

# The Taussky-Kruskemper method for construction of root lattices\*

Research Article

Aginaldo José Ferrari 

**Abstract:** In this paper, we present a method to construct the root lattices based on the Taussky-Kruskemper method which computes the generator matrix of an integral lattice, given its Gram matrix. This yields an algebraic lattice, in the sense that the lattice is built via the embedding of a number field.

**2020 MSC:** 11H06, 11H31, 11H71, 52C07

**Keywords:** Root lattices, Number field, Minimum product distance

## 1. Introduction

A lattice  $\Lambda \subseteq \mathbb{R}^n$  is a discrete set generated by integer combinations of  $m$  linearly independent vectors  $v_1, v_2, \dots, v_m \in \mathbb{R}^n$ ,  $m \leq n$ . In this paper, we consider  $m = n$ . A lattice  $\Lambda$  has diversity  $k \leq n$  if  $k$  is the maximum number such that for all  $y = (y_1, \dots, y_n) \in \Lambda$ ,  $y \neq 0$ , there are at least  $k$  non-zero coordinates. Given a full diversity lattice  $\Lambda \subseteq \mathbb{R}^n$  ( $k = n$ ), the minimum product distance is defined as  $d_{\min}(\Lambda) = \min\{\prod_{i=1}^n |y_i|\}$ , for all  $y = (y_1, \dots, y_n) \in \Lambda$ ,  $y \neq 0$  [6]. Signal constellations having lattice structure have been studied as meaningful means for signal transmission over single-antenna Rayleigh fading channel [9]. Usually the problem of finding good signal constellations for a Rayleigh fading channel whose efficiency, measured by lower error probability in the transmission, is strongly related to the lattice diversity and minimum product distance, and has been studied in the last years [1, 2, 3, 5, 6, 7, 8, 9,

\* This work was supported by CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) under Grant No. 405842/2023-6.

Aginaldo José Ferrari (Corresponding Author); Department of Mathematics, São Paulo State University, Bauru, Brazil, (agnaldo.ferrari@unesp.br).

© 2026 The Author(s). Published by iPeak Academy Ltd. This is an open access article under the CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>).

10, 13, 14, 15, 19]. For general lattices the minimum product distance is usually hard to estimate [17]. This parameter can be obtained in certain cases of lattices associated to number fields, through algebraic properties. The approach in this work, following [11] and [16] is the use of an algorithm which computes the generator matrix of an integral lattice, given its Gram matrix. This yields an algebraic lattice, in the sense that the lattice is built via the embedding of a number field. By this method, Oggier et al [19] constructed rotated cubic lattices in dimension up to 7 over totally real number field with small discriminant resulting in signal constellations with maximal diversity and best minimum product distance. In this work, using these ideas, we constructed the root lattices  $A_2$ ,  $D_3$ ,  $D_4$  and  $D_5$  over number fields with small discriminants, since the method allows us to control the number field  $\mathbb{K}$ , and we also calculated the minimum product distance as a way to measure the efficiency for the Rayleigh fading channel.

## 2. Basic results

Let  $\{v_1, \dots, v_n\}$  be a set of linearly independent vectors in  $\mathbb{R}^n$  and  $\Lambda = \{\sum_{i=1}^n a_i v_i; a_i \in \mathbb{Z}\}$  be a lattice. The set  $\{v_1, \dots, v_n\}$  is called a *basis* for  $\Lambda$ . A matrix  $M$  whose rows are these vectors is said to be a *generator matrix* for  $\Lambda$  while the associated *Gram matrix* is  $G = MM^t = (\langle v_i, v_j \rangle)_{i,j=1}^n$ . The *determinant* of  $\Lambda$  is  $\det(\Lambda) = \det(G)$ . If  $A$  is a integer matrix and  $\det(A) = \pm 1$ , then  $AM$  is another basis for  $\Lambda$ . The *determinant* of  $\Lambda$  is an invariant under change of basis [12]. The lattice  $\Lambda$  is called *integral* when the inner products of lattice vectors are all integers.

Let  $\mathbb{K}$  be an algebraic number field of degree  $n$ , i.e.,  $\mathbb{K} = \mathbb{Q}(\omega)$ , with  $\omega \in \mathbb{C}$  a root of a monic irreducible polynomial  $p(x) \in \mathbb{Z}[x]$ . The  $n$  distinct roots of  $p(x)$ , namely,  $\omega_1, \omega_2, \dots, \omega_n$ , are the conjugates of  $\omega$ . The *embeddings* of  $\mathbb{K}$  are homomorphisms  $\sigma_i(\omega) = \omega_i$ , for all  $i = 1, 2, \dots, n$ . So, the embeddings  $\sigma_i$ , for  $i = 1, \dots, n$ , are the  $n$  distinct  $\mathbb{Q}$ -homomorphisms from  $\mathbb{K}$  to  $\mathbb{C}$  such that  $\sigma_1, \dots, \sigma_{r_1}$  are real and  $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \dots, \sigma_{r_1+2r_2}$  are imaginary, where  $\sigma_{r_1+r_2+i}$  is the complex conjugate of  $\sigma_{r_1+i}$ , for all  $i = 1, \dots, r_2$ . In this case,  $n = r_1 + 2r_2$ . If all the embeddings of  $\mathbb{K}$  are real, in this case  $r_1 = n$  and  $r_2 = 0$ , (resp., complex, in this case,  $r_1 = 0$  and  $2r_2 = n$ ),  $\mathbb{K}$  is said to be totally real (resp., totally complex).

The set  $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} : \text{there is a monic polynomial } f(x) \in \mathbb{Z}[x] \text{ such that } f(\alpha) = 0\}$  is called the *ring of algebraic integers* of  $\mathbb{K}$ . It can be shown that  $\mathcal{O}_{\mathbb{K}}$ , as a  $\mathbb{Z}$ -module, has a basis  $\{\omega_1, \dots, \omega_n\}$  over  $\mathbb{Z}$ , where  $n$  is the degree of  $\mathbb{K}$ . Furthermore, if  $\{\omega_1, \dots, \omega_n\}$  is a  $\mathbb{Z}$ -basis of  $\mathcal{O}_{\mathbb{K}}$ , the integer  $d_{\mathbb{K}} = (\det[\sigma_j(\omega_i)]_{i,j=1}^n)^2$  is called the *discriminant* of  $\mathbb{K}$  and it is an invariant over change of basis. The *norm* and the *trace* of any element  $\alpha \in \mathbb{K}$  are defined as the rational numbers  $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$  and  $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ , respectively.

Let  $\mathbb{K}$  be a totally real number field of degree  $n$ , and denote by  $\sigma_i$ ,  $i = 1, \dots, n$  its  $n$  embeddings into  $\mathbb{R}^n$ . Let  $\alpha \in \mathbb{K}$  satisfies  $\sigma_i(\alpha) > 0$ ,  $\forall i$  and  $\mathcal{A}$  be a fractional ideal of  $\mathbb{K}$  with a  $\mathbb{Z}$ -basis  $\{v_1, \dots, v_n\}$ , i.e.,  $\mathcal{A} = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ . An *ideal lattice* is an integral lattice whose generator matrix  $M$  is given by

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(v_1) & \dots & \sqrt{\sigma_n(\alpha)}\sigma_n(v_1) \\ \vdots & & \vdots \\ \sqrt{\sigma_1(\alpha)}\sigma_1(v_n) & \dots & \sqrt{\sigma_n(\alpha)}\sigma_n(v_n) \end{pmatrix} \quad (1)$$

which satisfies that  $MM^T = (Tr_{\mathbb{K}/\mathbb{Q}}(\alpha v_i v_j))_{i,j=1}^n$  [5].

An order  $\mathfrak{D}$  in  $\mathbb{K}$  is a subring of  $\mathbb{K}$  which as a  $\mathbb{Z}$ -module is finitely generated and of maximal rank  $n = [\mathbb{K} : \mathbb{Q}]$ . We can show that  $\mathfrak{D} \subset \mathcal{O}_{\mathbb{K}}$  for any order of  $\mathbb{K}$ , so that  $\mathcal{O}_{\mathbb{K}}$  is also called the *maximal order* of  $\mathbb{K}$ .

Let  $\mathfrak{D}$  be an order of  $\mathbb{K}$ ,  $\mathcal{A}$  be an ideal of  $\mathfrak{D}$  and  $b_{\alpha}$  a symmetric bilinear form given by  $b_{\alpha} : \mathcal{A} \times \mathcal{A} \rightarrow \mathbb{Z}$ ,  $b_{\alpha}(x, y) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha xy)$ . The *minimum product distance* of an ideal lattice  $\Lambda = (\mathcal{A}, b_{\alpha})$

of determinant  $\det(b_\alpha)$  is

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]}} ,$$

where  $\min(\mathcal{A}) = \min_{0 \neq x \in \mathcal{A}} \frac{|N(x)|}{N(\mathcal{A})}$  and  $[\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]$  is the index of  $\mathfrak{D}$  in  $\mathcal{O}_{\mathbb{K}}$  [18].

If  $\mathcal{A}$  is principal, then the minimum product distance of  $\Lambda$  is

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}} \frac{1}{[\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]} } .$$

The *relative minimum product distance* of  $\Lambda$ , denoted by  $d_{p,rel}(\Lambda)$ , is the minimum product distance of a scaled version of  $\Lambda$  with unitary minimum norm vector, i.e., if the minimum norm of  $\Lambda$  is  $\mu$  then

$$d_{p,rel}(\Lambda) = \frac{1}{(\sqrt{\mu})^n} \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]} } .$$

In order to compare the relative minimum product distance in different dimensions, we will work with the normalized relative minimum product distance  $\sqrt[n]{d_{p,rel}(\Lambda)}$ .

Let  $\mathbb{K}$  be a number field, and  $\mathcal{O}_{\mathbb{K}}$  be its ring of integers. If  $I_{\mathbb{K}}$  denote the group of fractional ideals of  $\mathbb{K}$  and  $P_{\mathbb{K}}$  denote the subgroup of  $\mathbb{K}$  formed by the principal ideals, then the *ideal class group*, denoted by  $Cl(\mathbb{K})$ , is  $Cl(\mathbb{K}) = I_{\mathbb{K}}/P_{\mathbb{K}}$ . The *class number* of  $\mathbb{K}$ , denoted by  $h(\mathbb{K})$ , is the cardinality of  $Cl(\mathbb{K})$ . In particular, if  $\mathcal{O}_{\mathbb{K}}$  is a principal ideal domain, then  $h(\mathbb{K}) = 1$ . The class number of a field  $\mathbb{K}$  can be understand as the measure of how principal a ring of integers is, i.e., what is the proportion of principal ideals among all the ideals.

In this work, to calculate  $[\mathcal{O}_{\mathbb{K}} : \mathfrak{D}]$  and  $h(\mathbb{K})$  we use the software Mathematica and PARI [4], respectively.

### 3. Construction of ideal lattices

In this section we present the Taussky-Kruskemper method which prove that any integral lattice can be constructed as an ideal lattice of some algebra  $\mathbb{Z}[X]/(f(X))$ , where  $f(X) \in \mathbb{Z}[X]$  is monic and irreducible.

We denote by  $M$  a finitely generated free  $\mathbb{Z}$ -module of rank  $n$  and by  $b : M \times M \rightarrow \mathbb{Z}$  a symmetric bilinear form. Let  $f(X) \in \mathbb{Z}[X]$  be a monic irreducible polynomial of degree  $n$  and  $\theta$  be a root of  $f$ . Then  $\mathbb{Z}[X]/(f(X)) = \mathbb{Z}[\theta]$  with basis  $\{1, \theta, \dots, \theta^{n-1}\}$ . If  $\mathcal{A}$  is an ideal of  $\mathbb{Z}[\theta]$ , we set  $\mathcal{A}^\# = \{c \in \mathbb{Q}(\theta) \mid Tr(c\mathcal{A}) \subseteq \mathbb{Z}\}$ .

**Lemma 3.1.** [20] *The algebraic number  $\theta$  is the root of characteristic polynomial of the matrix  $A$  and the components of the corresponding eigenvector  $v_\theta$  can be chosen to form the basis of an ideal in the ring formed by the polynomials in  $\theta$  with rational integers coefficients.*

**Lemma 3.2.** [21] *Let the matrix  $A$  correspond to the ideal class determined by the ideal  $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$  and let the transpose  $A^t$  correspond to the ideal  $\mathcal{B} = (\beta_1, \dots, \beta_n)$ . Then  $\mathcal{B}$  belongs to the inverse class of  $\mathcal{A}$ .*

**Theorem 3.3.** [18] *Let  $B \in \mathcal{M}_n(\mathbb{Z})$  be a non-singular symmetric matrix. Let  $A \in \mathcal{M}_n(\mathbb{Z})$  be such that its characteristic polynomial  $\mathcal{X}_A$  is irreducible and  $B^{-1}AB = A^T$ . Then  $B$  is the matrix of an ideal lattice.*

**Proof.** Let  $\theta \in \mathbb{C}$  be a root of  $\mathcal{X}_A$ . It is an algebraic integer since  $\mathcal{X}_A$  is monic with coefficients in  $\mathbb{Z}$ . By Lemma 3.1, there exists an eigenvector  $v_\theta = (v_1, \dots, v_n)^T$  of  $A$  associated to  $\theta$ , with  $v_i \in \mathbb{Z}[\theta]$  and such that  $\{v_1, \dots, v_n\}$  is a  $\mathbb{Z}$ -basis of an ideal of  $\mathbb{Z}[\theta]$ . By the first proof of Lemma 3.2, there exists an eigenvector  $v'_\theta = (v'_1, \dots, v'_n)^T$  of  $A^T$  associated to  $\theta$ , with  $v'_j \in \mathbb{Q}(\theta)$  and such that

$$\text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(v_i v'_j) = \delta_{ij}, \forall i, j. \quad (2)$$

It follows from  $A^T = B^{-1}AB$  that  $A^T B^{-1}v_\theta = B^{-1}Av_\theta = \theta B^{-1}v_\theta$ , so that  $v'_\theta$  and  $B^{-1}v_\theta$  are both eigenvectors of  $A^T$  associated to  $\theta$ . Since  $\mathcal{X}_{A^T} = \mathcal{X}_A$  is irreducible over  $\mathbb{Q}$ , it is separable, that is the eigenvalues are distinct and consequently, the associated subspaces are of dimension 1. Thus, there exists  $\alpha \in \mathbb{Q}(\theta)$  such that  $v'_\theta = \alpha B^{-1}v_\theta$ , i.e.  $Bv'_\theta = \alpha v_\theta$ . Denote  $B = (b_{ij})_{i,j}$ . We have

$$\sum_{j=1}^n b_{ij} v'_j = \alpha v_i, \forall i \rightarrow \sum_{j=1}^n b_{ij} v'_j v_k = \alpha v_i v_k, \forall i, k \quad (3)$$

so that

$$\sum_{j=1}^n b_{ij} \text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(v'_j v_k) = \text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha v_i v_k).$$

By Equation 2, we get  $b_{ik} = \text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha v_i v_k)$  and we conclude that  $B$  is the matrix of an ideal lattice  $\mathcal{A} = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ .  $\square$

We show now that a matrix  $A$  such as described in the hypothesis of Theorem 3.3 always exists.

**Theorem 3.4.** [18] Let  $(M, b)$  be an integral lattice. Then there exists an algebraic integer  $\theta$ , an ideal  $\mathcal{A}$  of  $\mathbb{Z}[\theta]$  and  $\alpha \in (\mathcal{A}^2)^\# \subseteq \mathbb{Q}(\theta)$  such that  $b$  is isomorphic to

$$\begin{aligned} \mathcal{A} \times \mathcal{A} &\rightarrow \mathbb{Z} \\ (x, y) &\mapsto \text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy) \end{aligned}$$

Furthermore,  $\theta$  can be assumed to be totally real.

**Proof.** By Theorem 3.3, it is enough to show that there always exists a matrix  $A \in \mathcal{M}_n(\mathbb{Z})$  whose characteristic polynomial  $\mathcal{X}_A$  is irreducible and totally real, and that satisfies  $B^{-1}AB = A^T$ . Let  $N = (X_{ij})$  be the symmetric  $n \times n$  matrix where the coefficients  $X_{ij} = X_{ji}$  are indeterminates. It is shown in [16] that the characteristic polynomial  $\mathcal{X}_{BN}$  of  $BN$  is irreducible. By Hilbert's irreducibility theorem, there exists  $x_{ij} = x_{ji} \in \mathbb{Q}$  such that  $\mathcal{X}_{B(x_{ij})}$  is irreducible and totally real. Let  $A = B(x_{ij})$ . It satisfies  $B^{-1}AB = A^T$ .  $\square$

## 4. The lattice construction algorithm

In this section we present an algorithm which takes as input a lattice Gram matrix  $B$  and outputs a lattice generator matrix. More precisely, it computes a set of elements  $\{v_1, \dots, v_n\}$  and an element  $\alpha$  such that  $\mathcal{A} = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$  and the ideal lattice  $(\mathcal{A}, b_\alpha)$

$$\begin{aligned} b_\alpha : \mathcal{A} \times \mathcal{A} &\rightarrow \mathbb{Z} \\ (x, y) &\mapsto \text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy) \end{aligned}$$

has Gram matrix  $B$ .

The steps of algorithm are explained in details in [18].

### Step 1: Computation of the matrix $A$

A matrix  $A \in \mathcal{M}_n(\mathbb{Z})$  satisfying  $B^{-1}AB = A^T$  and whose characteristic polynomial is irreducible can be either generated randomly, or (possibly) constructed in order to obtain a specific number field with minimal polynomial  $\mathcal{X}_A$ .

### Step 2: Computation of a $\mathbb{Z}$ -basis of the ideal $\mathcal{A}$

Recall from the proof of Theorem 3.3 that there exists an eigenvector  $v_\theta$  of  $A$  associated to  $\theta$ , a root of  $\mathcal{X}_A$ , such that  $\mathcal{A} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ . In [20], it is shown that

$$v_j := (-1)^{i+j} \Delta_{ij} (A - \theta I_n) \quad (4)$$

where  $\Delta_{ij}$  is the  $j$ th minor of a given fixed row, say the  $i$ th row, of  $(A - \theta I_n)$ . It can be shown that this vector is indeed an eigenvector of  $A$ .

### Step 3: Computation of $\alpha$

Recall again from the proof of Theorem 3.3 that there exists an eigenvector  $v'_\theta = (v'_1, \dots, v'_n)^T$  of  $A^T$  associated to  $\theta$ , with  $v'_i \in \mathbb{Q}(\theta)$  and such that  $\text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(v_i v'_j) = \delta_{ij}, \forall i, j$ . It can be shown that

$$v'_j = \sum_{i=1}^n m_{ij} \theta^{i-1},$$

where  $(m_{ij})_{i,j=1}^n = G^{-1}(V^T)^{-1}$  with

$$G = (\text{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1} \theta^{j-1}))_{i,j=1}^n \quad (5)$$

and  $V = (v_1, \dots, v_n)$  is the matrix of the coordinates of  $v_1, \dots, v_n$  in the basis  $\{1, \theta, \dots, \theta^{n-1}\}$ . The element  $\alpha$  is obtained from  $\sum_{j=1}^n b_{ij} v'_j = \alpha v_i, \forall i$  (Equation 3). If  $B$  is diagonal, it is enough to compute one of the  $v'_i$ 's.

### Step 4: Computation of the generator matrix of the lattice

We have

$$M = \begin{pmatrix} \sqrt{\alpha_1} \sigma_1(v_1) & \cdots & \sqrt{\alpha_n} \sigma_n(v_1) \\ \sqrt{\alpha_1} \sigma_1(v_2) & \cdots & \sqrt{\alpha_n} \sigma_n(v_2) \\ \vdots & \cdots & \vdots \\ \sqrt{\alpha_1} \sigma_1(v_n) & \cdots & \sqrt{\alpha_n} \sigma_n(v_n) \end{pmatrix},$$

where  $\sigma_i, i = 1, \dots, n$  denote the real embeddings of  $\mathbb{Q}(\theta)$  and  $\alpha_i = \sigma_i(\alpha), i = 1, \dots, n$ .

## 5. Construction of root lattices

In this section, we construct the lattices  $A_2, D_3, D_4$  and  $D_5$  e calculate the relative minimum product distance. By the way, taking  $\alpha = 1$  in (1) with  $\{1, \theta, \dots, \theta^{n-1}\}$  a  $\mathbb{Z}$ -basis of  $\mathbb{Z}[\theta] \subseteq \mathcal{O}_{\mathbb{K}}$ , where  $\mathbb{K} = \mathbb{Q}(\theta)$ , we have that

$$\begin{aligned} d_{\mathbb{K}} &= (\det[\sigma_i(\theta^{j-1})]_{i,j=1}^n)^2 = (\det(M))^2 = \det(M) \det(M) = \det(M) \det(M^T) = \\ &= \det(M M^T) = \det(\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\theta^{i-1} \theta^{j-1}))_{i,j=1}^n = \det(G), \end{aligned}$$

since by (5) we have  $G = Tr_{\mathbb{K}/\mathbb{Q}}(\theta^{i-1}\theta^{j-1})_{i,j=1}^n$ .

### 5.1. $A_2$ -lattice

A generator matrix of  $A_2$ -lattice is given by  $M = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$ , where the Gram matrix associated is  $B = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ . Consider the number field  $\mathbb{K}$  given by  $X^2 - 3$ . The matrix

$$A = \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix},$$

satisfies  $\mathcal{X}_A(X) = X^2 - 3$ , where  $\mathcal{X}_A$  is irreducible over  $\mathbb{Q}$ , and  $B^{-1}AB = A^T$ . We compute the matrices  $V$  and  $G$  as explained, as  $v_\theta = (v_1, v_2)^T$ , where  $v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_n)$ , let  $i = 1$ , we get  $v_\theta = (1 - \theta, -2)^T$ . Let  $V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}$  and  $(1, \theta) \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} = (v_1, v_2)$ , so  $V = \begin{pmatrix} 1 & -2 \\ -1 & 0 \end{pmatrix}$  and consequently  $(V^T)^{-1} = \begin{pmatrix} 0 & -\frac{1}{2} \\ -1 & -\frac{1}{2} \end{pmatrix}$ . We have

$$G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^2 = \begin{pmatrix} Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix},$$

since  $\theta$  is a root of  $\mathcal{X}_A$ , the set of roots of  $\mathcal{X}_A$  is  $\{-\sqrt{3}, \sqrt{3}\}$ , this means that the real embeddings of  $\theta$  are  $\sigma_1(\theta) = -\sqrt{3}$  and  $\sigma_2(\theta) = \sqrt{3}$ , thus  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = \sigma_1(1) + \sigma_2(1) = 2$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) = 0$  and  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = \sigma_1(\theta^2) + \sigma_2(\theta^2) = \sigma_1(\theta)^2 + \sigma_2(\theta)^2 = 6$ . We have  $d_{\mathbb{K}} = \det(G) = 12$ , and consequently  $G^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{6} \end{pmatrix}$ . Let  $v'_\theta = (v'_1, v'_2)^T$ , where  $v'_1 = \sum_{i=1}^2 m_{i1}\theta^{i-1}$ ,  $v'_2 = \sum_{i=1}^2 m_{i2}\theta^{i-1}$  and

$$(m_{ij})_{i,j=1}^2 = G^{-1}(V^T)^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{6} \end{pmatrix} \begin{pmatrix} 0 & -\frac{1}{2} \\ -1 & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 & -\frac{1}{6} \\ -\frac{1}{6} & -\frac{1}{12} \end{pmatrix}.$$

Therefore,  $v'_\theta = (v'_1, v'_2)^T = (-\frac{1}{6}\theta, -\frac{1}{4} - \frac{1}{12}\theta)^T$ . The element  $\alpha$  is given by  $\alpha v_\theta = Bv'_\theta$ , i.e.,

$$\alpha \begin{pmatrix} 1 - \theta \\ -2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} -\frac{1}{6}\theta \\ -\frac{1}{4} - \frac{1}{12}\theta \end{pmatrix}.$$

Using for example the last row, we compute  $\alpha = \frac{1}{4}$ . Since

$$\alpha_1 = \sigma_1(\alpha) = \sigma_1(\frac{1}{4}) = \frac{1}{4},$$

$$\alpha_2 = \sigma_2(\alpha) = \sigma_2(\frac{1}{4}) = \frac{1}{4},$$

$$\sigma_1(v_1) = \sigma_1(1 - \theta) = \sigma_1(1) - \sigma_1(\theta) = 1 + \sqrt{3},$$

$$\sigma_2(v_1) = \sigma_2(1 - \theta) = \sigma_2(1) - \sigma_2(\theta) = 1 - \sqrt{3},$$

$\sigma_1(v_2) = \sigma_1(-2) = -2$  and  $\sigma_2(v_2) = \sigma_2(-2) = -2$ , it follows that the generator matrix of the lattice is thus given by

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{3}}{2} & \frac{1-\sqrt{3}}{2} \\ -1 & -1 \end{pmatrix}.$$

We thus have  $\det(b_\alpha) = \det(B) = 3$ ,  $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$  and  $h(\mathbb{K}) = 1$ . As the minimum norm of  $A_2$  is  $\mu = 2$ , it follows that the lattice built over  $\mathcal{O}_{\mathbb{K}}$  will have relative minimum product distance given by

$$\sqrt{d_{p,rel}(A_2)} = \left( \frac{1}{(\sqrt{\mu})^2} \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]} \right)^{1/2} = \left( \frac{1}{(\sqrt{2})^2} \sqrt{\frac{3}{12}} \right)^{1/2} = 0.5$$

## 5.2. $D_3$ -lattice

A generator matrix of  $D_3$ -lattice is given by  $M = \begin{pmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$ , where the Gram matrix associated is  $B = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$ . Consider the number field  $\mathbb{K}$  given by  $X^3 + X^2 - 4X - 2$ . The matrix

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

satisfies  $\mathcal{X}_A(X) = X^3 + X^2 - 4X - 2$ , where  $\mathcal{X}_A$  is irreducible over  $\mathbb{Q}$ , and  $B^{-1}AB = A^T$ . We compute the matrices  $V$  and  $G$  as explained, as  $v_\theta = (v_1, v_2, v_3)^T$ , where  $v_j = (-1)^{i+j} \Delta_{ij}(A - \theta I_n)$ , let  $i = 1$ , we get  $v_\theta = (\theta^2 - 3, -1, -\theta + 2)^T$ . Let  $V = \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix}$  and  $(1, \theta, \theta^2) \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix} = (v_1, v_2, v_3)$ , so  $V = \begin{pmatrix} -3 & -1 & 2 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$  and consequently  $(V^T)^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & -3 & 0 \end{pmatrix}$ . We have

$$G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^3 = \begin{pmatrix} Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) \end{pmatrix} = \begin{pmatrix} 3 & -1 & 9 \\ -1 & 9 & -7 \\ 9 & -7 & 41 \end{pmatrix},$$

since  $\theta$  is a root of  $\mathcal{X}_A$ , the set of roots of  $\mathcal{X}_A$  is  $\{-0.47068, -2.34292, 1.81361\}$ , this means that the real embeddings of  $\theta$  are  $\sigma_1(\theta) = -0.47068$ ,  $\sigma_2(\theta) = -2.34292$  and  $\sigma_3(\theta) = 1.81361$ , thus  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = \sigma_1(1) + \sigma_2(1) + \sigma_3(1) = 3$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) + \sigma_3(\theta) = -1$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = \sigma_1(\theta)^2 + \sigma_2(\theta)^2 + \sigma_3(\theta)^2 = 9$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) = \sigma_1(\theta)^3 + \sigma_2(\theta)^3 + \sigma_3(\theta)^3 = -7$  and  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) = \sigma_1(\theta)^4 + \sigma_2(\theta)^4 + \sigma_3(\theta)^4 = 41$ . We have  $d_{\mathbb{K}} = \det(G) = 316$ , and consequently

$$G^{-1} = \begin{pmatrix} \frac{80}{79} & -\frac{11}{158} & -\frac{37}{158} \\ -\frac{11}{158} & \frac{21}{158} & \frac{79}{158} \\ -\frac{37}{158} & \frac{79}{158} & \frac{13}{158} \end{pmatrix}.$$

Let  $v'_\theta = (v'_1, v'_2, v'_3)^T$ , where  $v'_1 = \sum_{i=1}^3 m_{i1}\theta^{i-1}$ ,  $v'_2 = \sum_{i=1}^3 m_{i2}\theta^{i-1}$ ,  $v'_3 = \sum_{i=1}^3 m_{i3}\theta^{i-1}$  and

$$(m_{ij})_{i,j=1}^3 = G^{-1}(V^T)^{-1} = \begin{pmatrix} \frac{80}{79} & -\frac{11}{158} & -\frac{37}{158} \\ -\frac{11}{158} & \frac{21}{158} & \frac{79}{158} \\ -\frac{37}{158} & \frac{79}{158} & \frac{13}{158} \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & -3 & 0 \end{pmatrix} = \begin{pmatrix} -\frac{37}{158} & -\frac{27}{158} & \frac{11}{158} \\ \frac{3}{158} & -\frac{49}{158} & -\frac{21}{158} \\ \frac{13}{158} & -\frac{7}{79} & -\frac{3}{79} \end{pmatrix}.$$

Therefore,  $v'_\theta = (v'_1, v'_2, v'_3)^T = (-\frac{37}{158} + \frac{3}{79}\theta + \frac{13}{158}\theta^2, -\frac{27}{158} - \frac{49}{158}\theta - \frac{7}{79}\theta^2, \frac{11}{158} - \frac{21}{158}\theta - \frac{3}{79}\theta^2)^T$ . The element  $\alpha$  is given by  $\alpha v_\theta = Bv'_\theta$ , i.e.,

$$\alpha \begin{pmatrix} \theta^2 - 3 \\ -1 \\ -\theta + 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} \begin{pmatrix} -\frac{37}{158} + \frac{3}{79}\theta + \frac{13}{158}\theta^2 \\ -\frac{27}{158} - \frac{49}{158}\theta - \frac{7}{79}\theta^2 \\ \frac{11}{158} - \frac{21}{158}\theta - \frac{3}{79}\theta^2 \end{pmatrix}.$$

Using for example the second row, we compute  $\alpha = \frac{65}{158} + \frac{77}{158}\theta + \frac{11}{158}\theta^2$ . Since  $\alpha_1 = \sigma_1(\alpha) = \sigma_1(\frac{65}{158} + \frac{77}{158}\theta + \frac{11}{158}\theta^2) = \frac{65}{158} + \frac{77}{158}\sigma_1(\theta) + \frac{11}{158}\sigma_1(\theta)^2 = 0.21285$ ,

$\alpha_2 = \sigma_2(\alpha) = \sigma_2\left(\frac{65}{158} + \frac{77}{158}\theta + \frac{11}{158}\theta^2\right) = \frac{65}{158} + \frac{77}{158}\sigma_2(\theta) + \frac{11}{158}\sigma_2(\theta)^2 = 0.03391$ ,  
 $\alpha_3 = \sigma_3(\alpha) = \sigma_3\left(\frac{65}{158} + \frac{77}{158}\theta + \frac{11}{158}\theta^2\right) = \frac{65}{158} + \frac{77}{158}\sigma_3(\theta) + \frac{11}{158}\sigma_3(\theta)^2 = 1.75322$ ,  
 $\sigma_1(v_1) = \sigma_1(\theta^2 - 3) = \sigma_1(\theta^2) - \sigma_1(3) = \sigma_1(\theta)^2 - 3 = -2.77846$ ,  
 $\sigma_2(v_1) = \sigma_2(\theta^2 - 3) = \sigma_2(\theta^2) - \sigma_2(3) = \sigma_2(\theta)^2 - 3 = 2.48929$ ,  
 $\sigma_3(v_1) = \sigma_3(\theta^2 - 3) = \sigma_3(\theta^2) - \sigma_3(3) = \sigma_3(\theta)^2 - 3 = 0.28916$ ,  
 $\sigma_1(v_2) = \sigma_2(v_2) = \sigma_3(v_2) = -1$ ,  
 $\sigma_1(v_3) = \sigma_1(-\theta + 2) = \sigma_1(-\theta) + \sigma_1(2) = -\sigma_1(\theta) + 2 = 2.47068$ ,  
 $\sigma_2(v_3) = \sigma_2(-\theta + 2) = \sigma_2(-\theta) + \sigma_2(2) = -\sigma_2(\theta) + 2 = 4.34292$ , and  
 $\sigma_3(v_3) = \sigma_3(-\theta + 2) = \sigma_3(-\theta) + \sigma_3(2) = -\sigma_3(\theta) + 2 = 0.18639$ , it follows that the generator matrix of the lattice is thus given by

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) \end{pmatrix} = \begin{pmatrix} -1.28188 & 0.45845 & 0.38288 \\ -0.46136 & -0.18417 & -1.32409 \\ 1.13988 & 0.79984 & 0.24680 \end{pmatrix}.$$

We thus have  $\det(b_\alpha) = \det(B) = 4$ ,  $[\mathcal{O}_\mathbb{K} : \mathbb{Z}[\theta]] = 1$  and  $h(\mathbb{K}) = 1$ . As the minimum norm of  $D_3$  is  $\mu = 2$ , it follows that the lattice built over  $\mathcal{O}_\mathbb{K}$  will have relative minimum product distance given by

$$\sqrt[3]{d_{p,rel}(D_3)} = \left( \frac{1}{(\sqrt{\mu})^3} \sqrt{\frac{\det(b_\alpha)}{d_\mathbb{K}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_\mathbb{K} : \mathbb{Z}[\theta]]} \right)^{1/3} = \left( \frac{1}{(\sqrt{2})^3} \sqrt{\frac{4}{316}} \right)^{1/3} = 0.34136$$

### 5.3. $D_4$ -lattice

A generator matrix of  $D_4$ -lattice is given by  $M = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$ , where the Gram matrix associated is  $B = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$ . Consider the number field  $\mathbb{K}$  given by  $X^4 - 8X^2 + 8X - 2$ . The matrix

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

satisfies  $\mathcal{X}_A(X) = X^4 - 8X^2 + 8X - 2$ , where  $\mathcal{X}_A$  is irreducible over  $\mathbb{Q}$ , and  $B^{-1}AB = A^T$ . We compute the matrices  $V$  and  $G$  as explained, as  $v_\theta = (v_1, v_2, v_3, v_4)^T$ , where  $v_j = (-1)^{i+j} \Delta_{ij}(A - \theta I_4)$ , let  $i = 1$ , we get  $v_\theta = (-\theta^3 + 2\theta^2 + \theta - 1, \theta - 1, -\theta^2 + 2\theta - 1, -\theta^2 + 3\theta - 1)^T$ . Let

$$V = \begin{pmatrix} v_{11} & v_{12} & v_{13} & v_{14} \\ v_{21} & v_{22} & v_{23} & v_{24} \\ v_{31} & v_{32} & v_{33} & v_{34} \\ v_{41} & v_{42} & v_{43} & v_{44} \end{pmatrix} \text{ and } (1, \theta, \theta^2, \theta^3)V = (v_1, v_2, v_3, v_4), \text{ so } V = \begin{pmatrix} -1 & -1 & -1 & -1 \\ 1 & 1 & 2 & 3 \\ 2 & 0 & -1 & -1 \\ -1 & 0 & 0 & 0 \end{pmatrix} \text{ and con-}$$

sequently  $(V^T)^{-1} = \begin{pmatrix} 0 & -1 & -1 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & -2 & 1 \\ -1 & 3 & -4 & 2 \end{pmatrix}$ . We have

$$G = (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^4 = \begin{pmatrix} Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^6) \end{pmatrix} =$$

$$= \begin{pmatrix} 4 & 0 & 16 & -24 \\ 0 & 16 & -24 & 136 \\ 16 & -24 & 136 & -320 \\ -24 & 136 & -320 & 1312 \end{pmatrix},$$

since  $\theta$  is a root of  $\mathcal{X}_A$ , the set of roots of  $\mathcal{X}_A$  is  $\{\sqrt{2} - \sqrt{2 - \sqrt{2}}, \sqrt{2} + \sqrt{2 - \sqrt{2}}, -\sqrt{2} - \sqrt{2 + \sqrt{2}}, -\sqrt{2} + \sqrt{2 + \sqrt{2}}\}$ , this means that the real embeddings of  $\theta$  are  $\sigma_1(\theta) = \sqrt{2} - \sqrt{2 - \sqrt{2}}$ ,  $\sigma_2(\theta) = \sqrt{2} + \sqrt{2 - \sqrt{2}}$ ,  $\sigma_3(\theta) = -\sqrt{2} - \sqrt{2 + \sqrt{2}}$  and  $\sigma_4(\theta) = -\sqrt{2} + \sqrt{2 + \sqrt{2}}$ , thus  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = 4$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = 0$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 16$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) = -24$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) = 136$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) = -320$  and  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^6) = 1312$ . We have  $d_{\mathbb{K}} = \det(G) = 2048$ , and consequently

$$G^{-1} = \begin{pmatrix} \frac{67}{4} & -\frac{131}{4} & \frac{9}{4} & \frac{17}{4} \\ -\frac{131}{4} & \frac{265}{4} & -\frac{19}{4} & -\frac{69}{8} \\ \frac{9}{4} & -\frac{19}{4} & \frac{3}{8} & -\frac{5}{8} \\ \frac{17}{4} & -\frac{69}{8} & \frac{3}{8} & \frac{9}{8} \end{pmatrix}.$$

Let  $v'_\theta = (v'_1, v'_2, v'_3, v'_4)^T$ , where  $v'_1 = \sum_{i=1}^4 m_{i1}\theta^{i-1}$ ,  $v'_2 = \sum_{i=1}^4 m_{i2}\theta^{i-1}$ ,  $v'_3 = \sum_{i=1}^4 m_{i3}\theta^{i-1}$ ,  $v'_4 = \sum_{i=1}^4 m_{i4}\theta^{i-1}$  and

$$(m_{ij})_{i,j=1}^4 = G^{-1}(V^T)^{-1} = \begin{pmatrix} -\frac{17}{4} & -\frac{7}{4} & -\frac{11}{2} & -\frac{21}{4} \\ \frac{69}{8} & \frac{17}{8} & \frac{21}{2} & \frac{23}{2} \\ -\frac{5}{8} & 0 & -\frac{3}{2} & -\frac{7}{8} \\ -\frac{9}{8} & -\frac{1}{4} & -\frac{11}{8} & -\frac{3}{2} \end{pmatrix}$$

Therefore,  $v'_\theta = (v'_1, v'_2, v'_3, v'_4)^T = (-\frac{17}{4} + \frac{69}{8}\theta - \frac{5}{8}\theta^2 - \frac{9}{8}\theta^3, -\frac{7}{4} + \frac{17}{8}\theta - \frac{1}{4}\theta^3, -\frac{11}{2} + \frac{21}{2}\theta - \frac{3}{4}\theta^2 - \frac{11}{8}\theta^3, -\frac{21}{4} + \frac{23}{2}\theta - \frac{7}{8}\theta^2 - \frac{3}{2}\theta^3)^T$ . The element  $\alpha$  is given by  $\alpha v_\theta = Bv'_\theta$ , i.e.,

$$\alpha \begin{pmatrix} -\theta^3 + 2\theta^2 + \theta - 1 \\ \theta - 1 \\ -\theta^2 + 2\theta - 1 \\ -\theta^2 + 3\theta - 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} \begin{pmatrix} -\frac{17}{4} + \frac{69}{8}\theta - \frac{5}{8}\theta^2 - \frac{9}{8}\theta^3 \\ -\frac{7}{4} + \frac{17}{8}\theta - \frac{1}{4}\theta^3 \\ -\frac{11}{2} + \frac{21}{2}\theta - \frac{3}{4}\theta^2 - \frac{11}{8}\theta^3 \\ -\frac{21}{4} + \frac{23}{2}\theta - \frac{7}{8}\theta^2 - \frac{3}{2}\theta^3 \end{pmatrix}.$$

Using for example the second row, we compute  $\alpha = -\frac{29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3$ . Since

$$\alpha_1 = \sigma_1(\alpha) = \sigma_1\left(-\frac{29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3\right) = -\frac{29}{4} + 20\sigma_1(\theta) - \frac{7}{4}\sigma_1(\theta)^2 - \frac{21}{8}\sigma_1(\theta)^3 = 4.27312$$

$$\alpha_2 = \sigma_2(\alpha) = \sigma_2\left(-\frac{29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3\right) = -\frac{29}{4} + 20\sigma_2(\theta) - \frac{7}{4}\sigma_2(\theta)^2 - \frac{21}{8}\sigma_2(\theta)^3 = 0.84820$$

$$\alpha_3 = \sigma_3(\alpha) = \sigma_3\left(-\frac{29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3\right) = -\frac{29}{4} + 20\sigma_3(\theta) - \frac{7}{4}\sigma_3(\theta)^2 - \frac{21}{8}\sigma_3(\theta)^3 = 0.00061$$

$$\alpha_4 = \sigma_4(\alpha) = \sigma_4\left(-\frac{29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3\right) = -\frac{29}{4} + 20\sigma_4(\theta) - \frac{7}{4}\sigma_4(\theta)^2 - \frac{21}{8}\sigma_4(\theta)^3 = 0.87806$$

$$\sigma_1(v_1) = \sigma_1(-\theta^3 + 2\theta^2 + \theta - 1) = -\sigma_1(\theta)^3 + 2\sigma_1(\theta)^2 + \sigma_1(\theta) - 1 = 0.21768,$$

$$\sigma_2(v_1) = 0.32647, \sigma_3(v_1) = 51.72790, \sigma_4(v_1) = -0.27202,$$

$$\sigma_1(v_2) = \sigma_1(\theta - 1) = \sigma_1(\theta) - 1 = -0.35115,$$

$\sigma_2(v_2) = 1.17958$ ,  $\sigma_3(v_2) = -4.26197$ ,  $\sigma_4(v_2) = -0.56645$ ,  
 $\sigma_1(v_3) = \sigma_1(-\theta^2 + 2\theta - 1) = -\sigma_1(\theta)^2 + 2\sigma_1(\theta) - 1 = -0.12330$ ,  
 $\sigma_2(v_3) = -1.39141$ ,  $\sigma_3(v_3) = -18.16440$ ,  $\sigma_4(v_3) = -0.32087$ ,  
 $\sigma_1(v_4) = \sigma_1(-\theta^2 + 3\theta - 1) = -\sigma_1(\theta)^2 + 3\sigma_1(\theta) - 1 = 0.52553$ ,  
 $\sigma_2(v_4) = 0.78817$ ,  $\sigma_3(v_4) = -21.42640$  and  $\sigma_4(v_4) = 0.11267$ , it follows that the generator matrix of the lattice is thus given by

$$\begin{aligned}
 M &= \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) & \sqrt{\alpha_4}\sigma_4(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) & \sqrt{\alpha_4}\sigma_4(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) & \sqrt{\alpha_4}\sigma_4(v_3) \\ \sqrt{\alpha_1}\sigma_1(v_4) & \sqrt{\alpha_2}\sigma_2(v_4) & \sqrt{\alpha_3}\sigma_3(v_4) & \sqrt{\alpha_4}\sigma_4(v_4) \end{pmatrix} = \\
 &= \begin{pmatrix} 0.44998 & 0.30067 & 1.28146 & -0.25489 \\ -0.72588 & 1.08637 & -0.10558 & -0.53079 \\ -0.25489 & -1.28146 & -0.44998 & -0.30067 \\ 1.08637 & 0.72588 & -0.53079 & 0.10558 \end{pmatrix}.
 \end{aligned}$$

We thus have  $\det(b_\alpha) = \det(B) = 4$ ,  $[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$  and  $h(\mathbb{K}) = 1$ . As the minimum norm of  $D_4$  is  $\mu = 2$ , it follows that the lattice built over  $\mathcal{O}_{\mathbb{K}}$  will have relative minimum product distance given by

$$\sqrt[4]{d_{p,rel}(D_4)} = \left( \frac{1}{(\sqrt{\mu})^4} \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]} \right)^{1/4} = \left( \frac{1}{(\sqrt{2})^4} \sqrt{\frac{4}{2048}} \right)^{1/4} = 0.32421$$

#### 5.4. $D_5$ -lattice

A generator matrix of  $D_5$ -lattice is given by  $M = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$ , where the Gram matrix

associated is  $B = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix}$ . Consider the number field  $\mathbb{K}$  given by  $X^5 - 4X^4 - 3X^3 + 12X^2 + 3X - 8$ . The matrix

$$A = \begin{pmatrix} -1 & -1 & -3 & -2 & -2 \\ -1 & -1 & -3 & 0 & 0 \\ 1 & 0 & 4 & 0 & 1 \\ 0 & 1 & -1 & 2 & 0 \\ -1 & 0 & 0 & -1 & 0 \end{pmatrix},$$

satisfies  $\chi_A(X) = X^5 - 4X^4 - 3X^3 + 12X^2 + 3X - 8$ , where  $\chi_A$  is irreducible over  $\mathbb{Q}$ , and  $B^{-1}AB = A^t$ . We compute the matrices  $V$  and  $G$  as explained, as  $v_\theta = (v_1, v_2, v_3, v_4, v_5)^T$ , where  $v_j = (-1)^{i+j} \Delta_{ij}(A - \theta I_5)$ , let  $i = 1$ , we get

$$v_\theta = (\theta^4 - 5\theta^3 + 2\theta^2 + 7\theta - 4, -\theta^3 + 3\theta^2 + \theta - 5, \theta^3 - 2\theta^2 - \theta + 3, -2\theta^2 + \theta + 4, -\theta^3 + 5\theta^2 - 8)^T$$

Let
 
$$V = \begin{pmatrix} v_{11} & v_{12} & v_{13} & v_{14} & v_{15} \\ v_{21} & v_{22} & v_{23} & v_{24} & v_{25} \\ v_{31} & v_{32} & v_{33} & v_{34} & v_{35} \\ v_{41} & v_{42} & v_{43} & v_{44} & v_{45} \\ v_{51} & v_{52} & v_{53} & v_{54} & v_{55} \end{pmatrix}$$
 and  $(1, \theta, \theta^2, \theta^3, \theta^4)V = (v_1, v_2, v_3, v_4, v_5)$ , so

$$V = \begin{pmatrix} -4 & -5 & 3 & 4 & -8 \\ 7 & 1 & -1 & 1 & 0 \\ 2 & 3 & -2 & -2 & 5 \\ -5 & -1 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and consequently } (V^T)^{-1} = \begin{pmatrix} 0 & -1 & 0 & 1 & 1 \\ 0 & 2 & 2 & 1 & 0 \\ 0 & -1 & 1 & 2 & 2 \\ 0 & 3 & 5 & 2 & 1 \\ 1 & -1 & 9 & 3 & 5 \end{pmatrix}.$$

We have

$$\begin{aligned} G &= (Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^5 \\ &= \begin{pmatrix} Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^6) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^6) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^7) \\ Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^6) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^7) & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^8) \end{pmatrix} = \\ &= \begin{pmatrix} 5 & 4 & 22 & 64 & 262 \\ 4 & 22 & 64 & 262 & 1004 \\ 22 & 64 & 262 & 1004 & 4000 \\ 64 & 262 & 1004 & 4000 & 15852 \\ 262 & 1004 & 4000 & 15852 & 63086 \end{pmatrix}, \end{aligned}$$

since  $\theta$  is a root of  $\mathcal{X}_A$ , the set of roots of  $\mathcal{X}_A$  is  $\{-1.26452, -1.15765, 0.87812, 1.56341, 3.98063\}$ , this means that the real embeddings of  $\theta$  are  $\sigma_1(\theta) = -1.26452$ ,  $\sigma_2(\theta) = -1.15765$ ,  $\sigma_3(\theta) = 0.87812$ ,  $\sigma_4(\theta) = 1.56341$  and  $\sigma_5(\theta) = 3.98063$ , thus  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = 5$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = 4$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 22$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) = 64$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) = 262$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^5) = 1004$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^6) = 4000$ ,  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^7) = 15852$  and  $Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^8) = 63086$ . We have  $d_{\mathbb{K}} = \det(G) = 246832$ . So, we have

$$(m_{ij})_{i,j=1}^5 = G^{-1}(V^T)^{-1} = \begin{pmatrix} -\frac{17863}{15427} & -\frac{59777}{25515} & -\frac{48234}{142811} & -\frac{12436}{15427} & \frac{3170}{15427} \\ \frac{15427}{8167} & \frac{15427}{56271} & \frac{15427}{30854} & \frac{15427}{49535} & -\frac{15427}{9902} \\ -\frac{15427}{16432} & -\frac{15427}{86143} & -\frac{15427}{70501} & -\frac{15427}{13833} & \frac{15427}{12495} \\ -\frac{15427}{6559} & -\frac{15427}{16301} & -\frac{15427}{13105} & -\frac{15427}{1921} & -\frac{15427}{3127} \\ \frac{30854}{30854} & \frac{30854}{30854} & \frac{30854}{30854} & \frac{30854}{30854} & -\frac{30854}{30854} \end{pmatrix}$$

Therefore,  $v'_\theta = (v'_1, v'_2, v'_3, v'_4, v'_5)^T$ , onde  $v'_1 = -\frac{17863}{15427} + \frac{25515\theta}{15427} + \frac{8167\theta^2}{15427} - \frac{16432\theta^3}{15427} + \frac{6559\theta^4}{30854}$ ,  $v'_2 = -\frac{59777}{15427} + \frac{142811\theta}{30854} + \frac{56271\theta^2}{30854} - \frac{86143\theta^3}{30854} + \frac{16301\theta^4}{30854}$ ,  $v'_3 = -\frac{48234}{15427} + \frac{117781\theta}{30854} + \frac{49535\theta^2}{30854} - \frac{70501\theta^3}{30854} + \frac{13105\theta^4}{30854}$ ,  $v'_4 = -\frac{12436}{15427} + \frac{12692\theta}{15427} + \frac{9902\theta^2}{15427} - \frac{13833\theta^3}{30854} + \frac{1921\theta^4}{30854}$  e  $v'_5 = \frac{3170}{15427} - \frac{20657\theta}{30854} + \frac{2304\theta^2}{15427} + \frac{12495\theta^3}{30854} - \frac{3127\theta^4}{30854}$ .

The element  $\alpha$  is given by  $\alpha v_\theta = Bv'_\theta$ , i.e.,

$$\alpha \begin{pmatrix} \theta^4 - 5\theta^3 + 2\theta^2 + 7\theta - 4 \\ -\theta^3 + 3\theta^2 + \theta - 5 \\ \theta^3 - 2\theta^2 - \theta + 3 \\ -2\theta^2 + \theta + 4 \\ -\theta^3 + 5\theta^2 - 8 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix} v'_\theta.$$

Using for example the fourth row, we compute

$$\alpha = \frac{\frac{20192}{15427} - \frac{23178\theta}{15427} - \frac{14535\theta^2}{30854} + \frac{15170\theta^3}{15427} - \frac{3068\theta^4}{15427}}{-2\theta^2 + \theta + 4}$$

Since

$$\alpha_1 = \sigma_1(\alpha) = \frac{\frac{20192}{15427} - \frac{23178\sigma_1(\theta)}{15427} - \frac{14535\sigma_1(\theta)^2}{30854} + \frac{15170\sigma_1(\theta)^3}{15427} - \frac{3068\sigma_1(\theta)^4}{15427}}{-2\sigma_1(\theta)^2 + \sigma_1(\theta) + 4} = 0.08935,$$

$$\begin{aligned}
\alpha_2 = \sigma_2(\alpha) &= \frac{\frac{20192}{15427} - \frac{23178\sigma_2(\theta)}{15427} - \frac{14535\sigma_2(\theta)^2}{30854} + \frac{15170\sigma_2(\theta)^3}{15427} - \frac{3068\sigma_2(\theta)^4}{15427}}{-2\sigma_2(\theta)^2 + \sigma_2(\theta) + 4} = 3.29642, \\
\alpha_3 = \sigma_3(\alpha) &= \frac{\frac{20192}{15427} - \frac{23178\sigma_3(\theta)}{15427} - \frac{14535\sigma_3(\theta)^2}{30854} + \frac{15170\sigma_3(\theta)^3}{15427} - \frac{3068\sigma_3(\theta)^4}{15427}}{-2\sigma_3(\theta)^2 + \sigma_3(\theta) + 4} = 0.05212, \\
\alpha_4 = \sigma_4(\alpha) &= \frac{\frac{20192}{15427} - \frac{23178\sigma_4(\theta)}{15427} - \frac{14535\sigma_4(\theta)^2}{30854} + \frac{15170\sigma_4(\theta)^3}{15427} - \frac{3068\sigma_4(\theta)^4}{15427}}{-2\sigma_4(\theta)^2 + \sigma_4(\theta) + 4} = 0.56021, \\
\alpha_5 = \sigma_5(\alpha) &= \frac{\frac{20192}{15427} - \frac{23178\sigma_5(\theta)}{15427} - \frac{14535\sigma_5(\theta)^2}{30854} + \frac{15170\sigma_5(\theta)^3}{15427} - \frac{3068\sigma_5(\theta)^4}{15427}}{-2\sigma_5(\theta)^2 + \sigma_5(\theta) + 4} = 0.00188, \\
\sigma_1(v_1) &= 3.01313, \sigma_2(v_1) = 0.13007, \sigma_3(v_1) = 0.89806, \sigma_4(v_1) = -1.30014, \sigma_5(v_1) = -8.74112, \\
\sigma_1(v_2) &= 0.55449, \sigma_2(v_2) = -0.58569, \sigma_3(v_2) = -2.48568, \sigma_4(v_2) = 0.07481, \\
\sigma_5(v_2) &= -16.55790, \sigma_1(v_3) = -0.95548, \sigma_2(v_3) = -0.07413, \sigma_3(v_3) = 1.25679, \\
\sigma_4(v_3) &= 0.36945, \sigma_5(v_3) = 30.40340, \sigma_1(v_4) = -0.46254, \sigma_2(v_4) = 0.16200, \sigma_3(v_4) = 3.33591, \\
\sigma_4(v_4) &= 0.67487, \sigma_5(v_4) = -23.71030, \sigma_1(v_5) = 2.01704, \sigma_2(v_5) = 0.25229, \\
\sigma_3(v_5) &= -4.82159, \sigma_4(v_5) = 0.39993, \text{ and } \sigma_5(v_5) = 8.15231, \text{ it follows that the generator matrix} \\
\text{of the lattice is thus given by}
\end{aligned}$$

$$\begin{aligned}
M &= \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) & \sqrt{\alpha_4}\sigma_4(v_1) & \sqrt{\alpha_5}\sigma_5(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) & \sqrt{\alpha_4}\sigma_4(v_2) & \sqrt{\alpha_5}\sigma_5(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) & \sqrt{\alpha_4}\sigma_4(v_3) & \sqrt{\alpha_5}\sigma_5(v_3) \\ \sqrt{\alpha_1}\sigma_1(v_4) & \sqrt{\alpha_2}\sigma_2(v_4) & \sqrt{\alpha_3}\sigma_3(v_4) & \sqrt{\alpha_4}\sigma_4(v_4) & \sqrt{\alpha_5}\sigma_5(v_4) \\ \sqrt{\alpha_1}\sigma_1(v_5) & \sqrt{\alpha_2}\sigma_2(v_5) & \sqrt{\alpha_3}\sigma_3(v_5) & \sqrt{\alpha_4}\sigma_4(v_5) & \sqrt{\alpha_5}\sigma_5(v_5) \end{pmatrix} = \\
&= \begin{pmatrix} 0.90070 & 0.23615 & 0.20503 & -0.97312 & -0.37940 \\ 0.16575 & -1.06339 & -0.56750 & 0.05599 & -0.71869 \\ -0.28562 & -0.13460 & 0.28693 & 0.27652 & 1.31966 \\ -0.13826 & 0.29413 & 0.76162 & 0.50512 & -1.02914 \\ 0.60294 & 0.45807 & -1.10082 & 0.29934 & 0.35385 \end{pmatrix}.
\end{aligned}$$

We thus have  $\det(b_\alpha) = \det(B) = 4$ ,  $[\mathcal{O}_\mathbb{K} : \mathbb{Z}[\theta]] = 1$  and  $h(\mathbb{K}) = 1 = \min\{\mathcal{A}\}$ . As the minimum norm of  $D_5$  is  $\mu = 2$ , it follows that the lattice built over  $\mathcal{O}_\mathbb{K}$  will have relative minimum product distance given by

$$\sqrt[5]{d_{p,rel}(D_5)} = \left( \frac{1}{(\sqrt{\mu})^5} \sqrt{\frac{\det(b_\alpha)}{d_\mathbb{K}}} \frac{\min\{\mathcal{A}\}}{[\mathcal{O}_\mathbb{K} : \mathbb{Z}[\theta]]} \right)^{1/5} = \left( \frac{1}{(\sqrt{2})^5} \sqrt{\frac{4}{246832}} \right)^{1/5} = 0.23466$$

## 6. Minimum product distance performance

In this section we present Table 1, comparing the relative minimum product distance of lattices constructed in the sections above and the  $\mathbb{Z}^n$ -lattices with the best relative minimum product distance known.

**Table 1. Performance**

| Dimension | $\sqrt[n]{d_{p,rel}(\Lambda)}$ | $\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$ |
|-----------|--------------------------------|-------------------------------------|
| 2         | 0.50000                        | 0.66874                             |
| 3         | 0.34136                        | 0.52275                             |
| 4         | 0.32421                        | 0.43899                             |
| 5         | 0.23466                        | 0.38321                             |

Despite the relative minimum product distance of lattices  $A_2, D_3, D_4$  and  $D_5$  being smaller than the

distances of the  $\mathbb{Z}^n$ -lattices, for  $n = 2, 3, 4, 5$  respectively, these distances can be improved if we consider algorithms that search for number fields with minimum discriminant.

## 7. Conclusion

In this work, we construct root lattices using the Taussky–Kruskemper method, which, from the generator matrix of a lattice, produces as output the generator matrix of the same lattice constructed algebraically over a totally real number field, where it is possible to compute the minimum product distance, an important parameter when the constructed lattice is regarded as a signal constellation for transmission over a Rayleigh fading channel. Through this method, one can control the discriminant of the number field used in the construction and, consequently, the minimum product distance. However, such control of the discriminant relies on computational algorithms that search for minimal discriminants, a task that may incur a high computational cost. As future work, we intend to investigate the construction of other families of root lattices in higher dimensions, such as the  $\mathbb{Z}^n$  and  $D_n$  families.

## Acknowledgment

We are grateful to the reviewers for their thorough reading of the manuscript and for the valuable comments and suggestions, which helped us to improve the work.

## References

- [1] A. A. Andrade, C. Alves, and T. B. Carlos, Rotated lattices via the cyclotomic field  $\mathbb{Q}(\zeta_{2^r})$ , *Int. J. Appl. Math.* 19(3) (2006) 321–331.
- [2] A. A. Andrade, A. J. Ferrari, C. Alves, and T. B. Carlos, Lattices via cyclotomic fields in dimensions 2 and 4, *Int. J. Appl. Math.* 20(8) (2007) 1093–1103.
- [3] A. A. Andrade, A. J. Ferrari, C. W. O. Benedito, and S. I. R. Costa, [Constructions of algebraic lattices](#), *Comput. Appl. Math.* 29(3) (2010) 1–13.
- [4] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, [PARI/GP: A Software Package for Computer-Aided Number Theory](#).
- [5] E. Bayer-Fluckiger, Lattices and number fields, *Contemp. Math.* 241 (1999) 69–84.
- [6] E. Bayer-Fluckiger, [Ideal Lattices](#), in: G. Wüstholtz, ed., *A Panorama of Number Theory or The View from Baker’s Garden*, Cambridge University Press, Cambridge (2002) 168–184.
- [7] E. Bayer-Fluckiger and G. Nebe, [On the Euclidean minimum of some real number fields](#), *J. Théor. Nombres Bordeaux* 17(2) (2005) 437–454.
- [8] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, [New algebraic constructions of rotated  \$\mathbb{Z}^n\$ -lattice constellations for the rayleigh fading channel](#), *IEEE Trans. Inform. Theory* 50(4) (2004) 702–714.
- [9] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore, [Good lattice constellations for both Rayleigh fading and Gaussian channels](#), *IEEE Trans. Inform. Theory* 42(2) (1996) 502–518.
- [10] A. Campello and J. Strapasson, [On sequences of projections of the cubic lattice](#), *Comput. Appl. Math.* 32(1) (2013) 57–69.
- [11] P. E. Conner and R. Perlis, [A Survey of Trace Forms of Algebraic Number Fields](#), World Scientific (1984).
- [12] J. H. Conway and N. J. A. Sloane, [Sphere Packings, Lattices and Groups](#), vol. 290 in *Grundlehren der mathematischen Wissenschaften*, Springer, New York (1999).

- [13] A. J. Ferrari, A. A. Andrade, R. R. Araujo, and J. C. Interlando, [Trace forms of certain subfields of cyclotomic fields and applications](#), J. Algebra Comb. Discrete Struct. Appl. 7(2) (2020) 141–160.
- [14] A. J. Ferrari, A. A. Andrade, J. C. Interlando, and C. Alves, [Characterizations of totally real subfields of 2-power cyclotomic fields and applications to signal set design](#), J. Algebra Comb. Discrete Struct. Appl. 11(2) (2024) 73–81.
- [15] A. J. Ferrari, G. C. Jorge, and A. A. Andrade, [Rotated  \$D\_n\$ -lattices in dimensions power of 3](#), J. Algebra Comb. Discrete Struct. Appl. 8(3) (2021) 151–160.
- [16] M. Kruskemper, Algebraic construction of bilinear forms over  $\mathbb{Z}$ , Pub. Math. de Besancon Th (1996) 97–1997.
- [17] D. Micciancio and S. Goldwasser, [Complexity of lattice problems: a cryptographic perspective](#), The Springer International Series in Engineering and Computer Science 671 (2002).
- [18] F. Oggier, [Algebraic Methods for Channel Coding](#), Ph.D. thesis, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland (2005).
- [19] F. Oggier and E. Bayer-Fluckiger, [Best Rotated Cubic Lattice Constellations for the Rayleigh Fading Channel](#), in: IEEE International Symposium on Information Theory (ISIT), IEEE, Yokohama, Japan (2003) 37–.
- [20] O. Taussky, [On a theorem of Latimer and Macduffee](#), Canad. J. Math. 1 (1949) 300–302.
- [21] O. Taussky, [On matrix classes corresponding to an ideal and its inverse](#), Illinois J. Math. 1(1) (1957) 108–113.