not commutative, there is no well defined sesquilinear form $\langle \cdot, \cdot \rangle$ on $V \otimes_H W$ that satisfies

$$\langle \mathbf{x} \otimes \mathbf{y}, \mathbf{z} \otimes \mathbf{w} \rangle = \langle \mathbf{x}, \mathbf{z} \rangle_V \langle \mathbf{y}, \mathbf{w} \rangle_W.$$

Nevertheless, we can define a $\mathbb{Q}$-linear form $\langle \cdot, \cdot \rangle$ on $V \otimes W$ the following way:

$$\langle \mathbf{x} \otimes \mathbf{y}, \mathbf{z} \otimes \mathbf{w} \rangle := \mathrm{tr}(\langle \mathbf{x}, \mathbf{z} \rangle_V \langle \mathbf{y}, \mathbf{w} \rangle_W).$$

Corollary 3.4 of [5] states a splitness criterion for shortest vectors in the tensor product of Hermitian lattices which is similar to Kitaoka's theorem.

Theorem 9.16 (Coulangeon)**.** *Let L be a Hermitian lattice. Set $r_{\mathbb{K}} = \sup\{r > 1 : \gamma_r^2/r < 1\}$. If $\mathrm{rank} L \leq r_{\mathbb{K}}$, then every minimal vector of $L \otimes M$ is of the form $\mathbf{x} \otimes \mathbf{y}$ for any Hermitian lattice M.*

As an example at the end of Section 3 in [5] it is mentioned that $r_{\mathbb{Q}(\sqrt{-3})} \geq 4$. The maximal order of $\mathbb{Q}(\sqrt{-3})$ is the ring of Eisenstein integers, complex

numbers of the form $a + b\omega$ where a and b are integers and ω is a primitive cube root of unity. The Eisenstein integers form a hexagonal lattice in the complex plane.

We refer the reader to the IRS article for the generalization of the original IRS algorithm to algebraic number fields. We note that the algorithm uses the existence of an isomorphism $\psi : \mathcal{A} \to M_n(\mathbb{K})$ such that the image of a maximal order Λ in $\mathcal{A}$ is of the form

$$\Lambda' := \psi(\Lambda) = \begin{pmatrix} R & \cdots R & J^{-1} \\ \vdots & \ddots & \vdots \\ R & \cdots R & J^{-1} \\ J & \cdots J & R \end{pmatrix},$$

where J is a fractional ideal of R in $\mathbb{K}$. (This notation means that Λ' consists of all matrices with elements belonging to the designated sets.) This structure is exactly the tensor product of a Hermitian lattices and its dual, therefore the splitness criterion of Coulangeon can be used in a similar way as we used Kitaoka's theorem for the simpler case of $\mathbb{Q}$.

Thus, for example, in the case of $\mathbb{Q}(\sqrt{-3})$ the IRS algorithm can be simplified in dimensions at most 4. However, for the field of Gaussian rationals, $\mathbb{Q}(\sqrt{-1})$, Coulangeon's theorem is trivial since $r_{\mathbb{Q}(\sqrt{-1})} = 1$.

Note that Theorem 9.16 holds both in the imaginary quadratic and quaternionic cases. Thus by elaborating further it might be possible to extend our results to the quaternion case as well.

10 Concluding remarks

This research was motivated by an algorithmic problem: the task of finding rank one elements in full matrix algebras over $\mathbb{Q}$ which are given by structure constants. We started out with a theorem from the paper of Ivanyos, Rónyai and Schicho [14] which led to questions related to lattices and their invariants such as the Hermite and the much more recent Bergé-Martinet constant. We have shown that the latter gives the best possible bound in Theorem 3.2. Also we collected information on small dimensional extremal lattices relevant to our problem. By using a surprising result of Kitaoka on tensor products of lattices, we improved and simplified the IRS algorithm in small dimensions. Also, via extending Kitaoka's approach we obtained a tool for possible further improvement.

There are several relevant open questions and possible ways for generalization. We propose the following problems for further research:

1. The next step would be to examine thoroughly the case of Hermitian lattices and see if it is possible to improve the IRS algorithm even where Coulangeon's theorem does not help.

2. One could try to establish Kitaoka-type bounds for the special case $M = L^*$ with the Bergé-Martinet constant in the place of the Hermite-constant.

3. Although not in direct connection with our goals, it is nevertheless an interesting question whether Theorem 6.1 implies that there are singular matrices with a norm smaller than the norm of the smallest rank one matrix in sufficiently large dimensions.

Acknowledgement

I would like to express my sincere gratitude to my advisor, Lajos Rónyai for his supervision and guidance throughout this work. I am also thankful to Andor Szabó for the final proofreading.

References

[1] AM. Bergé and J. Martinet, "Sur un problème de dualité lié aux sphères en géométrie des nombres", *J. Number Theory* **32** (1989), 14–42.

[2] J. Buchmann, "Reducing lattice bases by means of approximations", in: *Algorithmic number theory*, LNCS 877, Springer-Verlag (1994), 160–168.

[3] J. H. Conway and N. J. A. Sloane, "Sphere Packings, Lattices and Groups", 2nd ed. *Springer* (1993).

[4] J. H. Conway and N. J. A. Sloane, "On Lattices Equivalent to their Duals", *J. Number Theory* **48** (1994), 373–382.

[5] R. Coulangeon, "Tensor products of hermitian lattices", *Acta Arithmetica* **92** (2000), 115-130.

[6] J. Cremona, T. Fisher, C. O'Neil, D. Simon and M. Stoll, "Explicit n-descent on elliptic curves. I. Algebra", *J. Reine Angew. Math.* **615** (2008), 121–155.

[7] J. Cremona, T. Fisher, C. O'Neil, D. Simon and M. Stoll, "Explicit n-descent on elliptic curves. II. Geometry", *J. Reine Angew. Math.* **632** (2009), 63–84B.

[8] J. Cremona, T. Fisher, C. O'Neil, D. Simon and M. Stoll, "Explicit n-descent on elliptic curves. III. Algorithms", *arXiv:1107.3516v1 [math.NT]* (2011).

[9] W. M. Eberly, "Decompositions of algebras over $\mathbb{R}$ and $\mathbb{C}$", *Computational Complexity*, **1** (1991), 207-230.

[10] W. A. de Graaf, M. Harrison, J. Pílniková, J. Schicho, "A Lie algebra method for rational parametrization of Severi-Brauer surfaces", *Journal of Algebra*, **303** (2006), 514–529.

[11] W. A. de Graaf, G. Ivanyos, "Finding maximal tori and splitting elements in matrix algebras", In: F. van Oystaeyen, M. Saorin (eds.), *Interactions*

Between Ring Theory and Representations of Algebras, (Proc. Euroconference in Murcia, 1998), *Lecture Notes in Pure and Applied Mathematics* **210**, Marcel Dekker (2000), 95–105.

[12] T. C. Hales, "A proof of the Kepler conjecture", *Annals of Mathematics. Second Series* **162** (3) (2005), 1065–1185.

[13] K. Ireland and M. Rosen, "A classical introduction to modern number theory", *Springer* (1982).

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

[15] G. Ivanyos, L. Rónyai, "Finding maximal orders in semisimple algebras over" $\mathbb{Q}$, *Comput. complexity*, **3** (1993), 245–261.

[16] J. Kepler, "Strena seu de nive sexangula" (1611).

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

[18] J. Martinet, "Perfect Lattices in Euclidean Spaces", *Springer* (2003).

[19] J. Milnor and D. Husemoller, "Symmetric bilinear forms", *Springer* (1973).

[20] P. Q. Nguyen, "Hermite's Constant and Lattice Algorithms", *Chapter of the book The LLL Algorithm: Survey and Applications, P. Q. Nguyen and B. Vallée (Eds.), Springer (Series: Information Security and Cryptography)* (2009).

[21] V. Pan, "Univariate polynomials: nearly optimal algorithms for numerical factorization and root finding", *Journal of Symbolic Computation*, **33** (2002), 701–733.

[22] C. Poor and D. S. Yuen, "The Bergé-Martinet constant and slopes of Siegel cusp forms", *Bull. London Math. Soc.* **38** (2006), 913–924.

[23] L. Rónyai, "Zero divisors in quaternion algebras", *Journal of Algorithms*, **9** (1988) 494–506.

[24] L. Rónyai, "Computing the structure of finite algebras", *Journal of Symbolic Computation*, **9** (1990) 355–373.

[25] L. Rónyai, "Algorithmic properties of maximal orders in simple algebras over $\mathbb{Q}$", *Comput. Complexity*, **2** (1992), 225–243.

[26] A. Schönhage, "The fundamental theorem of algebra in terms of computational complexity", *Preliminary report*, Universität Tübingen (1982).