ALGEBRAIC METHODS FOR CHANNEL CODING

THÈSE N^{O} 3182 (2005)

PRÉSENTÉE À LA FACULTÉ SCIENCES DE BASE

Institut de mathématiques B

SECTION DE MATHÉMATIQUES

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Frédérique OGGIER

Diplôme de Mathématiques et Informatique, Université de Genève
de nationalité suisse et originaire de Salquenen (VS)

acceptée sur proposition du jury:

Prof. E. Bayer Fluckiger, Prof. R. Urbanke, directeurs de thèse
Prof. J.-C. Belfiore, rapporteur
Prof. J. Morales, rapporteur
Prof. A. Shokrollahi, rapporteur

Lausanne, EPFL
2005

Acknowledgements

First of all, I would like to thank my advisors, Prof. Eva Bayer-Fluckiger and Prof. Rüdiger Urbanke. This work would not exist without them. I also thank Prof. John H. Maddocks, Prof. Jean-Claude Belfiore, Prof. Jorge Morales and Prof. Amin Shokrollahi for accepting to be in the committee.

Un grand merci à tous mes collègues mathématiciens pour leur disponibilité et leur enthousiasme à discuter des questions mathématiques. Merci à Christian Maire (notamment pour ses conseils sur la théorie du corps de classe), à Stéphane Vinatier et à Grégory Berhuy (que ce soit pour ses conseils sur les réseaux ou sur les algèbres centrales simples). Merci à Philippe Chabloz, à Marina Monsurrò et à Leonardo Zapponi pour leur enthousiasme. Enfin merci à Emmanuel Lequeu pour ses conseils sur la théorie des algèbres centrales simples.

Ringrazio Emanuele Viterbo per la collaborazione, per la sua disponibilità e per tutto quello che mi ha insegnato.

A special thanks to Sergio Servetto, who first supervised my research work.

Finally, I would like to thank the researchers I had the opportunity to work with. I thank N.J.A Sloane who accepted to be my host while I was visiting AT&T Shannon Labs. It was a great pleasure to work with him. I also thank Suhas Diggavi and Jean-Claude Belfiore for their collaboration.

Abstract

This work is dedicated to developing algebraic methods for channel coding. Its goal is to show that in different contexts, namely single-antenna Rayleigh fading channels, coherent and non-coherent MIMO channels, algebraic techniques can provide useful tools for building efficient coding schemes.

Rotated lattice signal constellations have been proposed as an alternative for transmission over the single-antenna Rayleigh fading channel. It has been shown that the performance of such modulation schemes essentially depends on two design parameters: the modulation diversity and the minimum product distance. Algebraic lattices, i.e., lattices constructed by the canonical embedding of an algebraic number field, or more precisely ideal lattices, provide an efficient tool for designing such codes, since the design criteria are related to properties of the underlying number field: the maximal diversity is guaranteed when using totally real number fields and the minimum product distance is optimized by considering fields with small discriminant. Furthermore, both shaping and labelling constraints are taken care of by constructing $\mathbb{Z}^n$-lattices. We present here the construction of several families of such n-dimensional lattices for any n, and compute their performance. We then give an upper bound on their minimal product distance, and show that with respect to this bound, existing lattice codes are optimal in the sense that no further significant coding gain could be reached.

Cyclic division algebras have been introduced recently in the context of coherent Space-Time coding. These are non-commutative algebras which naturally yield families of invertible matrices, or in other words, linear codes that fullfill the rank criterion. In this work, we further exploit the algebraic structures of cyclic algebras to build Space-Time Block codes (STBCs) that satisfy the following properties: they have full rate, full diversity, non-vanishing constant minimum determinant for increasing spectral efficiency, uniform average transmitted energy per antenna and good shaping. We give algebraic constructions of such STBCs for 2, 3, 4 and 6 antennas and show that these are the only cases where they exist.

We finally consider the problem of designing Space-Time codes in the noncoherent case. The goal is to construct maximal diversity Space-Time codewords, subject to a fixed constellation constraint. Using an interpretation of the noncoherent coding problem in terms of packing subspaces according to a given metric, we consider the construction of non-intersecting subspaces on finite alphabets. Techniques used here mainly derive from finite projective geometry.

Version abrégée

Ce travail est consacré au développement de méthodes algébriques pour le codage de canal. Son objectif est de montrer que dans différents contextes, à savoir les canaux à évanouissement de Rayleigh pour une antenne et les canaux à antennes multiples pour les cas cohérent et non-cohérent, des méthodes algébriques peuvent fournir des outils efficaces pour la construction de codes.

Des constellations de signaux formées à partir de réseaux tournés ont été proposées comme alternative pour la transmission sur des canaux à évanouissement de Rayleigh pour une antenne. Il a été montré que la performance de tels schémas de modulation dépend essentiellement de deux paramètres: la diversité en modulation et la distance produit minimale. Les réseaux algébriques, i.e., les réseaux construits par plongement d'un corps de nombres, ou plus précisément les réseaux idéaux, s' avèrent être un outil adapté, puisque les critères de performance peuvent être exprimés en terme de propriétés du corps de nombres sousjacent: la diversité maximale est garantie lorsque l'on considère des corps totalement réels, alors que la distance produit minimale peut être optimisée en considérant des corps de petit discriminant. De plus, les contraintes de forme de la constellation ainsi que son étiquettage sont prises en compte en construisant des réseaux $\mathbb{Z}^n$. Nous présentons ici la construction de plusieurs familles de tels réseaux n-dimensionaux pour tout n, et calculons leur performance. Nous donnons ensuite une borne supérieure à la distance produit minimale, et montrons que par rapport à cette borne, les codes en réseaux existants sont optimaux, dans le sens qu'il n'est pas possible d'obtenir de gain de codage significatif.

Les algèbres cycliques à division ont été introduites récemment dans le cadre du codage spatio-temporel cohérent. Ces dernières sont des algèbres non-commutatives qui fournissent naturellement des familles de matrices inversibles, ou en d' autres mots, des codes linéaires qui satisfont le critère du rang. Dans ce travail, nous exploitons les structures algébriques des algèbres cycliques pour construire des codes spatio-temporels qui possèdent les propriétés suivantes: ils ont un débit maximal, une diversité maximale, un déterminant minimum constant qui ne diminue pas lorsque l' efficacité spectrale augmente, une énergie moyenne transmise par antenne qui est uniforme et finalement aucune perte de forme. Nous présentons des constructions algébriques de tels codes pour 2, 3, 4 et 6 antennes et montrons que ces dimensions sont les seules qui existent.

Nous considérons finalement le problème du codage spatio-temporel dans le cas non-cohérent. Le but est de construire des codes spatio-temporels ayant diversité maximale, et sujets à une contrainte sur la constellation de signaux utilisée. En utilisant l' interprétation du codage dans le cas non-cohérent en terme d'empilement de sous-espaces en fonction d' une certaine métrique, nous considérons la construction de sous-espaces qui ne s' intersectent pas sous la contrainte d' un alphabet fini. Les techniques utilisées ici découlent principalement de géométrie projective finie.

Contents

Introduction

Elementary number theory was the basis of the development of error correcting codes in the early years of coding theory. Finite fields were the key tool in the design of powerful binary codes and gradually entered in the general mathematical background of communications engineers. Thanks to the technological developments, attention moved to the design of signal space codes in the framework of coded modulation systems. Here, the theory of Euclidean lattices became of great interest for the design of dense signal constellations well suited for transmission over the Additive White Gaussian Noise channel.

More recently, the incredible boom of wireless communications forced coding theorists to deal with fading channels. New code design criteria had to be considered in order to improve the poor performance of wireless transmission systems. It is in that context that rotated lattice signal constellations have been proposed for transmission over the single-antenna Rayleigh fading channel. It has been shown that algebraic lattices, i.e., lattices constructed by the canonical embedding of an algebraic number field, provide an efficient tool for designing such lattice codes. The reason is that the two main design parameters, namely the modulation diversity and the minimum product distance, can be related to properties of the underlying number field: the maximal diversity is guaranteed when using totally real number fields and the minimum product distance can be related to the field discriminant. Furthermore, both shaping and labelling constraints are taken care of by constructing $\mathbb{Z}^n$-lattices.

The first part of this work is dedicated to algebraic lattices for a single-antenna Rayleigh fading channel. In Chapter 1, we recall the channel model considered, and explain how design criteria are derived. In Chapter 2, we introduce the definition of ideal lattices, and prove some of their properties that are related to the lattice code parameters. Finally we present in Chapter 3 the construction of such n-dimensional lattices and compute their performance. We then give an upper bound on their minimal product distance, and show that with respect to this bound, existing lattice codes are optimal in the sense that no further significant coding gain could be reached.

These last ten years, the need for higher data transmission has led to consider communication channels using multiple antennas. Efficient coding schemes for MIMO channels are still today a very active area of research. The second part of this work considers the design of such codes, in the so-called coherent and noncoherent case.

More complicated channel models required more sophisticated tools for code design, and only recently cyclic division algebras have been introduced in the context of coherent Space-Time coding. These are non-commutative algebras which naturally yield families of invertible matrices, or in other words, linear codes that fullfill the rank criterion. In Chapter 5, we first recall well known results on cyclic algebras, before exploiting further the algebraic structures of cyclic algebras to show why there are an adapted tool for building Space-Time Block codes (STBCs). Thanks to the properties derived, we construct in Chapter 6 STBCs that satisfy the following properties: they have full rate, full diversity, non-vanishing constant minimum determinant for increasing spectral efficiency, uniform average transmitted energy per antenna and good shaping. We give algebraic constructions of such STBCs for 2, 3, 4 and 6 antennas and show that these are the only cases where they exist.

We finally consider in Chapter 7 the problem of designing Space-Time codes in the noncoherent case. The goal is to construct maximal diversity Space-Time codewords, subject to a fixed constellation constraint. Here we first recall how the noncoherent coding problem can be interpreted in terms of packing subspaces according to a given metric. Using techniques that are mainly derive from finite projective geometry, we then consider the construction of non-intersecting subspaces on finite alphabets.

CHAPTER 1

Code Design Criteria for the Rayleigh Fading Channel

We consider the transmission of data over a single antenna fading channel. In this chapter, we focus on the design criteria for such a channel. We start by detailing both the channel and the transmission system model that we consider. Though most of the analysis we present is valid for any code constellation, we focus on lattice codes. We then present the design parameters related to the model: *diversity* and *product distance*. Finally, we discuss how the labelling and shaping problem motivate the choice of particular lattice code constructions.

1. The Fading Channel Model

We consider a wireless channel modeled as an independent Rayleigh flat fading channel. We assume that perfect *Channel State Information* (CSI) is available at the receiver and no inter-symbol interference is present. The discrete time model of the channel is given by

$$r' = \alpha' x + n' \tag{1}$$

where x is a symbol from a complex signal set, n' is the complex white Gaussian noise and α' the complex zero mean Gaussian fading coefficient (see Fig. 1). The complex

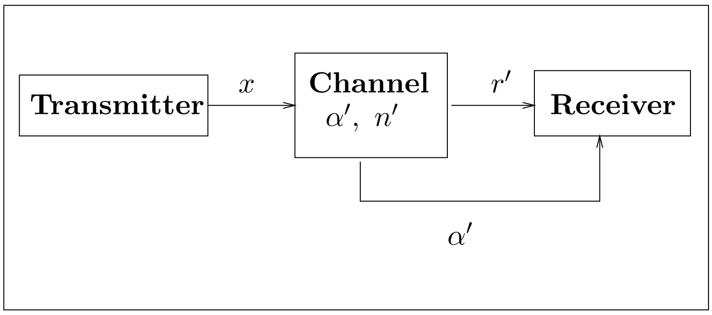

FIGURE 1. The channel model: the transmitter sends a complex symbol x, the channel attenuates the signal (this is modeled by the fading α') and adds noise (n'), so that the receiver gets the modified symbol $r' = \alpha' x + n'$. We assume the receiver estimates the channel (i.e. α').

fading coefficients are assumed to be independent from one symbol to the next. This assumption can be made reasonable by introducing a channel interleaver which breaks up the actual fading process correlations.

Since CSI is available at the receiver, the phase φ of the fading coefficient $\alpha' = |\alpha'|e^{i\varphi}$ can be removed, so that we get

$$r = \alpha x + n, \tag{2}$$

where $\alpha = |\alpha'|$ is now a real Rayleigh distributed fading coefficient and $n = n'e^{-i\varphi}$ remains the complex white Gaussian noise. In this case, both in-phase and quadrature components of the transmitted symbol are subject to the same fading. In order to fully exploit the diversity capabilities of the codes, we will additionally introduce an *in-phase/quadrature component interleaver* which will enable us to consider the fading channel model in (2), where we assume that $x \in \mathbb{R}$, n is a real Gaussian random variable and the fading coefficients are independent from one real transmitted symbol to the next.

When considering coded transmissions, codewords will be n-dimensional real vectors $\mathbf{x} = (x_1, \ldots, x_n)$ taken from some finite signal constellation $S \subseteq \mathbb{R}^n$. Each vector component is assumed to be affected by an independent real fading coefficient[1]. This is possible by implementing the modulator as follows (see Fig. 2). Given a pair of codewords $\mathbf{x}$ and $\mathbf{y}$, the component interleaver swaps the quadrature components between the two codewords in a chosen way. For example, $x_{2j} \leftrightarrow y_{2j}$, $j = 1, \ldots, n/2$, n even, as shown in Fig. 2-(a). Then, a pairing of the components yields complex symbols (of the form $x_j + iy_{j+1}$, j odd). Each of them is sent over a time interval T (see Fig. 2-(b)) and affected by the fading (that we can now assume real) and the complex noise: $(x_j + iy_{j+1})\alpha_j + n_j$. Finally, the deinterleaver at the receiver rebuilds a real vector

$$x_j\alpha_j + iy_{j+1}\alpha_j + \Re(n_j) + i\Im(n_j) \leftrightarrow \begin{pmatrix} x_j\alpha_j + \Re(n_j) \\ y_{j+1}\alpha_j + \Im(n_j) \end{pmatrix}$$

from which it restores the two initial codewords, now affected by real independent fading coefficients (see Fig. 2-(c)).

[1] This assumption will be of importance later for the computation of the channel error probability.

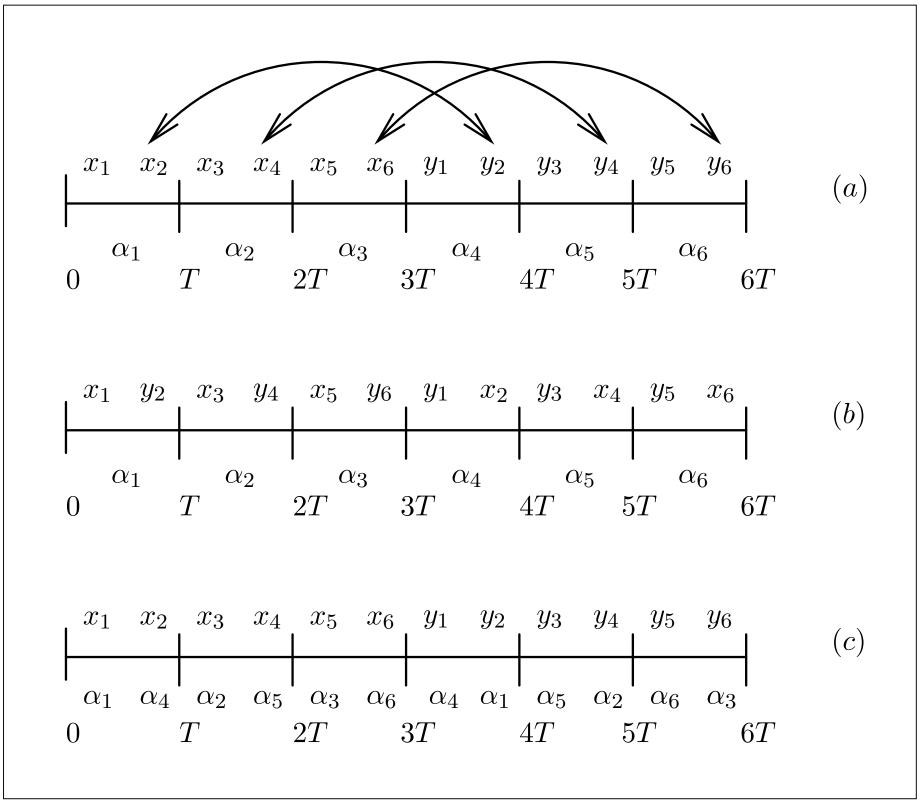
x_1 x_2 x_3 x_4 x_5 x_6 y_1 y_2 y_3 y_4 y_5 y_6
(a)
α_1 α_2 α_3 α_4 α_5 α_6
0 T $2T$ $3T$ $4T$ $5T$ $6T$
x_1 y_2 x_3 y_4 x_5 y_6 y_1 x_2 y_3 x_4 y_5 x_6
(b)
α_1 α_2 α_3 α_4 α_5 α_6
0 T $2T$ $3T$ $4T$ $5T$ $6T$
x_1 x_2 x_3 x_4 x_5 x_6 y_1 y_2 y_3 y_4 y_5 y_6
(c)
α_1 α_4 α_2 α_5 α_3 α_6 α_4 α_1 α_5 α_2 α_6 α_3
0 T $2T$ $3T$ $4T$ $5T$ $6T$

FIGURE 2. The channel component interleaver/deinterleaver: (a) before interleaving at the transmitter, (b) on the channel, (c) after deinterleaving at the receiver.

REMARK 1.1. We considered a *real* fading channel model. An alternative approach is the *complex* fading model, consisting of the model described in (1) with a complex fading. In this case, the I/Q component interleaver is no more required.

2. The Transmission System

Based on the above considerations on the channel model, we consider the communication system shown in Fig. 3. The mapper associates an m-tuple of input bits to a signal point $\mathbf{x} = (x_1, x_2, \dots x_n)$ in the n-dimensional Euclidean space $\mathbb{R}^n$. Each point is labeled with an m-bit binary label. The spectral efficiency will be measured in number of bits per two dimensions

$$\eta = \frac{2m}{n}. \tag{3}$$

When using lattice codes, $\mathbf{x}$ belongs to an n-dimensional signal constellation S (of cardinality 2^m) carved from the set of lattice points $\Lambda = \{\mathbf{x} = \mathbf{u}M\}$, where $\mathbf{u}$ is an integer

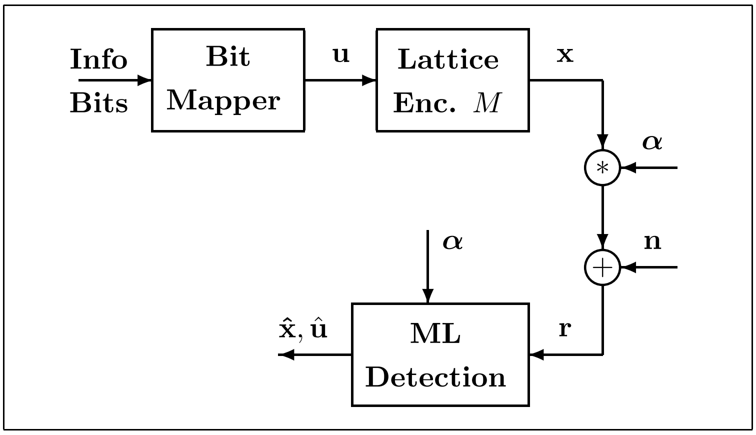

FIGURE 3. Transmission system model: the information bits are mapped to a signal point $\mathbf{x} \in \mathbb{R}^n$. In the case of lattice codes, they are first mapped to a point $\mathbf{u} \in \mathbb{Z}^n$, which is then mapped to a signal point $\mathbf{x} \in \mathbb{R}^n$ using a lattice encoder.

vector and M is the lattice generator matrix. The information bits are used to label the integer components of $\mathbf{u}$, as detailed in Section 4.

The constellation points are transmitted over an independent Rayleigh fading channel as described in Section 1, i.e.,

$$\mathbf{r} = \mathbf{xH} + \mathbf{n}.$$

Recall that $\mathbf{r} = (r_1, \ldots, r_n)$ is the received point, $\mathbf{n} = (n_1, n_2, \ldots n_n)$ is a noise vector, whose real components n_i are zero mean, N_0 variance Gaussian distributed independent random variables and $\mathbf{H} = \mathrm{diag}(\alpha_1, \alpha_2, \ldots \alpha_n)$ is the diagonal channel fading matrix, where the α_i are independent real Rayleigh random variables with unit second moment (i.e., $E[\alpha_i^2] = 1$), that is, the channel power gain is assumed normalized.

Assuming perfect CSI, *Maximum Likelihood* (ML) detection requires the minimization of the following metric

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2. \tag{4}$$

In other words, the decoded point $\hat{\mathbf{x}}$ satisfies

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in S} \|\mathbf{r} - \mathbf{xH}\|^2 = \arg\min_{\mathbf{x}' \in S'} \|\mathbf{r} - \mathbf{x}'\|^2, \tag{5}$$

where $S' = \mathbf{H}S$ is the "faded signal constellation". The minimization of (5) can be a very complex operation for an arbitrary signal set with a large number of points.

REMARK 2.1. In the case of lattice codes, a more efficient ML detection is done by applying the *Sphere Decoder*, a universal lattice decoder [**53**]. Having decoded $\hat{\mathbf{x}}$, we then obtain the corresponding integer component vector $\hat{\mathbf{u}}$ from which the decoded bits can be extracted.

3. Searching for Optimal Lattice Constellations

In order to derive code design criteria for the above system, we estimate its error probability.

Denote by $P_e(S)$ the probability of error when sending a point of the finite signal constellation S, and by $P(\mathbf{x} \rightarrow \hat{\mathbf{x}})$ the pairwise error probability, the probability that, when $\mathbf{x}$ is transmitted, the received point is "closer" to $\hat{\mathbf{x}}$ than to $\mathbf{x}$ according to the metric defined in (4).

For an arbitrary signal constellation S, we have

$$P_e(S) = \frac{1}{|S|} \sum_{\mathbf{x} \in S} P_e(S|\mathbf{x} \text{ transmitted}).$$

This can be simplified a lot in the case of lattice codes. Since an infinite lattice is *geometrically uniform*, we may simply write the probability of error when sending a point of the lattice $P_e(\Lambda) = P_e(\Lambda|\mathbf{x})$ for any transmitted point $\mathbf{x} \in \Lambda$. Let us then assume that S is a finite constellation carved from Λ.

We now apply the union bound which gives an upper bound to the point error probability

$$P_e(S) \leq P_e(\Lambda) = \bigcup_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x} \rightarrow \hat{\mathbf{x}}) \leq \sum_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x} \rightarrow \hat{\mathbf{x}}) \tag{6}$$

where the first inequality takes into account the edge effects of the finite constellation S compared to the infinite lattice Λ.

We first derive an upper bound for the conditional error probability $P(\mathbf{x} \rightarrow \hat{\mathbf{x}}|\boldsymbol{\alpha})$. An error occurs while decoding with the ML rule (4) if the received point $\mathbf{r}$ is closer to $\hat{\mathbf{x}}$ than to $\mathbf{x}$, i.e., if $m(\hat{\mathbf{x}}|\mathbf{r}, \boldsymbol{\alpha}) \leq m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha})$. The conditional pairwise error probability is given by

$$\begin{aligned} P(\mathbf{x} \to \hat{\mathbf{x}}|\boldsymbol{\alpha}) &= P(\sum_{i=1}^{n} |r_i - \alpha_i \hat{x}_i|^2 \leq \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \mid \mathbf{x} \text{ transmitted}) \\ &= P(\sum_{i=1}^{n} |\alpha_i (x_i - \hat{x}_i) + n_i|^2 \leq \sum_{i=1}^{n} |n_i|^2) \\ &= P(\sum_{i=1}^{n} \alpha_i^2 (x_i - \hat{x}_i)^2 + 2 \sum_{i=1}^{n} \alpha_i (x_i - \hat{x}_i) n_i \leq 0) \ . \end{aligned}$$

Let $\chi = \sum_{i=1}^{n} \alpha_i (x_i - \hat{x}_i) n_i$ be a linear combination of the Gaussian random variables n_i, that is, χ is Gaussian with zero mean and variance

$$\sigma_\chi^2 = N_0 \sum_{i=1}^{n} \alpha_i^2 (x_i - \hat{x}_i)^2 \ .$$

Let $A = \frac{1}{2} \sum_{i=1}^{n} \alpha_i^2 (x_i - \hat{x}_i)^2$ be a constant. We can write the conditional pairwise error probability in terms of χ and A:

$$P(\mathbf{x} \to \hat{\mathbf{x}}|\boldsymbol{\alpha}) = P(\chi \geq A) = Q(A/\sigma_\chi)$$

where $Q(x) = (2\pi)^{-1} \int_x^\infty \exp(-t^2/2) dt$ is the Gaussian tail function. Since $Q(x)$ can be upper bounded by an exponential $Q(x) \leq \frac{1}{2} \exp(-x^2/2)$, the conditional pairwise error probability becomes

$$P(\mathbf{x} \to \hat{\mathbf{x}}|\boldsymbol{\alpha}) \leq \frac{1}{2} \exp(-\frac{A^2}{2\sigma_\chi^2}) = \frac{1}{2} \exp(-\frac{1}{8N_0} \sum_{i=1}^{n} \alpha_i^2 (x_i - \hat{x}_i)^2) \ .$$

The pairwise error probability $P(\mathbf{x} \to \hat{\mathbf{x}})$ is computed by averaging $P(\mathbf{x} \to \hat{\mathbf{x}}|\boldsymbol{\alpha})$ over the fading coefficients $\boldsymbol{\alpha}$:

$$P(\mathbf{x} \to \hat{\mathbf{x}}) = \int P(\mathbf{x} \to \hat{\mathbf{x}}|\boldsymbol{\alpha}) \mathbf{p}(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \leq \frac{1}{2} \int \exp(-\frac{1}{8N_0} \sum_{i=1}^{n} \alpha_i^2 (x_i - \hat{x}_i)^2) \mathbf{p}(\boldsymbol{\alpha}) d\boldsymbol{\alpha}.$$

The differential probability is $\mathbf{p}(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = p(\alpha_1) \cdots p(\alpha_n) d\alpha_1 \cdots d\alpha_n$, where $p(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$ is the normalized Rayleigh distribution. Replacing in the last inequality we obtain

$$\begin{aligned} P(\mathbf{x} \to \hat{\mathbf{x}}) &\leq \frac{1}{2} \prod_{i=1}^{n} \int_0^\infty \exp(-\frac{1}{8N_0} \alpha_i^2 (x_i - \hat{x}_i)^2) p(\alpha_i) d\alpha_i \\ &= \frac{1}{2} \prod_{i=1}^{n} \int_0^\infty 2\alpha_i \exp(-C_i \alpha_i^2) d\alpha_i \end{aligned}$$

where $C_i = 1 + (x_i - \hat{x}_i)^2 / (8N_0)$. Computing the integral, we obtain

$$P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \frac{1}{2} \prod_{i=1}^{n} \frac{1}{1 + \frac{(x_i - \hat{x}_i)^2}{8N_0}} \ . \tag{7}$$

For large signal to noise ratios

$$P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \frac{1}{2} \prod_{x_i \neq \hat{x}_i} \frac{1}{\frac{(x_i - \hat{x}_i)^2}{8N_0}} = \frac{1}{2} \frac{(8N_0)^l}{d_p^{(l)}(\mathbf{x}, \hat{\mathbf{x}})^2} \tag{8}$$

where

$$d_p^{(l)}(\mathbf{x}, \hat{\mathbf{x}}) = \prod_{x_i \neq \hat{x}_i} |x_i - \hat{x}_i| \tag{9}$$

is the *l-product distance* of $\mathbf{x}$ from $\hat{\mathbf{x}}$ when these two points differ in l components. Rearranging equation (6), we obtain

$$P_e(S) \leq \sum_{l=L}^{n} \frac{1}{2} \frac{(8N_0)^l}{d_p^{(l)}(\mathbf{x}, \hat{\mathbf{x}})^2} \ , \tag{10}$$

where L is the minimum number of different components of any two distinct constellation points. It is called *modulation diversity* or *diversity order* of the signal constellation. In other words, L is the minimum Hamming distance between any two coordinate vectors of the constellation points.

The dominant terms in the sum (10) are found for $L = \min(l)$. Among the terms in (10) satisfying $L = \min(l)$, the dominant term is found for $d_{p,min} = \min d_p^{(L)}$. This thus gives us all the ingredients to obtain a low error probability asymptotically. In order of relevance we have to

$$\boxed{\begin{array}{l}(1)\ \text{Maximize the diversity } L = \min(l).\\ (2)\ \text{Maximize } d_{p,min} = \min(d_p^{(L)}(\mathbf{x}, \hat{\mathbf{x}})).\end{array}}$$

Remark 3.1. The diversity is obviously bounded by the dimension n of the constellation, so that the maximal diversity is $L = n$. Consequently, high diversity is obtained in high dimension.

Remark 3.2. Note that the bound (10) still holds in the case of complex fading.

The performance between two systems S_1, S_2 having the same diversity can be compared via their minimum product distance [**8**], that we denote by $d_{p,min}(S_i)$, $i = 1, 2$.

Definition 3.1. *The asymptotic coding gain between two systems having the same spectral efficiency and the same diversity L is given by*

$$\gamma_{asympt.} = \left(\frac{d_{p,min}(S_1)}{d_{p,min}(S_2)} \right)^{1/L} \tag{11}$$

with the definitions given above.

In general, the asymptotic coding gain may not be defined for systems with different diversities L_1 and L_2; in such cases the coding gain varies with the signal to noise ratio.

4. Rotated $\mathbb{Z}^n$–lattice Constellations

In the design of signal constellations, two more fundamental operations should always be kept in mind: bit labelling and constellation shaping. These issues may be very critical for the complexity of practical implementations and are strictly related to each other.

Recall that the bit labelling consists in mapping the input bits to the points in the signal constellation. If we want to avoid the use of a huge look-up table to perform bit labelling, we need a simple algorithm that maps bits to signal points. When considering a lattice constellation

$$\Lambda = \{\mathbf{x} = \mathbf{u}M : \mathbf{u} = (u_1, \dots, u_n) \in S_0^n\},$$

the simplest labelling algorithm we can use is obtained by performing the bit labelling on the integer components u_i of the vector $\mathbf{u}$. These are usually restricted to a so-called $2^\eta/2$-PAM constellation $S_0 = \{\pm 1, \pm 3, \dots, \pm(2^\eta/2 - 1)\}$, where η is the number of bits per 2-dimension as defined in (3). Gray bit labelling of each $2^\eta/2$-PAM one dimensional component proved to be the most effective strategy to reduce bit error performance. If we restrict ourselves to the above simple labelling algorithm, we observe that this induces a constellation shape similar to the fundamental parallelotope of the underlying lattice.

On the other hand, it is well known that constellations bounded by a sphere have the best shaping gain. Unfortunately, labelling a spherically shaped constellation is not always an easy task, without using a look-up table. Thus a good trade-off is to choose a lattice whose fundamental paralletope shape won't induce too much energy loss.

Cubic shaped lattice constellations are good candidates: they are only slightly worse in terms of shaping gain but are usually easier to label.

We conclude this chapter by summarizing some of the reasons why lattice codes provide good codes for the fading channel model considered.

- The computation of the error probability shows that the diversity is the first parameter to optimize. As pointed out (see Remark 3.1), we need to build constellations in high dimension, and lattices have a structure convenient to handle in dimension n, even for n big.
- The decoding complexity is an important issue. Maximum likelihood can be performed efficiently on lattice codes using the Sphere Decoder (see Remark 2.1).
- As shown above, restricting to $\mathbb{Z}^n$–lattice codes offers both efficient shaping and labelling.

The problem that can now be addressed is the construction of such $\mathbb{Z}^n$-lattices with maximal diversity and optimal minimum product distance. This will be discussed in the next chapters, through the concept of *ideal lattices*.

CHAPTER 2

Ideal Lattices

Algebraic lattices are lattices obtained via the ring of integers of a number field. This chapter is dedicated to *ideal lattices*, i.e., more general algebraic lattices endowed with a trace form. We will define both *real* and *complex* ideal lattices, and focus on two properties: their diversity and minimum distance. Motivated by the communication problem of Chapter 1, we look for both maximal diversity and maximal minimum product distance.

1. First Definitions

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$, of degree $n = [K : \mathbb{Q}]$. Let $\bar{\ }: K \to K$ denote a $\mathbb{Q}$-linear involution of K, i.e., an additive and multiplicative map such that $\bar{\bar{x}} = x$ for all $x \in K$. The set $F = \{x \in K \mid \bar{x} = x\}$ is a field, called the *fixed field* of the involution.

Let $\mathcal{O}_K$ be the ring of integers of K. Recall that $\mathcal{O}_K$, as well as more generally any non-zero ideal of $\mathcal{O}_K$, is a free $\mathbb{Z}$-module of rank n. It thus has a $\mathbb{Z}$–basis with n elements, called an *integral basis* of K. Let $\mathcal{D}_{K/\mathbb{Q}}$ be the *different* of $K/\mathbb{Q}$. It is an integral ideal, whose inverse $\mathcal{D}_{K/\mathbb{Q}}^{-1} = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$ is called the *codifferent* of $K/\mathbb{Q}$. An integral lattice is a pair (L, b), where L is a free $\mathbb{Z}$-module of finite rank n, and $b : L \times L \to \mathbb{Z}$ is a symmetric, $\mathbb{Z}$-bilinear form. The lattice (L, b) is said to be positive (resp. negative) *definite* if $b(x, x) > 0$ (resp. $b(x, x) < 0$) for all $0 \neq x \in L$.

Definition 1.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$, and let $\alpha \in F$ be such that $\alpha\mathcal{I}\bar{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$. An* ideal lattice *is an integral lattice $(\mathcal{I}, b_\alpha)$, where*

$$b_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z},\ b_\alpha(x, y) = Tr_{K/\mathbb{Q}}(\alpha x\bar{y}),\ \forall x, y \in \mathcal{I}.$$

Note that the condition $\alpha\mathcal{I}\bar{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$ guarantees the lattice to be integral, and α is chosen to be in F, so that the trace form is symmetric:

$$b_\alpha(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x\bar{y}) = \overline{\mathrm{Tr}_{K/\mathbb{Q}}(\bar{\alpha}\bar{x}y)} = b_\alpha(y, x),$$

where last equality holds since $\mathrm{Tr}_{K/\mathbb{Q}}(z) \in \mathbb{Q}$ for all $z \in K$. Given a number field K, definite ideal lattices do not always exist. We have the following result, proven in [**3**].

PROPOSITION 1.1. *There exists a definite ideal lattice $(\mathcal{I}, b_\alpha)$ if and only if F is totally real, and either $K = F$, or K is a totally imaginary quadratic extension of F.*

In other words, K has to be totally real or *CM*.

DEFINITION 1.2. *A number field K is called a* CM-field if there exists a totally real number field F such that K is a totally imaginary quadratic extension of F.

Note that in the case of CM-fields, the $\mathbb{Q}$-linear involution is given by the complex conjugation.

REMARK 1.1. Denote by K^{Gal} the Galois closure of K. Notice that if K is a CM field, then complex conjugation commutes with all the elements of $\mathrm{Gal}(K^{Gal}/\mathbb{Q})$.

2. Embeddings and Diversity

Let K be a number field of degree n and denote by $\{\sigma_j\}_{j=1}^n$ its embeddings into $\mathbb{C}$. Let r_1 be the number of real embeddings and r_2 the number of pairs of imaginary embeddings of K, so that we have $n = r_1 + 2r_2$. The pair (r_1, r_2) is called the *signature* of K. Let us order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$.

DEFINITION 2.1. *We call* canonical embedding *the homomorphism $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ defined by*

$$\sigma(x) = (\sigma_1(x) \ldots \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$, we define $\sigma : K \to \mathbb{R}^n$ by

$$\begin{aligned} \sigma(x) \quad = \quad & (\sigma_1(x), \ldots \sigma_{r_1}(x), \\ & \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)) \in \mathbb{R}^n \end{aligned} \tag{12}$$

where $\Re$ and $\Im$ denote resp. the real and imaginary part.

Thanks to the canonical embedding, a basis of K can be embedded into $\mathbb{R}^n$ so as to give a basis in $\mathbb{R}^n$.

THEOREM 2.1. [**47**, p. 154] *If $\{\omega_1, \ldots, \omega_n\}$ is a basis for K over $\mathbb{Q}$, then $\sigma(\omega_1), \ldots,$ $\sigma(\omega_n)$ are linearly independent over $\mathbb{R}^n$.*

PROOF. It is sufficient to prove that $D = \det(\sigma(\omega_i)_{i=1}^n)$ is non-zero, where $\sigma(\omega_j)$ is the canonical embedding of ω_j as defined in (12). Denote by $c_R(j)$, resp. $c_I(j)$, the column $(\Re\sigma_{r_1+j}(\omega_i))_{i=1}^n$, resp. $(\Im\sigma_{r_1+j}(\omega_i))_{i=1}^n$, $j = 1,\ldots,r_2$. Replace $c_R(j)$ by $c_R(j) + ic_I(j)$, then $c_I(j)$ by $(-2i)c_I(j)$, and finally add $c_R(j)$ to $c_I(j)$, so as to obtain a new determinant $E = (-2i)^{r_2}D$. Since $E^2 = \mathrm{disc}(\omega_1,\ldots,\omega_n) \neq 0$, it follows that $D \neq 0$. □

The above notions can be slightly generalized, adjoining a *twisting element* to the embedding [**3**].

DEFINITION 2.2. *Let α be a totally real, totally positive element of K, i.e., $\sigma_i(\alpha)$ is real and positive for all i. Set $\alpha_i = \sigma_i(\alpha)$. Let $\sigma_\alpha : K \to \mathbb{R}^n$ be the embedding defined by*

(13)
$$\begin{aligned}\sigma_\alpha(x) \quad = \quad & (\sqrt{\alpha_1}\sigma_1(x),\ldots,\sqrt{\alpha_{r_1}}\sigma_{r_1}(x),\sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)),\sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)),\\ & \ldots,\sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)),\sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))).\end{aligned}$$

We call it a twisted embedding.

The proof of Theorem 2.1 easily extends to the case of twisted embeddings, using that

$$(\sigma_\alpha(\omega_j))_{j=1}^n = (\sigma(\omega_j))_{j=1}^n \mathrm{diag}(\sqrt{\alpha_1},\ldots,\sqrt{\alpha_{r_1}},\sqrt{2\alpha_{r_1+1}},\ldots,\sqrt{2\alpha_{r_1+r_2}}),$$

so that the twisted embedding of a basis of K also gives a basis in $\mathbb{R}^n$.

COROLLARY 2.1. *Let G be a free $\mathbb{Z}$-module of rank n of $\mathcal{O}_K$ with $\mathbb{Z}$-basis $\{\omega_1,\ldots,\omega_n\}$. Then the image $\sigma_\alpha(G)$ of G in $\mathbb{R}^n$ is a lattice with generators $\sigma_\alpha(\omega_1),\ldots,\sigma_\alpha(\omega_n)$.*

So far, the main ingredient to define both the canonical and the twisted embedding of K into $\mathbb{R}^n$ is a $\mathbb{Z}$-basis with n elements. Since an ideal $\mathcal{I} \subseteq \mathcal{O}_K$ also has such a basis, we assume in the following that we are working with $\mathcal{I} \subseteq \mathcal{O}_K$ ($\mathcal{I}$ being possibly $\mathcal{O}_K$ itself). Let $\{\omega_1,\ldots,\omega_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{I}$. By Corollary 2.1, the lattice $\sigma_\alpha(\mathcal{I})$ has generators $\sigma_\alpha(\omega_1),\ldots,\sigma_\alpha(\omega_n)$.
Recall that a lattice Λ can be defined by means of its generator matrix M, i.e.,

$$\Lambda = \{\mathbf{x} = \boldsymbol{\lambda}M | \boldsymbol{\lambda} \in \mathbb{Z}^n\},$$

and its corresponding *Gram matrix* is defined by $G = MM^T$, where T denotes the transpose. The lattice $\sigma_\alpha(\mathcal{I})$ has a generator matrix M given by

(14)

$$\begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_1) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\omega_1) & \dots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\omega_1) \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \dots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_n) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\omega_n) & \dots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix}$$

where $\alpha_j = \sigma_j(\alpha),\ \forall j$.

Proposition 2.1. [**3**] *Let K be either totally real or CM. Then the lattice $\sigma_\alpha(\mathcal{I})$ is a positive definite ideal lattice.*

Proof. We show that the associated bilinear form is a trace form. We have $G = MM^T = (g_{ij})_{i,j=1}^n$, with

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{r_1}\alpha_k\sigma_k(\omega_i\omega_j) + \\ &\quad \sum_{k=1}^{r_2} 2\alpha_{r_1+k}[\Re(\sigma_{r_1+k}(\omega_i))\Re(\sigma_{r_1+k}(\omega_j)) + \Im(\sigma_{r_1+k}(\omega_i))\Im(\sigma_{r_1+k}(\omega_j))] \\ &= \sum_{k=1}^{r_1}\alpha_k\sigma_k(\omega_i\omega_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k}\Re(\sigma_{r_1+k}(\omega_i)\sigma_{r_1+k}(\overline{\omega_j})) \\ &= \sum_{k=1}^{r_1}\alpha_k\sigma_k(\omega_i\omega_j) + \sum_{k=1}^{r_2}\alpha_{r_1+k}\sigma_{r_1+k}(\omega_i\overline{\omega_j}) + \sum_{k=1}^{r_2}\alpha_{r_1+k}\overline{\sigma_{r_1+k}(\omega_i\overline{\omega_j})} \\ &= \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega_i\overline{\omega_j}) \end{aligned}$$

The second equality holds since the complex conjugation commutes with all σ_i, $i = 1, \dots, n$ (see Remark 1.1). The lattice is definite (by Proposition 1.1), and positive definite since α is chosen totally positive. □

Notice the hypothesis on α, compared to Definition 1.1. Here α is no more asked to satisfy $\alpha\mathcal{I}\bar{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$. Thus, the lattice is not necessarily integral. This condition has been replaced by requiring α to be totally real and totally positive, so that $\sqrt{\alpha_j}$ is well-defined for all j.

The determinant of a lattice gives the squared volume of the fundamental region [**11**]. In the case of ideal lattices, it is related to d_K, the discriminant of the number field K. We denote it either $\det(\Lambda)$ or $\det(b)$ if $\Lambda = (L, b)$.

Proposition 2.2. [**3**] *Let $(\mathcal{I}, b_\alpha)$ be an ideal lattice. We have*

$$|\det(b_\alpha)| = N(\alpha)N(\mathcal{I})^2|d_K|.$$

Proof. Since $\mathcal{I}$ is a free $\mathbb{Z}$-submodule of rank n of $\mathcal{O}_K$, there exists (see [**47**, p.31]) a basis $u_1, \ldots, u_n$ for $\mathcal{O}_K$ and positive integers $q_1, \ldots, q_n$ such that $q_1u_1, \ldots, q_nu_n$ is a basis for $\mathcal{I}$. Expressing the generator matrix of $(\mathcal{I}, b_\alpha)$ in this basis, it is a straighforward computation to show that

$$|\det(b_\alpha)| = N(\alpha)N(\mathcal{I})N(\bar{\mathcal{I}})|d_K|.$$

□

The concept of ideal lattices has two faces. One may see a lattice in $\mathbb{R}^n$ given by its generator matrix, while one may prefer the algebraic point of view given by the embedding of a ring of integers. Before going on further, we emphasize the correspondance between the two points of view, that is between points $\mathbf{x} \in \Lambda \subseteq \mathbb{R}^n$ and algebraic integers. Using the generator matrix (14), a lattice point can be expressed as

$$\begin{aligned}
\mathbf{x} &= (x_1, \ldots, x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+r_2}) \\
&= (\sum_{i=1}^n \lambda_i \sqrt{\alpha_1}\sigma_1(\omega_i), \ldots, \sum_{i=1}^n \lambda_i \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\omega_i), \ldots, \sum_{i=1}^n \lambda_i \sqrt{2\alpha_{r_2+r_1}}\Im\sigma_{r_2+r_1}(\omega_i)), \\
&\quad \lambda_i \in \mathbb{Z},\ i = 1, \ldots, n \\
&= (\sqrt{\alpha_1}\sigma_1(\sum_{i=1}^n \lambda_i\omega_i), \ldots, \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\sum_{i=1}^n \lambda_i\omega_i), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_2+r_1}(\sum_{i=1}^n \lambda_i\omega_i)).
\end{aligned}$$

Thus

$$\mathbf{x} = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x)) = \sigma_\alpha(x)$$

for $x = \sum_{i=1}^n \lambda_i\omega_i \in \mathcal{I}$ an algebraic integer. This correspondance between a vector $\mathbf{x}$ in $\mathbb{R}^n$ and an algebraic integer x in $\mathcal{O}_K$ makes easier to compute some properties of lattices that are difficult to find in general.

Recall that given two vectors $\mathbf{x}$ and $\mathbf{u}$ in $\mathbb{R}^n$, their diversity (or minimum Hamming distance) is the number of components which differ, i.e., $\#\{i \mid x_i \neq u_i,\ i = 1, \ldots, n\}$. Given a set S of vectors in $\mathbb{R}^n$, the *diversity* or *minimum Hamming distance* of S is

$$\min_{\mathbf{x},\mathbf{u}\in S} \#\{i \mid x_i \neq u_i,\ i = 1, \ldots, n\}.$$

This definition applies to $S = \Lambda$, a lattice in $\mathbb{R}^n$. Since the lattice has a group structure, that is, the sum of two vectors of Λ is still in Λ, the Hamming distance between two vectors can be reformulated as the number of non-zero components of any vector in Λ.

Definition 2.3. *The diversity of a lattice $\Lambda \in \mathbb{R}^n$ is defined by*

$$div(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \#\{i \mid x_i \neq 0,\ i = 1, \ldots, n\}.$$

The following has been proved in [**19**] for $\alpha = 1$.

Theorem 2.2. *Ideal lattices $\Lambda = (\mathcal{I}, b_\alpha)$ exhibit a diversity*

$$div(\Lambda) = r_1 + r_2,$$

where (r_1, r_2) is the signature of K.

Proof. Let $\mathbf{x} \neq \mathbf{0}$ be an arbitrary point of Λ:

$$\mathbf{x} = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(x), \ldots, \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(x))$$

with $x \in \mathcal{I} \subseteq \mathcal{O}_K$. Since $\mathbf{x} \neq 0$, we have $x \neq 0$ and the first r_1 coefficients are non zero. The minimum number of non zero coefficients among the $2r_2$ that are left is r_2 since the real and imaginary parts of any one of the complex embeddings may not vanish simultaneously. We thus have a diversity $L \geq r_1 + r_2$. Applying the canonical embedding to $x = 1$ gives exactly $r_1 + r_2$ non zero coefficients, which concludes the proof. □

3. The Minimum Product Distance

We study the problem of computing the minimum product distance of ideal lattices. Let Λ be a lattice in $\mathbb{R}^n$. If Λ has diversity $l \leq n$, we define its l minimum product distance by

$$d^l_{p,min}(\Lambda) = \min_{\mathbf{x} \neq \mathbf{u} \in \Lambda} \prod |x_i - u_i|,$$

or equivalently, since we may consider the distance of $\mathbf{x} = (x_1, \ldots, x_n)$ from the origin, by

$$d^l_{p,min}(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \prod |x_i|,$$

where both products are taken over the l non zero components of the vectors.

By Theorem 2.2, ideal lattices built over a totally real number field (i.e., of signature $(n, 0)$) have maximal diversity. In the following, we will focus on this case, and thus we assume that the diversity is always maximal.

Definition 3.1. *Given an n-dimensional lattice Λ with full diversity $div(\Lambda) = n$, we define the* minimum product distance

$$d_{p,min}(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \prod_{i=1}^{n} |x_i|.$$

We are interested in giving a closed form expression for $d_{p,min}$.

Let K be a totally real number field of degree n with discriminant d_K. The minimum product distance of an ideal lattice is related to algebraic properties of the underlying number field.

Theorem 3.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$. The minimum product distance of an ideal lattice $\Lambda = (\mathcal{I}, b_\alpha)$ of determinant* $\det(b_\alpha)$ *is*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{d_K}} \min(\mathcal{I}),$$

where $\min(\mathcal{I}) = \min_{0 \neq x \in \mathcal{I}} \frac{|N(x)|}{N(\mathcal{I})}$.

Proof. Let $\mathbf{x} = \sigma_\alpha(x)$ be a lattice point in $\mathbb{R}^n$, with $x \in \mathcal{I} \subseteq \mathcal{O}_K$ its corresponding algebraic integer. We have:

$$\begin{aligned} d_{p,min}(\Lambda) &= \min_{0 \neq \mathbf{x} \in \Lambda} \prod_{j=1}^{n} |x_j| = \min_{x \in \mathcal{I}} \prod_{j=1}^{n} |\sqrt{\sigma_j(\alpha)} \sigma_j(x)| \\ &= \sqrt{N(\alpha)} \min_{x \neq 0 \in \mathcal{I}} |N(x)|. \end{aligned}$$

We conclude using Proposition 2.2. □

Corollary 3.1. *If $\mathcal{I}$ is principal, then the minimum product distance of Λ is*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{d_K}}.$$

Proof. This is immediate from the theorem, since $\min_{x \neq 0 \in \mathcal{I}} |N(x)| = N(\mathcal{I})$ when $\mathcal{I}$ is principal. □

We already mentioned that the construction of ideal lattices starts from a $\mathbb{Z}$-basis with n elements. So far, we have considered $\mathcal{O}_K$ and its ideals. However, there are other ways of obtaining such a basis. In other words, there are other free $\mathbb{Z}$-modules of rank n in K than $\mathcal{O}_K$ and its ideals.

Definition 3.2. *An* order $\mathfrak{O}$ *in K is a subring of K which as a $\mathbb{Z}$-module is finitely generated and of maximal rank $n = [K : \mathbb{Q}]$.*

We can show that $\mathfrak{O} \subset \mathcal{O}_K$ for any order of K, so that $\mathcal{O}_K$ is also called the *maximal order* of K. Let $\mathcal{I}$ be a non-zero ideal of $\mathfrak{O}$. Then $\mathcal{I}$ is a $\mathbb{Z}$-module of maximal rank n. What we have seen so far easily extends to an ideal of an order $\mathfrak{O}$. First note that Corollary 2.1, the definition of generator matrix (14), as well as Proposition 2.1 still hold. Proposition 2.2 also holds, replacing d_K, the discriminant of K, by disc($\mathfrak{O}$), the discriminant of the order. The minimum product distance is slightly different.

THEOREM 3.2. *Let $\mathfrak{O}$ be an order of K, and $\mathcal{I}$ be an ideal of $\mathfrak{O}$. The minimum product distance of an ideal lattice $\Lambda = (\mathcal{I}, b_\alpha)$ of determinant* $\det(b_\alpha)$ *is*

$$\sqrt{\frac{\det(b_\alpha)}{d_K}\frac{\min(\mathcal{I})}{[\mathcal{O}_K : \mathfrak{O}]}},$$

where $[\mathcal{O}_K : \mathfrak{O}]$ is the index of $\mathfrak{O}$ in $\mathcal{O}_K$.

PROOF. Let $\mathbf{x} = \sigma_\alpha(x)$ be a lattice point in $\mathbb{R}^n$, with $x \in \mathcal{I} \subseteq \mathfrak{O}$ its corresponding algebraic integer. We have, as in the proof of Theorem 3.1,

$$d_{p,min}(\Lambda) = \sqrt{N(\alpha)} \min_{0 \neq x \in \mathcal{I}} |N(x)|.$$

Proposition 2.2 for the case of a general order gives $|\det(b_\alpha)| = N(\alpha)N(\mathcal{I})N(\bar{\mathcal{I}})|\text{disc}(\mathfrak{O})|$. Since $\text{disc}(\mathfrak{O}) = d_K \cdot [\mathcal{O}_K : \mathfrak{O}]^2$, we conclude as follows:

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{\text{disc}(\mathfrak{O})}} \min(\mathcal{I}).$$

□

COROLLARY 3.2. *If $\mathcal{I}$ is principal, then the minimum product distance of Λ is*

$$\sqrt{\frac{\det(b_\alpha)}{d_K}\frac{1}{[\mathcal{O}_K : \mathfrak{O}]}}.$$

□

4. Bounds on the Minimum Product Distance

We discuss the existence of upper bounds on the minimum product distance. The aim is to figure out what would be the maximal minimum product distance attained by ideal lattices.

It is straightforward to observe that given a number field K of degree n, it is better to use the ring of integers $\mathcal{O}_K$ (Theorem 3.1) rahter than one of its orders (Theorem 3.2). We thus focus on the former case.

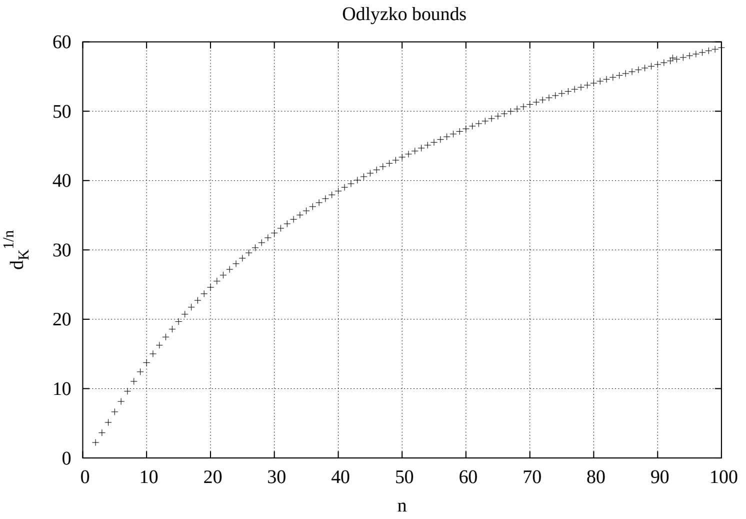

Figure 1. Odlyzko's bounds for small dimensions

Consider the case when $\mathcal{I} \subseteq \mathcal{O}_K$ is principal. Then, for a given lattice $\Lambda = (\mathcal{I}, b_\alpha)$, the quantity $d_{p,min}$ only depends on d_K, the discriminant of K, so that we can use Odlyzko's bounds. Odlyzko [**35**] derived lower bounds for the *root discriminant* $d_K^{1/n}$. Asymptotically, we have the following behaviour:

$$d_K^{1/n} \geq (60.8395...)^{r_1/n}(22.3816...)^{2r_2/n} - O(n^{-2/3}). \tag{15}$$

Bounds for lower dimensions are given in an analytic form which is hard to evaluate. Tables containing these values are available (see for example [**2**]). Odlyzko's bounds for small dimensions are shown in Figure 1.

The $d_{p,min}$ in the non-principal case gives rise to the quantity $\min(\mathcal{I})$ which is hard to evaluate. Recall that by Theorem 3.1, we have

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{d_K}} \min(\mathcal{I}), \text{ where } \min(\mathcal{I}) = \min_{x \neq 0 \in \mathcal{I}} \frac{|N(x)|}{N(\mathcal{I})}.$$

The problem is to determine whether a better $d_{p,min}$ can be obtained considering non-principal ideals. Since $\min(\mathcal{I})$ increases when the ideal is non-principal, the question is whether the discriminant increases proportionally. What seems to be true according to known tables of number fields is that the discriminant of a number field increases with its class number. The same behaviour can be observed using Odlyzko's bounds.

Example 4.1. Let K be a number field of degree n and class number $h(K)$. The Hilbert class field H of K is the unique maximal unramified abelian extension of K. It satisfies the following properties:

1. $[H : K] = h(K)$,
2. $\sqrt[m]{d_H} = \sqrt[n]{d_K}$ where $m = [H : \mathbb{Q}]$.

Take now for example K a totally real number field of degree 8. Using Odlyzko's bound, $\sqrt[8]{d_K} \geq 10.568$, that is

$$d_K \geq (10.568)^8.$$

Suppose now we add the extra constraint that $h(K) = 2$. Then there exists H with $\sqrt[16]{d_H} = \sqrt[8]{d_K}$. Using again Odlyzko's bound, we get $\sqrt[16]{d_H} \geq 18.684$. Thus now

$$d_K \geq (18.684)^8,$$

instead of $d_K \geq (10.568)^8$.

However one may argue that $\min(\mathcal{I})$ may increase as much as the discriminant, and there is no counterargument since known bounds on $\min(\mathcal{I})$ depend on the discriminant, as for example Minkowski's bound:

$$\min(\mathcal{I}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{d_K},$$

where K is a number field of degree n and signature (r_1, r_2).

Though determining $d_{p,min}$ in the non-principal case is still an open question, we will see later on some examples (see Section 4.4 of Chapter 3) that non-principal ideals yield worse values for $d_{p,min}$.

5. Complex Ideal Lattices

All the theory explained so far considered lattices over $\mathbb{Z}$. We show here that such a theory can be applied to lattices over $\mathbb{Z}[i]$. This gives rise to what we call, following [**11**], a *complex lattice*, namely

$$\Lambda^c = \{\mathbf{x} = \boldsymbol{\lambda} M : \boldsymbol{\lambda} \in \mathbb{Z}[i]^n\}, \tag{16}$$

where $M \in \mathcal{M}_n(\mathbb{C})$ is the *lattice generator matrix* and MM^H is the *Gram matrix*, where H denotes the transpose conjugate.

Let L be an extension of degree n over $\mathbb{Q}(i)$ endowed with an involution given by complex conjugation. Let $\mathcal{O}_L$ be the ring of integers of L. Since $\mathbb{Z}[i]$ is principal, $\mathcal{O}_L$ is a free $\mathbb{Z}[i]$–module of rank n.

Definition 5.1. *A* complex ideal lattice *is a* $\mathbb{Z}[i]$*–lattice* $\Lambda^c = (\mathcal{I}, b)$*, where* $\mathcal{I}$ *is an* $\mathcal{O}_L$*-ideal and*

$$b : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}[i],\ b(x,y) = Tr_{L/\mathbb{Q}(i)}(x\bar{y}),\ \forall x, y \in \mathcal{I} \tag{17}$$

where $^-$ *denotes the complex conjugation.*

We denote by $\{\sigma_1, \ldots, \sigma_n\}$ the n embeddings of the relative extension $L/\mathbb{Q}(i)$ into $\mathbb{C}$ and define the relative canonical embedding of L into $\mathbb{C}^n$ as

$$\begin{gathered} \sigma : L \to \mathbb{C}^n \\ \sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)). \end{gathered} \tag{18}$$

Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}[i]$–basis of $\mathcal{I} \subseteq \mathcal{O}_L$.

Similarly to the real case, the generator matrix of the complex algebraic lattice $\sigma(\mathcal{I})$ is

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \vdots & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_n(\omega_n) \end{pmatrix}. \tag{19}$$

Let us verify that complex ideal lattices are well-defined via their generator matrix M.

Lemma 5.1. *The matrix M as defined in (19) is the generator matrix of a complex ideal lattice if and only if complex conjugation commutes with all σ_j, $j = 1, \ldots, n$.*

Proof. We have

$$\begin{aligned} MM^H &= \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \vdots & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_n(\omega_n) \end{pmatrix} \begin{pmatrix} \overline{\sigma_1(\omega_1)} & \ldots & \overline{\sigma_1(\omega_n)} \\ \vdots & & \vdots \\ \overline{\sigma_n(\omega_1)} & \ldots & \overline{\sigma_n(\omega_n)} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^n \sigma_i(\omega_1)\overline{\sigma_i(\omega_1)} & \ldots & \sum_{i=1}^n \sigma_i(\omega_1)\overline{\sigma_i(\omega_n)} \\ \vdots & & \vdots \\ \sum_{i=1}^n \sigma_i(\omega_n)\overline{\sigma_i(\omega_1)} & \ldots & \sum_{i=1}^n \sigma_i(\omega_n)\overline{\sigma_i(\omega_n)} \end{pmatrix} \end{aligned}$$

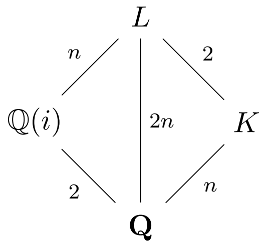

FIGURE 2. The compositum of a totally real field K and $\mathbb{Q}(i)$: relative degrees are shown on the branches

while the matrix of the trace form is given by

$$\begin{pmatrix} \sum_{i=1}^{n} \sigma_i(\omega_1\overline{\omega_1}) & \dots & \sum_{i=1}^{n} \sigma_i(\omega_1\overline{\omega_n}) \\ \vdots & & \vdots \\ \sum_{i=1}^{n} \sigma_i(\omega_n\overline{\omega_1}) & \dots & \sum_{i=1}^{n} \sigma_i(\omega_n\overline{\omega_n}) \end{pmatrix}$$

so that the complex conjugation must commute with all σ_i, $i = 1, \dots, n$. □

By Remark 1.1, we know that if we take L a CM field, then complex conjugation commutes with all σ_i, $i = 1, \dots, n$.

PROPOSITION 5.1. *Let $L/\mathbb{Q}$ be a CM field containing $\mathbb{Q}(i)$, then L is the compositum of $\mathbb{Q}(i)$ and K, its totally real subextension of degree 2.*

PROOF. Recall that K is the subfield fixed by the complex conjugation. Since L contains both $\mathbb{Q}(i)$ and K, it contains, by definition, $K\mathbb{Q}(i)$, the compositum of $\mathbb{Q}(i)$ and K. Now

$$[K\mathbb{Q}(i) : \mathbb{Q}] = [K : \mathbb{Q}][\mathbb{Q}(i) : \mathbb{Q}] = [L : \mathbb{Q}] \tag{20}$$

where the first equality holds since $K \cap \mathbb{Q}(i) = \mathbb{Q}$. This concludes the proof. □

The constructions we will deal with (see Section 6 of Chapter 3) are based on a totally complex number field L, which is the compositum of $\mathbb{Q}(i)$ and a totally real number field K as illustrated in Fig. 2. Then L is a CM field.

We now define, similarly to the real case, a *complex diversity* and a *complex mininum product distance.*

The complex diversity of a complex lattice is still the minimum Hamming distance between any two complex vectors, i.e., $\min_{0\neq\mathbf{x}\in\Lambda^c} \#\{i \mid x_i \neq 0,\ i = 1,\ldots,n\}$, with $\mathbf{x} = (x_1,\ldots,x_n)$, $x_i \in \mathbb{C}$ for all i.

PROPOSITION 5.2. *The* complex diversity *of $\Lambda^c = (\mathcal{I}, b)$, $\mathcal{I} \subseteq \mathcal{O}_L$, is n and we say that the lattice has full complex diversity.*

PROOF. Let $\mathbf{x} = (x_1,\ldots,x_n)$, $x_i \in \mathbb{C}$ for all i, be a lattice point different from the origin. Suppose that there exists an $x_j = 0$ for some $j = 1,\ldots,n$, then we get

$$0 = x_j = \sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i) = \sigma_j(\sum_{i=1}^{n} \lambda_i \omega_i),\ \ \lambda_i \in \mathbb{Z}[i] \text{ for all } i. \tag{21}$$

This implies $\sum_{i=1}^{n} \lambda_i \omega_i = 0$, a contradiction since $\{\omega_i\}_{i=1}^{n}$ is a $\mathbb{Z}[i]$-basis. □

The definition of minimum product distance can be derived from Definition 3.1.

DEFINITION 5.2. *Let $\mathbf{x} = (x_1,\ldots,x_n) \in \Lambda^c$, $x_i \in \mathbb{C}$, we define the* complex minimum product distance *as*

$$d_{p,min}(\Lambda^c) = \min_{0\neq\mathbf{x}\in\Lambda^c} \prod_{i=1}^{n} |x_i|. \tag{22}$$

We show now that the complex minimum product distance of complex ideal lattices is related to the relative discriminant.

PROPOSITION 5.3. *Let $\mathcal{I} = (\alpha)\mathcal{O}_L$ be a principal ideal of $\mathcal{O}_L$, where $L = K\mathbb{Q}(i)$ (see Fig. 2). Let $\Lambda^c = (\mathcal{I}, q)$ with*

$$\begin{array}{rccl} b: & \mathcal{I}\times\mathcal{I} & \rightarrow & \mathbb{Z}[i] \\ & (x,y) & \mapsto & c\,Tr_{L/\mathbb{Q}(i)}(x\bar{y}) \end{array} \tag{23}$$

be a complex ideal lattice over $\mathbb{Z}[i]$, where c is a normalization factor. Then

$$|\det(\Lambda^c)| = c^n |N_{L/\mathbb{Q}(i)}(\alpha)|^2\, |d_{L/\mathbb{Q}(i)}| \tag{24}$$

where $d_{L/\mathbb{Q}(i)}$ denotes the relative discriminant of L over $\mathbb{Q}(i)$.

PROOF. Let $\{\omega_j\}_{j=1}^{n}$ be a $\mathbb{Z}[i]$–basis of $\mathcal{O}_L$. By definition,

$$|\det(\Lambda^c)| = |\det\left(c\mathrm{Tr}_{L/\mathbb{Q}(i)}(\alpha\omega_j\overline{\alpha\omega_k})\right)|.$$

Notice that $\mathrm{Tr}_{L/\mathbb{Q}(i)}(\alpha\omega_j\overline{\alpha\omega_k})_{j,k=1}^n$ is a matrix of the form MAA^HM^H where M is the matrix of the embeddings as defined in (19) and A =diag$(\sigma_1(\alpha),\ldots,\sigma_n(\alpha))$. Thus

$$|\det(\Lambda^c)| = c^n|N_{L/\mathbb{Q}(i)}(\alpha)|\cdot|\det(\mathrm{Tr}_{L/\mathbb{Q}(i)}(\omega_j\overline{\omega_k})|\cdot|\overline{N_{L/\mathbb{Q}(i)}(\alpha)}|.$$

Since $\det(MM^H)=\det(M)\det(M^H)=\det(M)\overline{\det(M)}$, we have

$$|\det(\mathrm{Tr}_{L/\mathbb{Q}(i)}(\omega_j\overline{\omega_k}))| = |d_{L/\mathbb{Q}(i)}| \tag{25}$$

which concludes the proof. □

Theorem 5.1. *Let Λ^c denote a complex ideal lattice as described in Proposition 5.3, with $|\det(\Lambda^c)|=1$, we have*

$$d_{p,min}(\Lambda^c) = \frac{1}{\sqrt{|d_{L/\mathbb{Q}(i)}|}}. \tag{26}$$

Proof. Let $\{\omega_i\}_{i=1}^n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$, and $x=\sum_{i=1}^n\lambda_i\omega_i, \lambda_i\in\mathbb{Z}$.

$$\begin{aligned} d_{p,min}(\Lambda^c) &= \min_{\mathbf{x}\neq 0\in\Lambda^c}\prod_{j=1}^n|\sqrt{c}\sum_{i=1}^n\lambda_i\sigma_j(\alpha\omega_i)| \\ &= \sqrt{c^n}\min_{x\neq 0\in\mathcal{O}_L}|N_{L/\mathbb{Q}(i)}(\alpha\sum_{i=1}^n\lambda_i\omega_i)| \\ &= \sqrt{c^n}|N_{L/\mathbb{Q}(i)}(\alpha)| \end{aligned}$$

We conclude using Proposition 5.3:

$$d_{p,min}(\Lambda^c) = \sqrt{c^n}\sqrt{\frac{|\det(\Lambda^c)|}{|d_{L/\mathbb{Q}(i)}|}}\frac{1}{\sqrt{c^n}} = \frac{1}{\sqrt{|d_{L/\mathbb{Q}(i)}|}}. \tag{27}$$

□

Corollary 5.1. *If K has an odd discriminant d_K, then $d_{p,min}(\Lambda^c)=\frac{1}{\sqrt{d_K}}$.*

Proof. If d_K is odd, it satisfies $(d_K, d_{\mathbb{Q}(i)})=1$, since $d_{\mathbb{Q}(i)}=-4$. Thus, a $\mathbb{Z}[i]$–basis of L is given by the $\mathbb{Z}$–basis of K [**48**, p. 48], and $d_{L/\mathbb{Q}(i)}=d_K$. □

Remark 5.1. Since Odlyzko's bounds are valid for number fields of any signature, the bounds described in Section 4 also hold here.

CHAPTER 3

Lattice Codes

In the first chapter, we derived code design criteria for a single antenna Rayleigh fading channel. Modulation diversity, minimum product distance and shaping appeared to be, in this order of importance, the parameters to optimize. In the second chapter, we showed that in terms of algebraic lattices, these parameters can be expressed in a closed form and related to the structure of the underlying number field. Namely, the diversity depends on the signature, while the minimum product distance is related to the discriminant. Recall that in order to build efficient lattice codes, we have to satisfy the following conditions:

(1) Maximize the diversity, i.e., consider totally real number fields.

(2) Maximize the minimum product distance, i.e., minimize the discriminant of the number field.

(3) Ensure easy labelling and good shaping, i.e., build the $\mathbb{Z}^n$–lattice.

In this chapter, we show how to build lattice codes that fulfill these criteria. We develop four complementary methods for constructing $\mathbb{Z}^n$–ideal lattices in all dimensions.

(I) The cyclotomic construction: using the ring of integers of the maximal real subfield of a cyclotomic field $\mathbb{Q}(\zeta_p)$, we build the $\mathbb{Z}^n$–lattice in dimension $n = (p-1)/2$, $p \geq 5$ a prime.

(II) The cyclic construction: using the inverse of the codifferent of a cyclic field, we build the $\mathbb{Z}^n$–lattice in prime dimensions.

(III) The mixed constructions: we explain how to combine known constructions in order to find lattices in missing dimensions.

(IV) Krüskemper's method: we present an algorithm which, given a Gram matrix of a lattice, computes a generator matrix.

The cyclotomic construction is the first systematic construction that was found, though it is not available in all dimensions. The cyclic construction fills the gap in prime dimensions. The last method approaches the problem differently. It provides an algorithm which builds lattices over a number field, but with a degree of freedom on the latter. It thus allows to look for number fields with small discriminant, which optimizes the minimum product distance.

Finally, since the question of complex lattice codes has been addressed, we discuss the constructions of $\mathbb{Z}[i]^n$–lattices, and give some constructions.

1. The Cyclotomic Construction

Consider the cyclotomic field $\mathbb{Q}(\zeta_p)$ where $p \geq 5$ is a prime and $\zeta = \zeta_p = e^{-2i\pi/p}$ is a primitive pth root of unity. Let $K = \mathbb{Q}(\zeta + \zeta^{-1})$ be the maximal real subfield of $\mathbb{Q}(\zeta)$, whose degree over $\mathbb{Q}$ is $n = (p-1)/2$.

Let $\Lambda = (\mathcal{O}_K, q_\alpha)$ be an ideal lattice. A necessary (but not sufficient) condition for Λ to be isomorphic to $(\sqrt{c}\mathbb{Z})^n$, a scaled version of $\mathbb{Z}^n$, is that $\det(\Lambda) = c^n$, since the Gram matrix of $(\sqrt{c}\mathbb{Z})^n$ is cI_n, c an integer. In order to fulfill this condition (see Prop. 2.2 of Chapter 2), we need to find $\alpha \in K$ such that

$$N(\alpha)d_K = N(\alpha)p^{(p-3)/2} = c^{(p-1)/2}.$$

An element $\alpha \in K$ with norm p is easily found. We have

$$(p)\mathbb{Z}[\zeta] = (1-\zeta)^{p-1}\mathbb{Z}[\zeta]$$

in $\mathbb{Q}(\zeta)$ so that $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$. Using the transitivity of the norm, we get

$$\begin{aligned} N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) &= N_{K/\mathbb{Q}}(N_{\mathbb{Q}(\zeta)/K}(1-\zeta)) \\ &= N_{K/\mathbb{Q}}((1-\zeta)(1-\zeta^{-1})). \end{aligned}$$

Thus $(1-\zeta)(1-\zeta^{-1})$ is an element of $\mathbb{Z}[\zeta+\zeta^{-1}]$ whose norm is p.

As we already mentioned, this is not enough to guarantee the existence of a scaled version of $\mathbb{Z}^n$. To show its existence, we build it explicitly.

Recall that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\zeta+\zeta^{-1}]$. Let $\{e_j = \zeta^j + \zeta^{-j}\}_{j=1}^n$ be its canonical $\mathbb{Z}$-basis. Another basis is given by $\{e'_i\}_{i=1}^n$, where $e'_n = e_n$ and $e'_j = e_j + e'_{j+1}$, $j = 1, \ldots, n-1$.

Proposition 1.1. *Let* $\alpha = (1-\zeta)(1-\zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$. *Then*

$$\frac{1}{p}\ Tr_{K/\mathbb{Q}}(\alpha e'_i e'_j) = \delta_{ij}.$$

PROOF. It is a direct computation. Denote by $\sigma_j(\zeta)$ and $\alpha_j = \sigma_j(\alpha)$, $j = 1, \ldots, n$ the conjugates of ζ and α, respectively. Since

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta^k + \zeta^{-k}) = \sum_{j=1}^{n} \sigma_j(\zeta^k + \zeta^{-k}) = -1, \ \forall\ k = 1, \ldots, n, \tag{28}$$

we have

$$\begin{aligned} \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta^k + \zeta^{-k}) &= -2 - \sum_{j=1}^{n} \sigma_j(\zeta^{k+1} + \zeta^{-k-1} + \zeta^{-k+1} + \zeta^{k-1}) \\ &= \begin{cases} -p & \text{if } k \equiv \pm 1 \pmod p \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{29}$$

We first compute $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i e_j)$ (using (29) and (28)), for all $i, j = 1, \ldots, n$.

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i^2) &= \sum_{j=1}^{n} \alpha_j \sigma_j(\zeta^{2i} + \zeta^{-2i}) + 2\sum_{j=1}^{n} (2 - \sigma_j(\zeta + \zeta^{-1})) \\ &= \begin{cases} p & \text{if } i = n, \text{ i.e., } 2i \equiv -1 \pmod p \\ 2p & \text{otherwise} \end{cases} \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha e_i e_j) &= \sum_{k=1}^{n} \alpha_k \sigma_k(\zeta^{i+j} + \zeta^{-(i+j)}) + \sum_{k=1}^{n} \alpha_k \sigma_k(\zeta^{i-j} + \zeta^{-(i-j)}) \\ &= \begin{cases} -p & \text{if } |i - j| = 1 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

Thus the matrix of $\frac{1}{p}\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x y)$ in the basis $\{e_1, \ldots, e_n\}$ is given by

$$\begin{pmatrix} 2 & -1 & 0 & \cdots & 0 \\ -1 & 2 & & & \\ 0 & & \ddots & -1 & 0 \\ & & -1 & 2 & -1 \\ 0 & \cdots & 0 & -1 & 1 \end{pmatrix}.$$

This matrix is isomorphic to the identity matrix, which can be checked choosing the basis $\{e'_1, \ldots, e'_n\}$. □

In other words, the ideal lattice $\Lambda = (\mathcal{O}_K, \frac{1}{p} b_\alpha)$ with $\alpha = (1-\zeta)(1-\zeta^{-1})$ is isomorphic to $\mathbb{Z}^n$.

n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$	n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$
2	$1/\sqrt{5}$	0.66874	15	$1/31^7$	0.20138
3	$1/7$	0.52275	18	$1/\sqrt{37^{17}}$	0.18174
5	$1/11^2$	0.38321	20	$1/\sqrt{41^{19}}$	0.17136
6	$1/\sqrt{13^5}$	0.34344	21	$1/43^{10}$	0.16678
8	$1/\sqrt{17^7}$	0.28952	23	$1/47^{11}$	0.15859
9	$1/19^4$	0.27018	26	$1/\sqrt{53^{25}}$	0.14825
11	$1/23^5$	0.24045	29	$1/59^{14}$	0.13967
14	$1/\sqrt{29^{13}}$	0.20942	30	$1/\sqrt{61^{29}}$	0.13711

TABLE 1. Minimum product distances for the cyclotomic construction.

COROLLARY 1.1. *The minimum product distance of the ideal lattice* $\Lambda = (\mathcal{O}_K, \frac{1}{p} b_\alpha)$ *of dimension* $(p-1)/2$ *is*

$$d_{p,min}(\Lambda) = p^{-\frac{n-1}{2}}.$$

PROOF. By Corollary 3.1 of Chapter 2, the minimum product distance is given by $d_{p,min} = 1/\sqrt{d_K} = p^{-\frac{n-1}{2}}$, since $d_K = p^{\frac{p-3}{2}} = p^{n-1}$. □

Numerical values of the minimum product distance are given in Table 1. A lattice generator matrix of the $\mathbb{Z}^n$–lattice is easily computed. Since the n embeddings of K are

$$\sigma_k(e_j) = \zeta^{kj} + \zeta^{-kj} = 2\cos\left(\frac{2\pi kj}{p}\right), \quad k = 1, \ldots, n,$$

it is given by

$$\frac{1}{\sqrt{p}}\, TMA$$

where $M = (M_{k,j})_{k,j=1}^n = \left(2\cos\left(\frac{2\pi kj}{p}\right)\right)_{k,j=1}^n$ gives the embeddings of the canonical integral basis of K, $A = \text{diag}\left(\sqrt{\sigma_k(\alpha)}\right)$ and T is an upper triangular matrix with non zero coefficients 1 that gives the basis transformation matrix from $\{e_j\}$ to $\{e'_j\}$.

2. The Cyclic Constructions

Let K be a cyclic extension of $\mathbb{Q}$ of prime degree $n > 2$. Based on [**16**], we consider lattices constructed using the ideal $\mathcal{A}$ of $\mathcal{O}_K$ such that its square is the codifferent, i.e.,

$$\mathcal{A}^2 = \mathcal{D}^{-1}_{K/\mathbb{Q}}. \tag{30}$$

Since a Galois extension of odd degree is totally real, we construct lattices with full diversity $L = n$. The construction in [**16**] shows there exists a trace form over $\mathcal{A}$ which

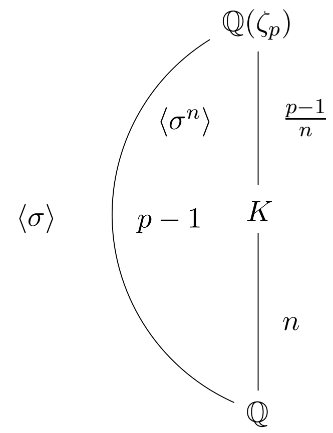

Figure 1. Extension tower for Case I

is isomorphic to the unit form up to a scaling factor. Let p be an odd prime. Depending on the ramification of p in $\mathcal{O}_K$, we derive three different classes of lattices.

(1) Case I: $p > n$ is the only prime which ramifies.
(2) Case II: $p = n$ is the only prime which ramifies.
(3) Case III: there are at least two primes p_1 and p_2 that ramify.

We present these three constructions which result in prime dimensional lattices not available from the cyclotomic constructions.

2.1. Case I: only $p > n$ ramifies. If only the prime $p > n$ ramifies in K (the extension is tamely ramified), we can embed K into the cyclotomic field $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_p$ is a primitive pth root of unity. Denote by G =Gal$(\mathbb{Q}(\zeta)/\mathbb{Q})$ the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Then G is cyclic of order $p-1$. Let σ be a generator of G. Since $[\mathbb{Q}(\zeta) : K] = \frac{p-1}{n}$, the element σ^n is a generator of the cyclic group Gal$(\mathbb{Q}(\zeta)/K)$ (see Fig. 1). Let r be a primitive element (mod p) (i.e., $r^{p-1} \equiv 1 \pmod p$ and $p-1$ is the smallest positive integer having this property), $\alpha = \prod_{i=0}^{m-1}(1-\zeta^{r^i})$, $m = \frac{p-1}{2}$ and let λ be such that $\lambda(r-1) \equiv 1(\text{mod } p)$. Note that $r^m \equiv -1 \pmod p$. According to the definition of r, we take $\sigma : \zeta \mapsto \zeta^r$.

Let us first compute some equalities.

Lemma 2.1. *The following equalities hold:*

(a) $\sigma(\alpha) = -\zeta^{p-1}\alpha$.
(b) $\sigma(\zeta^\lambda\alpha) = -\zeta^\lambda\alpha$.
(c) $(\zeta^\lambda\alpha)^2 = (-1)^m p$.

Proof. **(a).** We have

$$\sigma(\alpha) = (1-\zeta)^{-1}(1-\zeta)\prod_{i=0}^{m-2}(1-\zeta^{r^{i+1}})(1-\zeta^{r^m}) = -\zeta^{p-1}\alpha,$$

where the last equality derives from

$$(1-\zeta)^{-1}(1-\zeta^{-1}) = \frac{1-\zeta^{p-1}}{1-\zeta} = \zeta^{p-2}+\cdots+\zeta+1.$$

(b). Using the previous equality and the definition of λ, we have

$$\sigma(\zeta^\lambda\alpha) = \zeta^{\lambda+1}(-\zeta^{p-1}\alpha) = -\zeta^\lambda\alpha.$$

(c). Evaluating the cyclotomic polynomial of degree $p-1$

$$\Phi(x) = x^{p-1}+x^{p-2}+\cdots+x+1 = \prod_{i=0}^{p-2}(x-\sigma^i(\zeta))$$

in $x=1$, we get

$$\begin{aligned} p &= \prod_{i=0}^{p-2}(1-\zeta^{r^i}) = \prod_{i=0}^{m-1}(1-\zeta^{r^i})\prod_{j=0}^{m-1}(1-\zeta^{-r^j}) \\ &= (-1)^m\alpha^2\prod_{j=0}^{m-1}\zeta^{-r^j} = (-1)^m\alpha^2\zeta^{2\lambda}. \end{aligned}$$

Last equality holds since $\zeta^{-1-r\cdots-r^{m-1}} = \zeta^{\frac{1-r^m}{r-1}}$, and λ is the inverse of $r-1$ (mod p). □

Another technical lemma will be useful.

Lemma 2.2. *Let $\omega_{d,t} = \zeta^{r^{nd}+r^t}$, d,t integers such that $t\in\{0,\ldots,n-1\}$, $d\in\{1,\ldots,(p-1)/n\}$. Then*

$$\omega_{d,t}=1 \Leftrightarrow t=0 \text{ and } d=\frac{p-1}{2n}.$$

Proof. We have

$$\begin{aligned} \omega_{d,t}=1 &\Leftrightarrow r^{nd}\equiv r^{m+t} \pmod p \\ &\Leftrightarrow t = nd-m+k_1(p-1). \end{aligned} \tag{31}$$

Thus t is a multiple of n belonging to $\{0,\ldots,n-1\}$, that is $t=0$. Equation (31) then reduces to

$$r^{nd}\equiv -1 \pmod p \Leftrightarrow d = k_2\left(\frac{p-1}{2n}\right),\ k_2 \text{ odd}$$

so that $k_2=1$ and $d=\frac{p-1}{2n}$, which concludes the proof. □

The lattice construction is given by the following result.

PROPOSITION 2.1. *Define* $z=\zeta^\lambda\alpha(1-\zeta)$ *and*

$$x = Tr_{\mathbb{Q}(\zeta)/K}(z) = \sum_{j=1}^{\frac{p-1}{n}} \sigma^{jn}(z).$$

Then we have $Tr_{K/\mathbb{Q}}(x\sigma^t(x)) = \delta_{0,t}\, p^2$, $t=0,\dots,n-1$.

PROOF. Let us begin with a straightforward computation.

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}}(x\sigma^t(x)) &= \sum_{a=0}^{n-1}\sigma^a\{x\sigma^t(x)\} = \sum_{a=0}^{n-1}\sum_{c,j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z)\\
&= \sum_{a}\sum_{c,j}(-1)^{a+cn}\zeta^\lambda\alpha(1-\zeta^{r^{a+cn}})(-1)^{a+t+jn}\zeta^\lambda\alpha(1-\zeta^{r^{a+t+jn}})\\
&= (-1)^t\sum_{c}(-1)^c\sum_{a,j}(-1)^j(\zeta^\lambda\alpha)^2(1-\zeta^{r^{a+cn}})(1-\zeta^{r^{a+t+jn}})\\
&= (-1)^{t+m}p\sum_{c}(-1)^c\sum_{a,j}(-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}}
\end{aligned}$$

where the second equality (resp. the last) comes from Lemma 2.1-(a)-(b) (resp. 2.1-(c)). One can check that

$$\sum_{c=1}^{\frac{p-1}{n}}(-1)^c\sum_{a,j}(-1)^j\zeta^{r^{a+cn}+r^{a+t+jn}} = \sum_{d}(-1)^d\sum_{a,k}\zeta^{(r^{nd}+r^t)r^{a+kn}}$$

by letting all the indices run through all summation terms and verifying that they cover the same set of exponents of ζ (mod p).
Then note that r^{a+kn}, $a=0,\dots,n-1$, $k=1,\dots,\frac{p-1}{n}$ takes on the values $s=1,\dots,p-1$, so that denoting $\omega_{d,t}=\zeta^{(r^{nd}+r^t)}$, we get

$$\sum_{d}(-1)^d\sum_{a,k}\zeta^{(r^{nd}+r^t)r^{nk+a}} = \sum_{d}(-1)^d\sum_{s=1}^{p-1}\omega_{d,t}^s \tag{32}$$

where by Lemma 2.2

$$\sum_{s=1}^{p-1}\omega_{d,t}^s = \begin{cases} p-1 & \text{if } t=0 \text{ and } d=(p-1)/2\\ -1 & \text{otherwise.}\end{cases}$$

Thus for $t\neq 0$, equation (32) yields

$$(-1)^{t+m}p\sum_{d}(-1)^d\sum_{s=1}^{p-1}\omega_{d,t}^s = (-1)^{t+m}p\sum_{d=1}^{\frac{p-1}{n}}(-1)^d(-1) = 0$$

while for $t = 0$ we have

$$\begin{aligned}(-1)^{t+m} p \sum_d (-1)^d \sum_{s=1}^{p-1} \omega_{d,t}^s &= (-1)^m p \sum_{d=1, d \neq \frac{p-1}{2n}}^{\frac{p-1}{n}} (-1)^d (-1) + (-1)^m p (-1)^{\frac{p-1}{2n}} (p-1) \\ &= p + p(p-1) = p^2.\end{aligned}$$

Last equality holds since $(-1)^{m+\frac{p-1}{2n}} = 1$ and

$$(-1)^m \sum_{d=1, d \neq \frac{p-1}{2n}}^{\frac{p-1}{n}} (-1)^d (-1) = \begin{cases} (-1)^{m+1}(-1) = 1 & \text{if } p \equiv 1 \pmod 4 \ (m \text{ even}) \\ (-1)^{m+1}(1) = 1 & \text{if } p \equiv 3 \pmod 4 \ (m \text{ odd}). \end{cases}$$

This proves that

$$(-1)^{t+m} p \sum_d (-1)^d \sum_{a,k} \zeta^{(r^{nd}+r^t) r^{nk+a}} = \begin{cases} 0 & \text{i.e if } t \neq 0 \\ p^2 & \text{i.e if } t = 0. \end{cases}$$

□

The previous result gives a concrete method to construct x such that

$$\frac{1}{p^2} \mathrm{Tr}_{K/\mathbb{Q}}(x \sigma^t(x)) = \delta_{0,t}, \ t = 0, \ldots, n-1.$$

The corresponding lattice generator matrix can be constructed as follows. Choose a prime dimension $n > 2$ and a prime p such that $p \equiv 1 \pmod n$. Then compute (in the basis $\{1, \zeta, \ldots, \zeta^{p-2}\}$ of the cyclotomic field)

(1) a primitive element (mod p) r and an element λ such that $\lambda(r-1) \equiv 1 ($mod $p)$.
(2) the elements $\alpha = \prod_{i=0}^{m-1}(1 - \zeta^{r^i})$ and $z\zeta^\lambda \alpha(1-\zeta)$, with $m = (p-1)/2$.
(3) the element x and its conjugates, using $\sigma^n : \zeta \mapsto \zeta^{r^n}$.

The lattice generator matrix contains as first column $\sigma^i(x)$, $i = 0, \ldots, n-1$ and as other columns a cyclic shift of the first column (it is thus a circulant matrix). Finally, we normalize the matrix to get its determinant equal to 1.

Examples of parameters are given in Table 2. The lattices in dimensions marked with an $*$ coincide with the ones built in Section 1 from $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Note that the value of p is not unique and that any choice of p satisfying $p \equiv 1$ (mod n) will give a well defined cyclic field K. More precisely:

n	p	r	λ
3*	7	3	4
3	13	2	1
5*	11	2	1
5	31	3	16
7	29	2	1
11*	23	5	6
11	67	2	1
13	53	2	1
17	103	5	26
19	191	19	138
23*	47	5	12
29*	59	2	1

TABLE 2. Examples of parameters for Case I. The $*$ means that $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

LEMMA 2.3. *Let n be an odd prime. If p is an odd prime satisfying $p \equiv 1 \pmod{n}$, then there exists a cyclic field K of degree n such that p is the only prime which ramifies in K.*

PROOF. Let G be the cyclic subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ generated by σ^n of order $(p-1)/n$, which is an integer since $p \equiv 1 \pmod{n}$. Let $K = K^G$ be the subfield fixed by G. The extension $K/\mathbb{Q}$ is a Galois extension because $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is cyclic. Furthermore, K inherits the property that p is exactly the only prime which ramifies from $\mathbb{Q}(\zeta_p)$. □

EXAMPLE 2.1. We build a lattice generator matrix in dimension $n = 3$. We compute a prime p such that $p \equiv 1 \pmod 3$ and choose $p = 13$. These two parameters determine the field K in which we will work. Note that we do not need to know it explicitly, but in this case $K = \mathbb{Q}(\theta)$ where $\theta^3 - \theta^2 - 4\theta - 1 = 0$. It has discriminant 13^2 which shows that only $p = 13$ ramifies in K.

(1) We compute $r = 2$ and $\lambda = 1$.
(2) We get $z = (3,1,4,0,2,4,2,2,2,0,2,4)$ in the basis $\{1, \zeta, \ldots, \zeta^{11}\}$ of $\mathbb{Q}(\zeta)$,where $\zeta = \zeta_{13}$.
(3) We compute $x = \sigma^0(z) + \sigma^n(z) + \sigma^{2n}(z) + \sigma^{3n}(z)$, where $\sigma^n : \zeta \mapsto \zeta^{r^n} = \zeta^8$. Then $x = (5,0,3,3,-1,0,-1,-1,0,-1,3,3)$. Using that $\sigma : \zeta \mapsto \zeta^2$, we get

$$\begin{aligned}\sigma(x) &= (6,0,1,1,4,0,4,4,0,4,1,1), \text{ and}\\ \sigma^2(x) &= (2,0,-4,-4,-3,0,-3,-3,0,-3,-4,-4).\end{aligned}$$

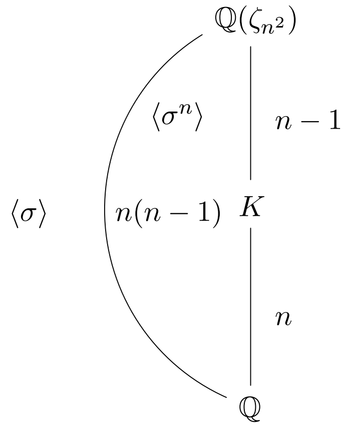

FIGURE 2. Extension tower for Case II

Replacing $\zeta = e^{2i\pi/13}$, we compute the lattice generator matrix

$$M = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) \\ \sigma(x) & \sigma^2(x) & x \\ \sigma^2(x) & x & \sigma(x) \end{pmatrix}.$$

Normalizing by $1/p$, we get

$$\frac{1}{13}M = \begin{pmatrix} 0.90636 & -0.24824 & 0.34188 \\ -0.24824 & 0.34188 & 0.90636 \\ 0.34188 & 0.90636 & -0.24824 \end{pmatrix}.$$

2.2. Case II: only $p = n$ ramifies. If only the odd prime $p = n$ ramifies in K (the extension is widely ramified), we can embed K in $\mathbb{Q}(\zeta_{n^2})$,where $\mu = \zeta_{n^2}$ is a primitive n^2th root of unity. Denote by σ the generator of $\mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$. If r is an element such that $r^{n(n-1)} \equiv 1 \pmod{n^2}$, where $n(n-1)$ is the smallest integer having that property, then σ may be defined as $\sigma : \mu \mapsto \mu^r$.

We have a result similar to the tamely ramified case.

PROPOSITION 2.2. *Let $T = Tr_{\mathbb{Q}(\mu)/K}(\mu) = \sum_{j=1}^{n-1} \sigma^{nj}(\mu)$. Then*

$$Tr_{K/\mathbb{Q}}((1+T)\sigma^t(1+T)) = \delta_{0,t}n^2,\ t = 0, \ldots, n-1.$$

PROOF. Straightforward computations yield

$$
\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}}((1+T)\sigma^t(1+T)) &= \sum_{a=0}^{n-1}\sigma^a((1+T)\sigma^t(1+T)) \\
&= n+\sum_a\sum_{j=1}^{n-1}\sigma^{a+t+nj}(\mu)+\sum_a\sum_{j=1}^{n-1}\sigma^{a+nj}(\mu)+\sum_a\sum_{j,k=1}^{n-1}\sigma^{a+nj}(\mu)\sigma^{a+t+kn}(\mu) \\
&= n+\sum_{s=0}^{n(n-1)-1}\mu^{r^{s+t}}+\sum_{s=0}^{n(n-1)-1}\mu^{r^s}+\sum_a\sum_{d,c=1}^{n-1}\mu^{r^{a+nd+nc}+r^{a+t+cn}}
\end{aligned}
$$

since the set of values $a+nj$, $a=0,\dots,n-1$, $j=1,\dots,n-1$ is the same as $s=0,\dots,n(n-1)-1$. The change of variables in the triple sum can be verified by enumerating the values taken on by the different powers as in the proof of Prop. 2.1. Since

$$
\mathrm{Tr}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\mu)=\sum_{s=0}^{n(n-1)-1}\mu^{r^s}=\sum_{s=0}^{n(n-1)-1}\mu^{r^{s+t}}=0,\ t=0,\dots,n-1,
$$

we get

$$
\mathrm{Tr}_{K/\mathbb{Q}}((1+T)\sigma^t(1+T))=n+\sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1}\mu^{(r^{nd}+r^t)r^s}=n+\sum_{d=1}^{n-1}\mathrm{Tr}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\omega_{d,t}) \tag{33}
$$

where $\omega_{d,t}=\mu^{r^{nd}+r^t}$. The expression $\mathrm{Tr}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\omega_{d,t})$ in (33) can take on three different values depending on $\omega_{d,t}$:

(1) $\omega_{d,t}=1 \Rightarrow \mathrm{Tr}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\omega_{d,t})=n(n-1)$.

(2) $\omega_{d,t}$ is a n^2th primitive root of unity $\Rightarrow \mathrm{Tr}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\omega_{d,t})=0$.

(3) $\omega_{d,t}$ is a root of unity which is not primitive: $\omega_{d,t}$ is of the form $\mu^{k_1 n}$, $k_1=1,\dots,n-1$, which is a nth root of unity $\Rightarrow \mathrm{Tr}_{\mathbb{Q}(\mu)/\mathbb{Q}}(\omega_{d,t})=-n$.

To prove the proposition, we distinguish the two cases $t=0$ and $t\neq 0$. In each case we determine whether $\omega_{d,t}$ is primitive or not.

- *First case:* $t=0$.

  We have $\omega_{d,t}=1$ only in this case. In fact

$$
r^{nd}+r^t\equiv 0 \pmod{n^2} \iff t=nd-\frac{n(n-1)}{2}+k_2n(n-1) \iff t=0
$$

  and it occurs for $d=(n-1)/2$:

$$
r^{nd}\equiv -1 \pmod{n^2} \Rightarrow d=\frac{n-1}{2}.
$$

We now verify that when $d \neq \frac{n-1}{2}$, $\omega_{d,t}$ is a primitive root of unity. Suppose it is not primitive, then

$$r^{nd}+1 \equiv 0 \pmod{n^2} \;\Rightarrow\; r^{nd}+1 \equiv 0 \pmod{n} \;\Rightarrow\; d=\frac{n-1}{2}+k_3\frac{n-1}{n}.$$

Since $d \geq n-1$ we must have $k_3=0$, which gives the case $\omega_{d,t}=1$. Putting all together, we obtain

$$n+\sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1}\mu^{(r^{nd}+r^t)r^s}=n+n(n-1)=n^2 \text{ for } t=0.$$

- *Second case:* $t \neq 0$.

  We determine the primitive roots of unity:

  $$r^{nd}+r^t \equiv 0 \pmod{n} \;\Rightarrow\; d=\frac{t-k_4}{n}+\frac{n-1}{2}+k_4.$$

  We need to take $k_4=t$ (since $d \geq n-1$, we cannot take $k_4=t+k_5n$). Thus there is only one d such that $\omega_{d,t}$ is not primitive. Putting all together, we obtain

  $$n+\sum_{d=1}^{n-1}\sum_{s=0}^{n(n-1)-1}\mu^{(r^{nd}+r^t)r^s}=n-n=0.$$

□

Let us now compute the corresponding lattice generator matrix. Choose a prime dimension $n>2$ and an element r such that $r^{n(n-1)} \equiv 1 \pmod{n^2}$, with $n(n-1)$ the smallest integer k such that $r^k \equiv 1 \pmod{n^2}$. Compute the element $1+T$ and its conjugates in the basis of the cyclotomic field using $\sigma^n : \mu \mapsto \mu^{r^n}$. The lattice generator matrix can be computed and normalized similarly to the tamely ramified case.

Example 2.2. We compute a lattice generator matrix in dimension $n=3$. This corresponds to the field $K=\mathbb{Q}(\theta)$ where $\theta^3-3\theta-1=0$, whose discriminant is 3^4. We compute $r=2$, and in the basis of $\mathbb{Q}(\zeta_9)$, $1+T$ and its conjugates:

$$\begin{aligned}1+T &= (1,1,-1,0,0,-1)\\ \sigma(1+T) &= (1,-1,1,0,-1,0)\\ \sigma^2(1+T) &= (1,0,0,0,1,1)\end{aligned}$$

$$\begin{tikzcd}
 & & \mathbb{Q}(\zeta_{p_1p_2}) \arrow[dll, dash] \arrow[dd, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\zeta_{p_1}) \arrow[dd, dash] & & & & \mathbb{Q}(\zeta_{p_2}) \arrow[dd, dash] \\
 & & K_1K_2 \arrow[dll, dash, "n"'] \arrow[dd, dash, "n^2"] \arrow[drr, dash, "n"] & & \\
K_1 \arrow[drr, dash, "n"'] & & & & K_2 \arrow[dll, dash, "n"] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

FIGURE 3. Extension tower for Case III.

Finally

$$\frac{1}{3}M = \begin{pmatrix} 0.84402 & -0.29312 & 0.44909 \\ 0.44909 & 0.84402 & -0.29312 \\ -0.29312 & 0.44909 & 0.84402 \end{pmatrix}.$$

2.3. Case III: at least two primes ramify. Suppose now that K contains at least two primes that ramify. We will use two fields where only one prime ramifies as building blocks to construct K.

LEMMA 2.4. *Let n be an odd prime. Take two distinct odd primes p_1, p_2 such that $p_i \equiv 1$ (mod n), but $p_i \not\equiv 1$ (mod n^2), $i = 1, 2$. Let K be a cyclic field of degree n such that p_1 and p_2 ramify. Then K is contained in the compositum K_1K_2 of two fields such that K_i is the cyclic field of degree n where only p_i ramifies, $i = 1, 2$.*

PROOF. Since $p_i \equiv 1 \pmod{n}$, $i = 1, 2$, we have the extension tower of Fig. 3. It is clear that K is a subextension of $\mathbb{Q}(\zeta_{p_1p_2})$. What is left to prove is that $K \subseteq K_1K_2$. Let G=Gal$(\mathbb{Q}(\zeta_{p_1p_2})/\mathbb{Q})$.

$$\begin{aligned} G &\cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \mathbb{Z}/(p_2-1)\mathbb{Z} \\ &\cong C_n \times C_n \times \mathbb{Z}/\left(\frac{p_1-1}{n}\right)\mathbb{Z} \times \mathbb{Z}/\left(\frac{p_2-1}{n}\right)\mathbb{Z}. \end{aligned}$$

Recall that an abelian group has a unique decomposition into its Sylow subgroups. G is thus the direct product of a n-Sylow subgroup and of Sylow p_i-subgroups where $(p_i, n) = 1$.

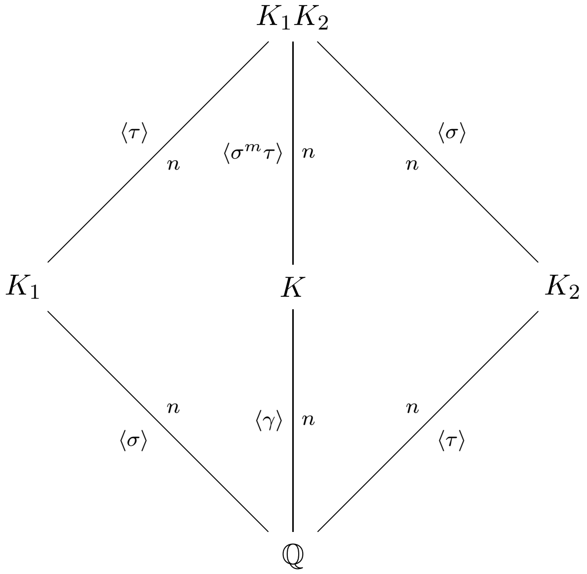

Figure 4. Detail of the extension tower for Case III

Let H=Gal$(\mathbb{Q}(\zeta_{p_1p_2})/K_1K_2)$. H is a subgroup of G of order $\frac{p_1-1}{n}\frac{p_2-1}{n}$. Because $(|H|,n)=1$, we deduce that H corresponds to the direct product of the Sylow p_i-subgroups of G where $(p_i,n)=1$. Let I=Gal$(\mathbb{Q}(\zeta_{p_1p_2})/K)$ a subgroup of G. Since I is of order $\frac{(p_1-1)(p_2-1)}{n}=n\frac{p_1-1}{n}\frac{p_2-1}{n}$, this implies that I contains a subgroup J of order $\frac{p_1-1}{n}\frac{p_2-1}{n}$. We use the same technique as before to obtain that J is also the direct product of the p_i-Sylow of G where $(p_i,n)=1$, so that $H\subseteq I$, implying that $K\subseteq K_1K_2$. □

Remark 2.1. We do not prove the case when p_1 or p_2 is equal to n, which can be handled in a similar way by replacing $\mathbb{Q}(\zeta_{p_1p_2})$ with $\mathbb{Q}(\zeta_{p_1n^2})$.

Proposition 2.3. *Let K_1,K_2 be two disjoint Galois extensions of $\mathbb{Q}$, whose discriminants are relatively prime. Let G_i =Gal$(K_i/\mathbb{Q})$ for $i=1,2$ and $G_1=\langle\sigma\rangle$, $G_2=\langle\tau\rangle$ be cyclic of order n. Let $K\subseteq K_1K_2$ be another cyclic extension of order n. If there exist $x_i\in K_i$, $i=1,2$ which satisfy*

(1) $Tr_{K_1/\mathbb{Q}}(x_1\sigma^t(x_1))=\delta_{0,t}p_1^2,\ t=0,\dots,n-1$

(2) $Tr_{K_2/\mathbb{Q}}((x_2\tau^t(x_2))=\delta_{0,t}p_2^2,\ t=0,\dots,n-1$

then there exists $x\in K$, given by $x=Tr_{K_1K_2/K}(x_1x_2)$, such that

$$Tr_{K/\mathbb{Q}}(x\gamma^t(x))=\delta_{0,t}p_1^2p_2^2,\ t=0,\dots,n-1$$

where $\langle\gamma\rangle=Gal(K/\mathbb{Q})$.

PROOF. We will use the fact that

$$\begin{aligned}\mathrm{Tr}_{K_1K_2/\mathbb{Q}}(x_1x_2) &= \sum_{i=1}^{n}\sum_{j=1}^{n}\sigma^i\tau^j(x_1x_2)\\ &= \sum_{i=1}^{n}\sigma^i(x_1)\sum_{j=1}^{n}\tau^j(x_2)\\ &= \mathrm{Tr}_{K_1/\mathbb{Q}}(x_1)\mathrm{Tr}_{K_2/\mathbb{Q}}(x_2).\end{aligned}$$

Let $1 \leq m \leq n-1$ be such that $\langle\sigma^m\tau\rangle$=Gal$(K_1K_2/K)$. Choose $\gamma = \sigma^{-m}\tau$ as generator of Gal$(K/\mathbb{Q})$, so that

$$\begin{aligned}x &= \sum_{b=0}^{n-1}(\sigma^m\tau)^b(x_1x_2)\\ x\gamma^t(x) &= \sum_{b,c=0}^{n-1}\sigma^{mb}(x_1)\tau^b(x_2)\sigma^{-mt}\tau^t\sigma^{mc}(x_1)\sigma^{-mt}\tau^t\tau^c(x_2)\\ &= \sum_{b,c=0}^{n-1}\sigma^{mb}(x_1\sigma^{m(c-t-b)}(x_1))\tau^b(x_2\tau^{t+c-b}(x_2))\end{aligned}$$

and

$$\begin{aligned}n\mathrm{Tr}_{K/\mathbb{Q}}(x\gamma^t(x)) &= \mathrm{Tr}_{K_1K_2/\mathbb{Q}}(x\gamma^t(x))\\ &= \sum_{b,c=0}^{n-1}\mathrm{Tr}_{K_1K_2/\mathbb{Q}}(\sigma^{mb}\tau^b[(x_1\sigma^{m(c-t-b)}(x_1))(x_2\tau^{c+t-b}(x_2))])\\ &= \sum_{b,c}\mathrm{Tr}_{K_1/\mathbb{Q}}(x_1\sigma^{m(c-t-b)}(x_1))\mathrm{Tr}_{K_2/\mathbb{Q}}(x_2\tau^{c+t-b}(x_2)). \qquad (34)\end{aligned}$$

Finally, the terms in the sum of (34) are different from zero only when $m(c-b-t)=0$ and $c+t-b=0$, which is equivalent to ask that $t=0$ and $c=b$. This means that (34) is non-zero if and only if $t=0$, and it is equal to $np_1^2p_2^2$. □

If we know that two primes p_1 and p_2 ramify in a cyclic field K of prime degree n, we know how to find an element $x \in K$ which gives the unit form. Note that no explicit knowledge of K is required to construct the lattice.

Choose a prime dimension n and two primes p_1 and p_2 that satisfy the hypotheses of Prop. 2.3. Then compute

(1) the elements x_1, x_2 and their conjugates using the techniques of Cases I and II, and embed them into either $\mathbb{Q}(\zeta_{p_1p_2})$ if $p_2 > n$ or into $\mathbb{Q}(\zeta_{p_1n^2})$ if $p_2 = n$.

(2) the element x using the knowledge of $\sigma^t(x_1)$ and $\tau^t(x_2)$, $t = 0, \ldots, n-1$.

(3) the conjugates in K of x using $\mathrm{Gal}(K/\mathbb{Q})$. The cyclic group $\mathrm{Gal}(K/\mathbb{Q})$ of order n must be carefully selected among the subgroups of order n of $\mathrm{Gal}(K_1K_2/\mathbb{Q})$.

Example 2.3. As an example, we use the two cases computed previously in dimension $n = 3$. Choose $p_1 = 13$ and $p_2 = 3$.

(1) Let $\zeta = \zeta_{117}$. In the basis of $\mathbb{Q}(\zeta)$ of degree 72, we have for example that

$$\begin{aligned} x_1 \ = (\ & 5,0,0,1,0,0,0,0,0,0,0,0,-3,0,0,0,0,0,3,0,0,-3,0,0,\\ & 0,0,0,3,0,0,0,0,0,0,0,0,-1,0,0,0,0,0,1,0,0,0,0,0,0,\\ & 0,0,0,-3,0,0,-1,0,0,0,0,0,-3,0,0,-1,0,0,0,0,0,0,0,0). \end{aligned}$$

Similarly we embed x_2 in $\mathbb{Q}(\zeta)$.

(2) We compute $x = x_1x_2 + \sigma(x_1)\tau(x_2) + \sigma^2(x_1)\tau^2(x_2)$, which gives

$$\begin{aligned} x \ = (\ & 13,5,-9,0,-2,7,0,2,0,0,7,-9,0,-3,7,0,0,2,0,0,-2,0,-2,\\ & 2,0,-5,3,0,7,-9,0,0,0,0,-5,2,0,7,-7,0,5,-7,0,0,7,0,2,\\ & -7,0,0,-7,0,-4,7,0,7,0,0,-2,-2,0,0,9,0,0,-3,0,0,-7,0,-5,2). \end{aligned}$$

(3) Using the generator $\gamma : \zeta \mapsto \zeta^{40}$ of $\mathrm{Gal}(K/\mathbb{Q})$, we compute the conjugates of x.

Finally the lattice generator matrix is given by

$$\begin{pmatrix} 0.55329 & 0.76837 & -0.32166 \\ -0.32166 & 0.55329 & 0.76837 \\ 0.76837 & -0.32166 & 0.55329 \end{pmatrix}$$

2.4. The minimum product distance. Since the ideal $\mathcal{A}$ given in (30) is principal for all the dimensions considered, we know, using Corollary 3.1 of Chapter 2, that the minimum product distance is given by

$$d_{p,min} = \frac{1}{\sqrt{d_K}}.$$

Some numerical values of $d_{p,min}$ for the Cases I and II are reported in Table 3. We have seen that for each prime dimension n, several constructions of lattices are available, all yielding maximum diversity. The minimum product distance gives us a way to rank them. For example, for $n = 5$, we can build the following lattices depending on the choice of the primes p.

(1) only 11 ramifies, with $d_{p,min} = 1/121$ (Case I)

n	N	d_K	d_p	$\sqrt[n]{d_{p,min}}$
3	7	7^2	$1/7$	0.52275
3	13	13^2	$1/13$	0.42529
5	11	11^4	$1/11^2$	0.38321
5	31	31^4	$1/31^2$	0.25319
7	29	29^6	$1/29^3$	0.23618
11	23	23^{10}	$1/23^5$	0.24045
11	67	67^{10}	$1/67^5$	0.14789
13	53	53^{12}	$1/53^6$	0.16002
17	103	103^{16}	$1/103^8$	0.11292
19	191	191^{18}	$1/191^9$	0.08308
23	47	47^{22}	$1/47^{11}$	0.15859
29	59	59^{28}	$1/59^{14}$	0.13967
3	9	9^2	$1/9$	0.48074
5	25	5^8	$1/5^4$	0.275945932
7	49	7^{12}	$1/7^6$	0.188638463

Table 3. Some minimum product distances for Cases I and II, N is such that $K \subseteq \mathbb{Q}(\zeta_N)$.

(2) only 31 ramifies, with $d_{p,min} = 1/961$ (Case I)

(3) only 5 ramifies, with $d_{p,min} = 1/625$ (Case II)

(4) 11 and 31 ramify, with $d_{p,min} = 1/(121 \cdot 961)$ (Case III)

(5) 11 and 5 ramify, with $d_{p,min} = 1/(121 \cdot 625)$ (Case III).

Since our aim is to maximize the $d_{p,min}$, the best choice in this example is to take the first construction in the above list, i.e., when only one prime ramifies, this prime being the smallest possible. This appears to be true in general.

Proposition 2.4. *For a given prime dimension $n > 2$, the construction of Case I, with the smallest possible p, maximizes the minimum product distance.*

Proof. (1) We first show that the discriminant of K in Case I is $d_K = p^{n-1}$. Since p is totally ramified in K, $pO_k = \mathfrak{p}^n$. This implies, since $p \nmid n$, that $\mathfrak{p}^{n-1} | \mathcal{D}_{K/\mathbb{Q}}$ but $\mathfrak{p}^n \nmid \mathcal{D}_{K/\mathbb{Q}}$ [**48**]. Thus we have $N(\mathcal{D}_{K/\mathbb{Q}}) = d_K = p^{n-1}$, since $\mathcal{D}_{K/\mathbb{Q}} = \mathfrak{p}^{n-1}$. In order to maximize $d_{p,min}$, one has to take the smallest $p > n$ that ramifies. This also shows that Case III is always worse than Case I as $d_K = (p_1p_2)^{n-1}$.

(2) Using the same technique as in the previous case, we find $\mathfrak{p}^n|\mathcal{D}_{K/\mathbb{Q}}$, but now we can have $\mathfrak{p}^k|\mathcal{D}_{K/\mathbb{Q}}$, for $k > n$. Consider the transitivity formula for the different:

$$\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathcal{D}_{\mathbb{Q}(\zeta)/K}\mathcal{D}_{K/\mathbb{Q}}. \tag{35}$$

Denote $\mathfrak{p} = (1-\zeta)\mathbb{Z}[\zeta]$, $\mathfrak{p}_K = \mathfrak{p} \cap \mathcal{O}_K$ and note that $\mathfrak{p}_K\mathbb{Z}[\zeta] = \mathfrak{p}^{n-1}$ as p is totally ramified. It is known that $\mathcal{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathfrak{p}^{n(2n-3)}$ and that $\mathcal{D}_{\mathbb{Q}(\zeta)/K} = \mathfrak{p}^{n-2}$. From (35) we then obtain that $\mathcal{D}_{K/\mathbb{Q}} = \mathfrak{p}^{2(n-1)^2} = (\mathfrak{p}^{n-1})^{2(n-1)} = \mathfrak{p}_K^{2(n-1)}$. We have $d_K = N_{K/\mathbb{Q}}(\mathfrak{p}_K^{2(n-1)}) = p^{2(n-1)}$. It follows that as long as $n^2 > p$ (true for $n > 2$), the minimum distance is smaller than in the case where $p > n$.

□

3. Mixed Constructions

We now present a technique to combine the previous constructions to build $\mathbb{Z}^n$–lattices in other dimensions.

PROPOSITION 3.1. *Let K be the compositum of N Galois extensions K_j of degree n_j with coprime discriminant i.e., $(d_{K_i}, d_{K_j}) = 1, \forall i \neq j$. Assume there exists an α_j such that the trace form over K_j, $Tr(\alpha_j xy)$, is isomorphic to the unit form $\langle 1, \ldots, 1\rangle$ of degree n_j for $j = 1, \ldots, N$. Then the form over K*

$$Tr(\alpha_1 xy) \otimes \cdots \otimes Tr(\alpha_N xy)$$

is isomorphic to the unit form $\langle 1, \ldots, 1\rangle$ of degree $n = \prod_{j=1}^{N} n_j$.

PROOF. Let us consider the case $K = K_1K_2$. Denote by $\{\omega_1, \ldots, \omega_{n_1}\}$ and $\{\omega'_1, \ldots, \omega'_{n_2}\}$ the integral bases of K_1 and K_2, respectively. As K_1 and K_2 are Galois extension over $\mathbb{Q}$ with coprime discriminants, we have that $\{\omega_j\omega'_k \mid j = 1, \ldots, n_1,\ k = 1, \ldots, n_2\}$ defines a basis for $\mathcal{O}_K$ [**48**] . We conclude using the fact that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\omega_i\omega_j\alpha_2\omega'_k\omega'_l) = \mathrm{Tr}_{K_1/\mathbb{Q}}(\alpha_1\omega_i\omega_j)\mathrm{Tr}_{K_2/\mathbb{Q}}(\alpha_2\omega'_k\omega'_l).$$

□

The lattice generator matrix can be immediatly obtained as the tensor product of the generator matrices $R^{(j)}$ corresponding to the forms $\mathrm{Tr}(\alpha_j xy)$, for $j = 1, \ldots, N$

$$R = R^{(1)} \otimes \cdots \otimes R^{(N)}.$$

In the case of the cyclotomic construction, Prop. 3.1 yields

Corollary 3.1. *Let $m = p_1 \cdots p_N$ be the product of N distinct primes, $\zeta_j = e^{-i2\pi/p_j}$ for $j = 1, \ldots, N$ and K be the compositum of $K_j = \mathbb{Q}(\zeta_j + \zeta_j^{-1})$, $j = 1, \ldots, N$, (i.e., the smallest field containing all K_j). Let $\alpha_j = (1 - \zeta_j)(1 - \zeta_j^{-1})$ then*

$$\frac{1}{p_1}\ Tr(\alpha_1 xy) \otimes \cdots \otimes \frac{1}{p_N}\ Tr(\alpha_N xy)$$

is isomorphic to the unit form $\langle 1, \ldots, 1\rangle$ of degree $n = \prod_{j=1}^{N}(p_j - 1)/2$.

The above generalizes the cyclotomic construction to $\mathbb{Q}(\zeta_m)$, where m is a square-free product of primes. The cyclotomic and cyclic constructions together allow to get lattice constructions in almost all dimensions. The missing ones are obtained by using Prop. 3.1.

Example 3.1. The only missing dimensions below 30 are 4 and 25.

(1) The case $n = 4$ can be obtained combining two rotated square lattices.

(2) The case $n = 25$ can be obtained combining the two rotated cubic lattices of dimension 5 constructed using Cases I and II of cyclic constructions.

3.1. The minimum product distance. For the mixed construction, we have the following:

Proposition 3.2. *Let $K = K_1K_2$ be the compositum of two Galois extensions of degree n_1 and n_2, with coprime discriminant. The discriminant of K is $d_K = d_{K_1}^{m_1} d_{K_2}^{m_2}$, where $m_j = [K : K_j] = n/n_j$, $j = 1, 2$.*

Proof. Since $\mathcal{D}_{K/\mathbb{Q}} = \mathcal{D}_{K_1/\mathbb{Q}}\mathcal{D}_{K_2/\mathbb{Q}}$ (see [**48**]), we directly deduce that

$$N_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}}) = N_{K/\mathbb{Q}}(\mathcal{D}_{K_1/\mathbb{Q}})N_{K/\mathbb{Q}}(\mathcal{D}_{K_2/\mathbb{Q}}) = N_{K_1/\mathbb{Q}}(\mathcal{D}_{K_1/\mathbb{Q}})^{m_1} N_{K_2/\mathbb{Q}}(\mathcal{D}_{K_2/\mathbb{Q}})^{m_2},$$

which proves the result, recalling that $N_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}}) = d_K$. □

A direct consequence is that we have for the mixed construction

$$d_{p,min} = \frac{1}{\sqrt{d_{K_1}^{m_1} d_{K_2}^{m_2}}}.$$

Numerical values of $d_{p,min}$ are given in Table 4. We note that the lattices in dimensions $n = 4$ and 25 have minimum product distance 1/40 and $1/(5^{20}11^{10})$ given by Proposition 3.2.

n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$	n	$d_{p,min}$	$\sqrt[n]{d_{p,min}}$
4	$1/(5\cdot 8)$	0.39763	22	$1/\sqrt{5^{11}23^{20}}$	0.16080
6	$1/\sqrt{5^3 7^4}$	0.34958	24	$1/\sqrt{7^{16}17^{21}}$	0.15134
10	$1/\sqrt{5^5 11^8}$	0.25627	25	$1/(5^{20}11^{10})$	0.10574
12	$1/\sqrt{5^6 13^{10}}$	0.22967	27	$1/\sqrt{7^{18}19^{24}}$	0.14124
15	$1/\sqrt{7^{10}11^{12}}$	0.20032	28	$1/\sqrt{5^{14}29^{26}}$	0.14005
16	$1/\sqrt{5^8 17^{14}}$	0.19361	30	$1/\sqrt{11^{24}13^{25}}$	0.13161
18	$1/\sqrt{5^9 19^{16}}$	0.18068			

TABLE 4. Minimum product distances for the mixed constructions.

4. Krüskemper's Method

This section is dedicated to 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. We will see there is a degree of freedom in choosing the number field we are working on, so that it allows to "optimize" the lattice we are looking for.

4.1. Taussky's and Krüskemper's theorems.

We present two theorems which prove that any integer 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 $b : M \times M \to \mathbb{Z}$ a symmetric bilinear form. Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and θ be a root of f. Then $\mathbb{Z}[X]/(f(X)) = \mathbb{Z}[\theta]$ with basis $\{1, \theta, \dots, \theta^{n-1}\}$. If $\mathcal{I}$ is an ideal of $\mathbb{Z}[\theta]$, we set $\mathcal{I}^{\#} = \{c \in \mathbb{Q}(\theta) \mid \mathrm{Tr}(c\mathcal{I}) \subseteq \mathbb{Z}\}$.

THEOREM 4.1. *(Taussky)*[**37**, p. 142] *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 χ_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 χ_A. It is an algebraic integer since χ_A is monic with coefficients in $\mathbb{Z}$.

By Theorem 1 of [**51**], there exists an eigenvector $\mathbf{v}_\theta = (v_1, \dots, v_n)^T$ of A associated to θ, 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 Theorem 1 of [**52**], there exists an eigenvector $\mathbf{v}'_\theta = (v'_1, \dots, v'_n)^T$ of

A^T associated to θ, with $v'_i \in \mathbb{Q}(\theta)$ and such that

$$\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(v_i v'_j) = \delta_{ij}, \ \forall i, j. \tag{36}$$

It follows from $A^T = B^{-1}AB$ that $A^T B^{-1}\mathbf{v}_\theta = B^{-1}A\mathbf{v}_\theta = \theta B^{-1}\mathbf{v}_\theta$, so that $\mathbf{v}'_\theta$ and $B^{-1}\mathbf{v}_\theta$ are both eigenvectors of A^T associated to θ. Since $\chi_{A^T} = \chi_A$ 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 $\mathbf{v}'_\theta = \alpha B^{-1}\mathbf{v}_\theta$, i.e. $B\mathbf{v}'_\theta = \alpha \mathbf{v}_\theta$. Denote $B = (b_{ij})_{i,j}$. We have

$$\sum_{j=1}^{n} b_{ij} v'_j = \alpha v_i, \ \forall i \ \Rightarrow \sum_{j=1}^{n} b_{ij} v'_j v_k = \alpha v_i v_k, \ \forall i, k, \tag{37}$$

so that

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

Using (36), we get $b_{ik} = \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha v_i v_k)$ and we conclude that B is the matrix of an ideal lattice $\mathcal{I} = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$. □

We show now that a matrix A such as described in the hypothesis of Theorem 4.1 always exists.

THEOREM 4.2. *(Krüskemper)* [**31**] *Let (M, b) be an integral lattice. Then there exists an algebraic integer θ, an ideal $\mathcal{I}$ of $\mathbb{Z}[\theta]$ and $\alpha \in (\mathcal{I}^2)^\# \subseteq \mathbb{Q}(\theta)$ such that b is isomorphic to*

$$\begin{array}{ccc} \mathcal{I} \times \mathcal{I} & \rightarrow & \mathbb{Z} \\ (x, y) & \mapsto & Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha xy). \end{array}$$

Furthermore, θ can be assumed to be totally real.

PROOF. By Theorem 4.1, it is enough to show that there always exists a matrix $A \in \mathcal{M}_n(\mathbb{Z})$ whose characteristic polynomial χ_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 [**31**] that the characteristic polynomial χ_{BN} of BN is irreducible. By Hilbert's irreducibility theorem, there exists $x_{ij} = x_{ji} \in \mathbb{Q}$ such that $\chi_{B(x_{ij})}$ is irreducible and totally real. Let $A = B(x_{ij})$. It satisfies $B^{-1}AB = A^T$. □

4.2. The lattice construction algorithm. Based on the proof of Theorem 4.1, we give 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 $\{v_1, \ldots, v_n\}$ and an element α such that $\mathcal{I} = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ and the ideal lattice $(\mathcal{I}, b_\alpha)$

$$\begin{array}{rcl} b_\alpha : \mathcal{I} \times \mathcal{I} & \rightarrow & \mathbb{Z} \\ (x, y) & \mapsto & \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha x y) \end{array}$$

has Gram matrix B.

Let B be a lattice Gram matrix.

Step 1: Computation of the matrix A

A matrix $A \in \mathcal{M}_n(\mathbb{Z})$ satisfying $AB = BA^T$ 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 χ_A.

Step 2: Computation of a $\mathbb{Z}$-basis of $\mathcal{I}$

Recall from the proof of Theorem 4.1 that there exists an eigenvector $\mathbf{v}_\theta$ of A associated to θ, a root of χ_A, such that $\mathcal{I} = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$.
In [**51**], it is shown that

$$v_j := (-1)^{i+j} \Delta_{ij}(A - \theta I_n) \tag{38}$$

where Δ_{ij} is the jth minor of a given fixed row, say the ith row, of $A - \theta I_n$.
Let us verify that this vector is indeed an eigenvector of A.

Proposition 4.1. *The vector $\mathbf{v}_\theta$ is an eigenvector of A associated to θ .*

Proof. We prove that $A\mathbf{v}_\theta = \theta\mathbf{v}_\theta$.
Denote by $(A)_i$ the ith row of A, and $A = (a_{ij})_{i,j=1}^n$. Without loss of generality, we choose $i = 1$. We first show that $(A)_1\mathbf{v}_\theta = \theta v_1$.

$$\begin{array}{rcl} (A)_1\mathbf{v}_\theta & = & a_{11}\Delta_{11}(A - \theta I_n) + a_{12}(-1)\Delta_{12}(A - \theta I_n) + \ldots + a_{1n}(-1)^{1+n}\Delta_{1n}(A - \theta I_n) \\ & = & \det(A - \theta I) + \theta\Delta_{11}(A - \theta I_n) = \theta v_1 \end{array}$$

A similar computation holds for $i = 2, \ldots, n$.

$$\begin{array}{rcl} (A)_i\mathbf{v}_\theta & = & a_{i1}\Delta_{11}(A - \theta I_n) + a_{i2}(-1)\Delta_{12}(A - \theta I_n) + \ldots + a_{in}(-1)^{1+n}\Delta_{1n}(A - \theta I_n) \\ & = & \det(\widetilde{A}) + \theta v_i \end{array}$$

where $\widetilde{A}$ is obtained from $A-\theta I$, replacing the first row by the ith row. Since $\det(\widetilde{A})=0$, this concludes the proof. □

Step 3: Computation of α

Recall again from the proof of Theorem 4.1 that there exists an eigenvector $\mathbf{v}'_\theta = (v'_1,\ldots,v'_n)^T$ of A^T associated to θ, with $v'_i \in \mathbb{Q}(\theta)$ and such that $\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(v_i v'_j) = \delta_{ij},\ \forall i,j$. The computation of $\mathbf{v}'_\theta$ is an intermediate step to the computation of α [**6**].

Proposition 4.2. *Let $\mathbf{v}'_\theta$ be a dual basis of $\mathbb{Z}[\theta]$ for the trace form, namely $Tr(v_i v'_j) = \delta_{ij}\ \forall\ i,j$. Then*

$$v'_j := \sum_{i=1}^{n} m_{ij}\theta^{i-1} \tag{39}$$

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

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

and $V=(v_1,\ldots,v_n)$ is the matrix of the coordinates of $v_1,\ldots,v_n$ in the basis $\{1,\theta,\ldots,\theta^{n-1}\}$.

Proof. The elements $\{v_i\}_{i=1}^n$ of the basis can be expressed in the dual basis as $v_i = \sum_{i=1}^n a_{ij}v'_j$. Multiplying by v_k and taking the trace form, we get $\mathrm{Tr}(v_i v_k) = \sum_{i=1}^n a_{ij}\mathrm{Tr}(v'_j v_k) = a_{ik}$. We thus conclude that

$$v_i = \sum_{i=1}^{n} \mathrm{Tr}(v_i v_j)v'_j,$$

which can be formulated as follows:

$$\begin{aligned}(v'_1,\ldots,v'_n) &= (v_1,\ldots,v_n)(\mathrm{Tr}(v_i v_j)_{i,j=1}^n)^{-1}\\ &= (1,\theta,\ldots,\theta^{n-1})V(V^TGV)^{-1}\\ &= (1,\theta,\ldots,\theta^{n-1})G^{-1}(V^T)^{-1}.\end{aligned}$$

This yields $v'_i = \sum_{j=1}^n m_{ij}\theta^j$. □

The element α is given by (37) $\alpha\mathbf{v}_\theta = B\mathbf{v}'_\theta$. Note that 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

$$M = \begin{pmatrix} \sqrt{\alpha}_1\sigma_1(v_1) & \dots & \sqrt{\alpha}_n\sigma_n(v_1) \\ \sqrt{\alpha}_1\sigma_1(v_2) & \dots & \sqrt{\alpha}_n\sigma_n(v_2) \\ \vdots & \dots & \vdots \\ \sqrt{\alpha}_1\sigma_1(v_n) & \dots & \sqrt{\alpha}_n\sigma_n(v_n) \end{pmatrix}$$

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

Let us illustrate the algorithm.

Example 4.1. We build a lattice generator matrix of $\mathbb{Z}^4$.

(1) Take A as follows.

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

Its characteristic polynomial $\chi_A(X) = X^4 - 6X^2 + 4$ is irreducible over $\mathbb{Q}$, and A satisfies $B^{-1}AB = A^T$, i.e., $A = A^T$.

(2) Let $i = 1$. We get $\mathbf{v}_\theta^T = (-\theta^3 + 2\theta, -2\theta^2 + 2, -2\theta, -2)$.

(3) We compute the matrices G and V as explained,

$$G = \begin{pmatrix} 4 & 0 & 12 & 0 \\ 0 & 12 & 0 & 56 \\ 12 & 0 & 56 & 0 \\ 0 & 56 & 0 & 288 \end{pmatrix} \text{ and } V = \begin{pmatrix} 0 & 2 & 0 & -2 \\ 2 & 0 & -2 & 0 \\ 0 & -2 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

so that

$$\mathbf{v}'_\theta = \left(\frac{7}{40}\theta - \frac{3}{80}\theta^3, \ \frac{3}{40} - \frac{1}{40}\theta^2, \ -\frac{11}{40}\theta + \frac{1}{20}\theta^3, \ -\frac{11}{40} + \frac{1}{20}\theta^2 \right).$$

Using for example the last row, we compute $\alpha = \frac{11}{80} - \frac{1}{40}\theta^2$.

(4) Recall that θ is a root of $\chi_A(X) = X^4 - 6X^2 + 4$. The set of roots of χ_A is $\{-\frac{1}{2}\sqrt{10} - \frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{10} + \frac{1}{2}\sqrt{2}, -\frac{1}{2}\sqrt{10} + \frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{10} - \frac{1}{2}\sqrt{2}\}$. This means that the real embeddings of θ are $\sigma_1(\theta) = -2.28824$, $\sigma_2(\theta) = 2.288245$, $\sigma_3(\theta) = -0.87403$, and $\sigma_4(\theta) = 0.87403$. The generator matrix of the lattice is thus

n	minimal polynomial	d_K
2	$X^2 - X - 1$	5
3	$X^3 - X^2 - 2X + 1$	49
4	$X^4 - X^3 - 3X^2 + X + 1$	725
5	$X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$	14641
6	$X^6 - X^5 - 7X^4 + 2X^3 + 7X^2 - 2X - 1$	300125
7	$X^7 - X^6 - 6X^5 + 4X^4 + 10X^3 - 4X^2 - 4X + 1$	20134393
8	$X^8 + 2X^7 - 7X^6 - 8X^5 + 15X^4 + 8X^3 - 9X^2 - 2X + 1$	282300416

TABLE 5. Number fields with the smallest discriminant in dimension 2 to 8. Note that for all of them $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 1$ and $h(K) = 1$.

given by

$$M = \begin{pmatrix} 0.60150 & -0.60150 & -0.37174 & 0.37174 \\ -0.68819 & -0.68819 & 0.16245 & 0.16245 \\ 0.37174 & -0.37174 & 0.60150 & -0.60150 \\ -0.16245 & -0.16245 & -0.68819 & -0.68819 \end{pmatrix}.$$

4.3. $\mathbb{Z}^n$-lattices with optimized $d_{p,min}$. We apply the algorithm of Section 4.2 to build $\mathbb{Z}^n$–lattices with optimized minimum product distance.

Recall that in the case of a principal ideal $\mathcal{I} \subseteq \mathfrak{O}$, we have by Theorem 3.2 (of Chapter 2)

$$d_{p,min} = \sqrt{\frac{\det(b_\alpha)}{d_K}\frac{1}{[\mathcal{O}_K : \mathfrak{O}]}},$$

where $[\mathcal{O}_K : \mathfrak{O}]$ is the index of $\mathfrak{O}$ in $\mathcal{O}_K$. Since we are looking for the lattice $\mathbb{Z}^n$, optimizing $d_{p,min}$ leads to look for symmetric matrices (the condition $B^{-1}AB = A^T$ simplifies to $A = A^T$) such that their characteristic polynomial is the minimal polynomial of an order of minimum determinant. Since the totally real number fields with smallest discriminant are known in dimensions up to 8 (see Table 5), we naturally try to find a symmetric matrix A whose characteristic polynomial is the minimal polynomial of the desired field.

EXAMPLE 4.2. Consider the number field K given by $X^2 - X - 1$, with discriminant $d_K = 5$. The matrix

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

satisfies $\chi_A(X) = X^2 - X - 1$. We thus have $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 1$ and the lattice built over $\mathcal{O}_K$ will have maximal minimum product distance $d_{p,min} = 1/\sqrt{5}$.

n	previous constructions	Krüskemper's method
2	0.66874	0.66874
3	0.52275	0.52275
4	0.02500	0.43899
5	0.38321	0.38321
6	0.34958	0.34958
7	0.23618	0.30080
8	0.28952	0.29382

TABLE 6. $d_{p,min}^{1/n}$ for all known constructions in dimension 2 to 8

Suitable matrices A have been found in dimensions 2 up to 7 by means of a random search. There is, to our knowldege, no systematic way to construct, if it exists, a symmetric matrix with integer coefficients given a polynomial. Using Krüskemper's method, we obtain the $\mathbb{Z}^n$–lattice over the field with minimum discriminant in all dimensions from 2 up to 7. The totally real field with smallest discriminant is also known in dimension 8 (see [**39**]). However, we have not found the corresponding matrix. We use instead the polynomial $p(X) = X^8 - 7X^6 + 14X^4 - 8X^2 + 1$ with discriminant 324000000. See Table 6 for the new values of $d_{p,min}$ compared to the known ones (namely the cyclotomic and cyclic constructions). We use Krüskemper's method to build lattices over number fields with smaller discriminant in dimensions 7, 13, 17 and 19.

4.4. $\mathbb{Z}^n$–lattices over non-principal ideals. All the lattice constructions considered so far are built over principal ideals. The algorithm of Section 4.2 is the first tool that we found that yields lattice constructions also over non-principal ideals. We thus use it for trying to understand what happens in the non-principal ideals case.

Though a closed form for the minimum product distance is available, namely (by Theorem 3.2 of Chapter 2),

$$d_{p,min} = \frac{1}{\sqrt{d_K}} \frac{\min(\mathcal{I})}{[\mathcal{O}_K : \mathbb{Z}[\theta]]},$$

it is difficult to evaluate the performance of lattice codes over non-principal ideals, since $\min(\mathcal{I})$ is difficult to compute. Let us first give an example.

EXAMPLE 4.3. Consider the number field K given by $p(X) = X^2 - X - 3292$ with discriminant $d_K = 13169$, $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 1$ and $h(K) = 4$. The $\mathbb{Z}^2$–lattice is built over the ideal $\mathcal{I} = \langle -56, 13 - \theta \rangle$, where θ is a root of $p(X)$. We compute $N(\mathcal{I}) = 56$ while the norm of an element $x = a(13 - \theta) - 56b) \in \mathcal{I}$ is $N(x) = 3136b^2 - 1400ab - 3136a^2$

which is minimal in $a=-1$ and $b=1$. We thus obtain

$$\min(\mathcal{I}) = \min_{x\in\mathcal{I}}\frac{N(x)}{N(\mathcal{I})} = 1400/56 = 25$$

so that $d_{p,min} = \frac{25}{\sqrt{13169}} = 0.217853$.

For comparison, the maximal $d_{p,min}$ when $h(K)=1$ is given by 0.4472. This naturally addresses the question of knowing whether a quadratic number field K with $h(K)\geq 2$ where we get the lattice $\mathbb{Z}^2$ can give a $d_{p,min} > 0.4472$.

We show that the answer is no for $n=2$.

Proposition 4.3. *In dimension 2, the minimum product distance is maximized for the number field given by* $X^2 - X - 1$.

Proof. Let $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ such that $\chi_A(X) = X^2 + X(-a-c) + ac - b^2$ is the minimal polynomial of a number field K of degree 2. The ideal $\mathcal{I}$ over which we build $\mathbb{Z}^2$ is given by $\mathcal{I} = \langle c-\theta, -b\rangle$. The norm of an element $y\in\mathcal{I}$, $y = y_1(c-\theta) - by_2$ is $N(y) = -y_1^2b^2 - y_1y_2(bc-ba) + y_2^2b^2$. The norm of the ideal $\mathcal{I}$ is $N(\mathcal{I}) = |\det \begin{pmatrix} c & -1 \\ -b & 0 \end{pmatrix}| = |b|$. We obtain that

$$\begin{aligned}\min(\mathcal{I}) &= \min_{y_1,y_2\in\mathbb{Z}}\frac{-y_1^2b^2 - y_1y_2(bc-ba) + y_2^2b^2}{|b|}\\ &= \frac{\min(b^2, |ba-bc|)}{|b|}\\ &= \min(|b|, |a-c|).\end{aligned}$$

Since $d_K = (-a-c)^2 - 4(ac-b^2)$, $\frac{\min(\mathcal{I})}{\sqrt{d_K}[\mathcal{O}_K:\mathbb{Z}[\theta]]} = \frac{\min(|b|,|a-c|)}{\sqrt{(a+c)^2-4(ac-b^2)}C}$, where $C = [\mathcal{O}_K : \mathbb{Z}[\theta]]$. We may assume that Tr($\theta$)=1, so that $a = -c+1$, which implies that

$$\frac{\min(\mathcal{I})}{\sqrt{d_K}C} = \frac{\min(|b|, |1-2c|)}{\sqrt{(2c-1)^2 + 4b^2C}}$$

We obtain a function which is decreasing for all values of b and c in $\mathbb{Z}$. The maximum is thus given by the smallest values of b and c such that $X^2 + X(-a-c) + ac - b^2$ defines a number field, that is $b=1$ and $c=0$. □

To get some insight of what happens in higher dimensions, we look at some examples in dimension 3. When this is possible (i.e., when the matrix A exists), we compute $\min(\mathcal{I})$ for some number fields whose class number is more than 1 (cubic number fields

minimal polynomial	d_K	$[\mathcal{O}_K : \mathbb{Z}[\theta]]$	$h(K)$	$\min(\mathcal{I})$	$d_{p,min}$
$X^3 - X^2 - 111X - 14$	217981	5	2	80	0.03426
$X^3 - X^2 - 123X - 449$	254872	2	5	1	0.00099
$X^3 - 198X - 720$	473688	6	3	91	0.02203
$X^3 - 57X - 57$	653049	1	6	7	0.00866
$X^3 - 179X + 162$	1389548	4	4	4	0.00084
$X^3 - X^2 - 88X + 253$	1407153	1	2	69	0.05816
$X^3 - 101X - 315$	1442129	1	2	35	0.02914
$X^3 - 367X - 2133$	1528201	7	2	183	0.02114
$X^3 - X^2 - 373X + 12$	1717325	11	2	11	0.00076
$X^3 - X^2 - 359X - 906$	1940509	9	5	300	0.02392

TABLE 7. Cubic fields whose class number is greater than 1 and the $d_{p,min}$

datas come from the tables of PARI [**2**]). It appears (see Table 7) that the $d_{p,min}$ are far smaller than the best one, $d_{p,min} = 0.1428$, reached with the number field with smallest discriminant, that is given by $X^3 - X^2 - 2X + 1$. We conjecture in general that when $h(K) \geq 2$, $\min(\mathcal{I})$ can be large, but not large enough to compensate the increase of the discriminant d_K.

5. Performance Analysis

We briefly recall all the constructions and summarize the best choice in terms of $d_{p,min}$ for each dimension.

5.1. A summary of the constructions.

We shortly recall the constructions presented and give some comments: it appears that some constructions are built over the same number fields, while some of them give exactly the same lattice constellations.

Construction I: the cyclotomic case. Let p be an odd prime, and ζ_p be a primitive pth root of unity. The $\mathbb{Z}^n$–lattice is built over the ring of integers of $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. The available dimensions are $n = (p-1)/2$. We have $d_{p,min} = p^{-\frac{n-1}{2}}$.

Construction II: the cylic case. We consider K a cyclic extension of $\mathbb{Q}$ of odd prime degree n. The $\mathbb{Z}^n$–lattice is constructed using the ideal $\mathcal{A}$ of K such that its square is the inverse different $\mathcal{A}^2 = \mathcal{D}_{K/\mathbb{Q}}^{-1}$, so that prime dimensions are found. The minimum product distance of this lattice is $d_{p,min} = \frac{1}{p^{(n-1)/2}}$.

Construction III: the mixed case. Constellations in other dimensions are derived from Constructions I and II via the compositum of the two fields involved. In terms of lattice generator matrices, we consider the tensor product of matrices from Constructions I and II.

Krüskemper's method. We obtain the rotated $\mathbb{Z}^n$–lattice over the number field with minimum discriminant in all dimensions from 2 up to 7. We use Krüskemper's method to build lattices over number fields with small (though not minimal) discriminant in dimensions 7, 13, 17 and 19, where the other available constructions appeared to yield a poor $d_{p,min}$.

Remark 5.1. Note that in the case when $n = (p-1)/2$, Constructions I and II give the same field, and consequently the same minimum product distance. Indeed, if $n = (p-1)/2$, Construction I is available over $\mathbb{Q}(\zeta + \zeta^{-1})$. Also, we have that $p \equiv 1 \pmod{n}$ which implies that Construction II exists and is defined over a totally real subextension of degree 2 of $\mathbb{Q}(\zeta_p)$.

Remark 5.2. In dimensions 2, 3 and 5, we notice that Construction I and Krüskemper's construction give indeed the same lattice. This is not true in general. We illustrate why this happens in dimension 2.

First note that we are working on the same number field $\mathbb{Q}(\sqrt{5})$.

Construction I: $\alpha = 2 - (\zeta + \zeta^{-1})$. The generator matrix is given by

$$\begin{pmatrix} \frac{1}{\sqrt{5}}\sigma_1(\sqrt{2-(\zeta+\zeta^{-1})}(\zeta^2+\zeta^{-2})) & \frac{1}{\sqrt{5}}\sigma_2(\sqrt{2-(\zeta+\zeta^{-1})}(\zeta^2+\zeta^{-2})) \\ -\frac{1}{\sqrt{5}}\sigma_1(\sqrt{2-(\zeta+\zeta^{-1})}) & -\frac{1}{\sqrt{5}}\sigma_1(\sqrt{2-(\zeta+\zeta^{-1})}) \end{pmatrix}$$

Krüskemper's construction: $\alpha = \frac{2}{5} + \frac{1}{5}\theta$. The generator matrix is given by

$$\begin{pmatrix} \frac{1}{\sqrt{5}}\sigma_1(\sqrt{2+\theta}(1-\theta)) & \frac{1}{\sqrt{5}}\sigma_2(\sqrt{2+\theta}(1-\theta)) \\ -\frac{1}{\sqrt{5}}\sigma_1(\sqrt{2+\theta}) & -\frac{1}{\sqrt{5}}\sigma_1(\sqrt{2+\theta}) \end{pmatrix}$$

Because $\theta = 1.61803 = -(\zeta^2 + \zeta^{-2}) = -2\cos(\frac{4\pi}{5})$ and $1 - \theta = -0.61803 = -(\zeta + \zeta^{-1}) = -2\cos(\frac{2\pi}{5})$, we immediately see that up to a sign, we have the same matrix, so that we have the same lattice. The same thing happens in dimension 3 and 5.

In Figure 5, we compare the discriminants found to Odlyzko's bounds. We observe that they are close to the bounds, except in dimensions 7, 13, 17, 19 and 25. Though the found discriminants are not in the continuity of the others (as shown in Figure 5), we

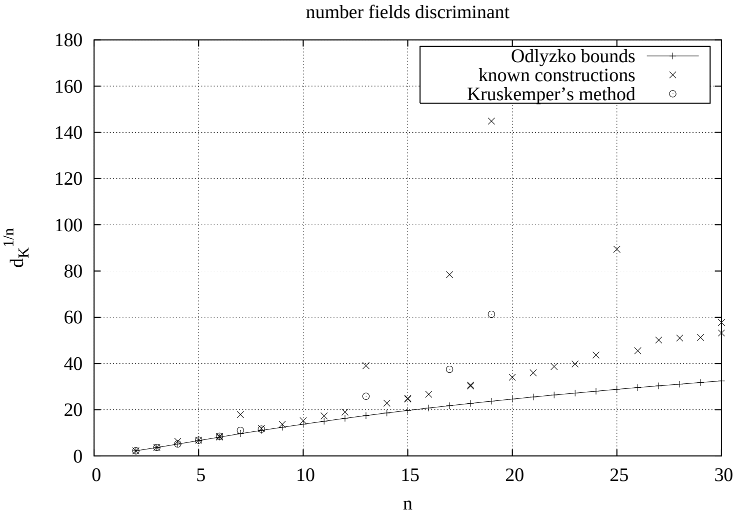

FIGURE 5. $d_{p,min}$ of the known (cyclotomic and cyclic) constructions compared to Krüskemper's method and Odlyzko's bounds.

n	coding gain
7	0.0301
13	0.0855
17	0.1179
19	0.2064
25	0.2461

TABLE 8. Values of coding gain in dB

show that they are almost optimal in the sense that any improvement would bring a negligeable coding gain.

Recall (Definition 3.1) that the coding gain is given by:

$$\gamma = 10 \log_{10} \left(\frac{d_{p,min}(1)}{d_{p,min}(2)} \right)^{1/n} \text{ [dB]}$$

where $d_{p,min}(i)$, $i = 1, 2$ are the minimum product distances of two constellations with the same maximal diversity. We compute the coding gain obtained using a number field whose discriminant would reach Odlyzko's bound (relatively to our constructions), see Table 8. We observe that the maximal gain would be of 0.2 dB, which is negligeable.

5.2. Simulation results. A rotated $\mathbb{Z}^n$–lattice with diversity L is obtained by applying the rotation matrix R to the integer grid $\mathbb{Z}^n$, i.e.

$$\Lambda = \{\mathbf{x} = \mathbf{u}R, \ \mathbf{u} \in \mathbb{Z}^n\}$$

n	Cyclotomic constructions	Cyclic constructions	Mixed constructions
2	0.66874	-	-
3	0.52275	0.52275	-
4	-	-	0.02500
5	0.38321	0.38321	-
6	0.34344	-	0.34958
7	-	0.23618	-
8	0.28952	-	-
9	0.27018	-	-
10	-	-	0.25627
11	0.24045	0.24045	-
12	-	-	0.22967
13	-	0.16002	-
14	0.20942	-	-
15	0.20138	-	0.20032
16	-	-	0.19361
17	-	0.11292	-
18	0.18174	-	0.18068
19	-	0.08308	-
20	0.17136	-	-
21	0.16678	-	-
22	-	-	0.16080
23	0.15859	0.15859	-
24	-	-	0.15134
25	-		0.10574
26	0.14825	-	-
27	-	-	0.14124
28	-	-	0.14005
29	0.13967	0.13967	-
30	0.13711	-	0.13161

TABLE 9. Comparison of the values of $d_{p,min}^{1/n}$ for cyclotomic, cyclic and mixed constructions.

The finite signal constellation is carved from this lattice by restricting the elements of $\mathbf{u}$ to a finite set of integers such as $\{\pm 1, \pm 3, \ldots \pm (2^{\eta/2} - 1)\}$, where η is the spectral efficiency measured in bits per two dimensions.

The rotated $\mathbb{Z}^n$–lattice constellations have been simulated over an independent Rayleigh fading channel as described in Chapter 1. Best minimum product distance lattices among the families we considered are summarized in Table 9. Note that the mixed construction yields a higher $d_{p,min}$, only for $n = 6$ and that $d_{p,min}^{1/n}$ decreases with n, suggesting that it vanishes asymptotically.

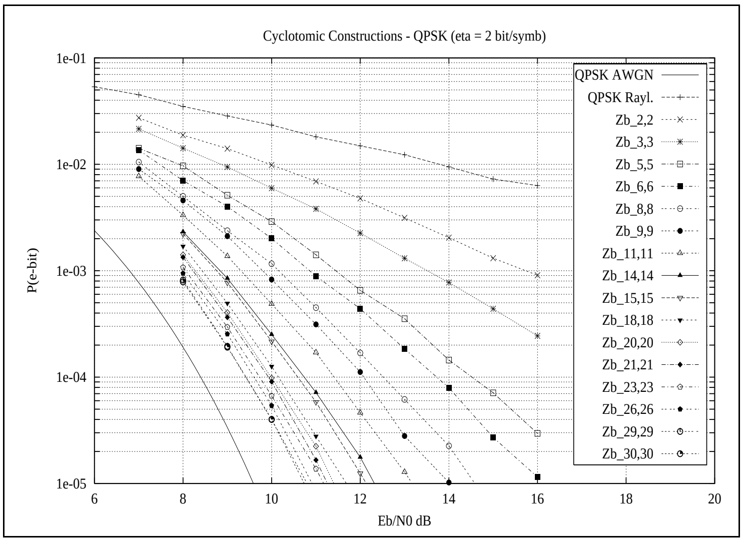

Figure 6. Cyclotomic construction with QPSK

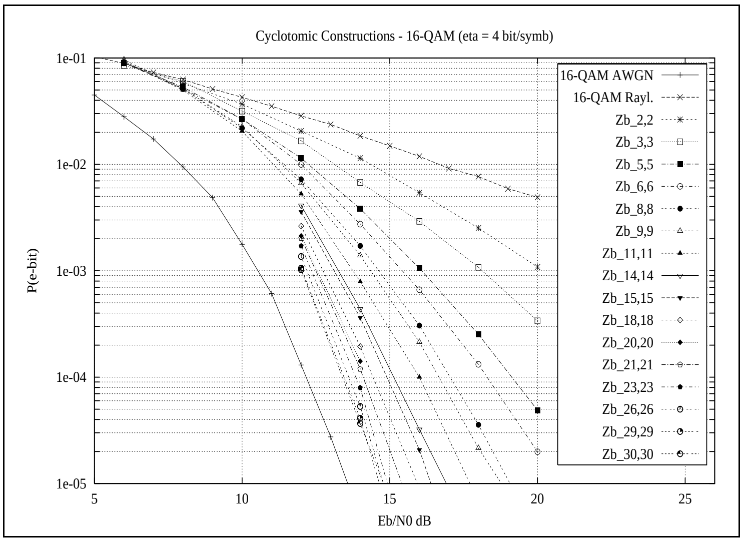

Figure 7. Cyclotomic construction with 16-QAM

Figures 6, 7, 8 and 9 show the bit error rates of the rotated $\mathbb{Z}^n$ constellations for $\eta = 2, 4$ and for the cyclotomic and cyclic constructions. For comparison, the performance of a standard component interleaved QPSK (resp. 16 QAM) over Gaussian and Rayleigh fading channels is reported in the figures. We can observe how the bit error rate performance over Rayleigh fading channel approaches the one over the Gaussian channel as the diversity increases. Clearly, this gain is obtained at the expense of a higher decoding complexity due to the greater lattice dimension [**53**], but no extra bandwidth is used.

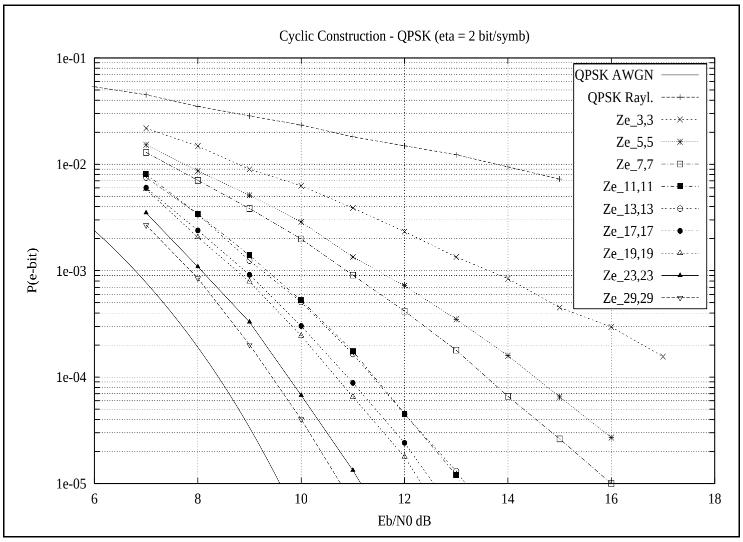

FIGURE 8. Cyclic construction with QPSK

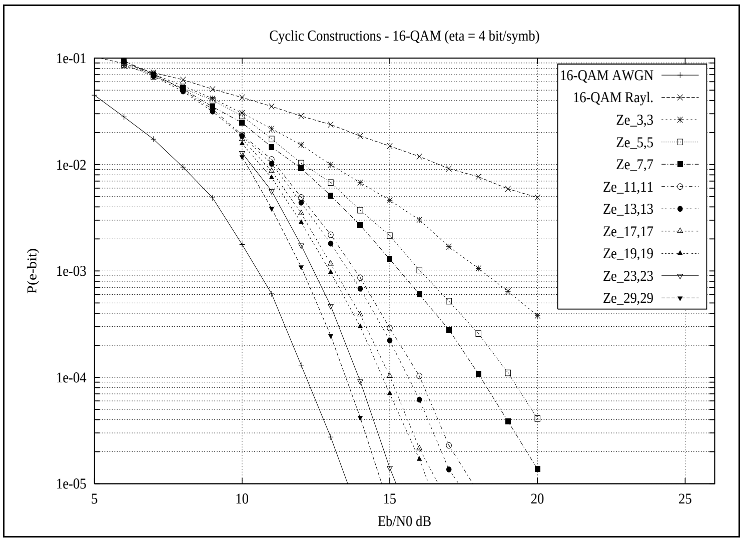

FIGURE 9. Cyclic construction with 16-QAM

6. Complex Constructions

This section discusses various constructions of complex lattices. We first recall a known construction over cyclotomic fields, in order to compute its minimum product distance, before introducing two new types of constructions.

6.1. Cyclotomic fields $\mathbb{Q}(\zeta_{2^r})$. Complex lattice constructions from cyclotomic fields were found in [**19, 12**]. Here we show that these lattices may be seen as ideal lattices, which allows to evaluate the complex minimum product distance (see Definition 5.2 of Chapter 2) in terms of field discriminants.

Let $L = \mathbb{Q}(\zeta)$, where $\zeta = \zeta_{2^r}$.

Proposition 6.1. *We have that $\mathcal{O}_L = \mathbb{Z}[\zeta]$ is a free $\mathbb{Z}[i]$-module of rank 2^{r-2} and a $\mathbb{Z}[i]$–basis is given by $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-2}-1}\}$.*

Proof. We show that $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-2}-1}\}$ is a $\mathbb{Z}[i]$–basis of $\mathbb{Z}[\zeta]$. Let x be in $\mathbb{Z}[\zeta]$. Since $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{r-1}-1}\}$ is a $\mathbb{Z}$–basis, we have:

$$\begin{aligned} x &= \sum_{k=0}^{2^{r-2}-1} a_k \zeta^k + \sum_{k=2^{r-2}}^{2^{r-1}-1} a_k \zeta^k, \ a_k \in \mathbb{Z} \\ &= \sum_{k=0}^{2^{r-2}-1} a_k \zeta^k + \sum_{l=0}^{2^{r-2}-1} i\tilde{a}_l \zeta^l, \ \tilde{a}_l = a_{l+2^{r-2}} \in \mathbb{Z} \\ &= \sum_{k=0}^{2^{r-2}-1} (a_k + i\tilde{a}_k)\zeta^k \end{aligned}$$

and this representation of x is unique. □

The following result was proved in [**19**].

Proposition 6.2. *Consider the ideal lattice $\Lambda^c = (\mathcal{O}_L, b)$ where $L = \mathbb{Q}(\zeta)$ is of degree $n = 2^{r-2}$ over $\mathbb{Q}(i)$ and $b(x, y) = \frac{1}{2^{r-2}} Tr_{L/\mathbb{Q}(i)}(x\bar{y})$, for all $x, y \in \mathcal{O}_L$. Then Λ^c is isomorphic to the $\mathbb{Z}[i]^n$–lattice.*

Let us now consider the product distance of Λ^c. Since $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta + \zeta^{-1})\mathbb{Q}(i)$, we apply Theorem 5.1 of Chapter 2.

Proposition 6.3. *The relative discriminant $d_{\mathbb{Q}(\zeta)/\mathbb{Q}(i)}$ satisfies*

$$|d_{\mathbb{Q}(\zeta)/\mathbb{Q}(i)}| = (2^{r-2})^{2^{r-2}} \tag{40}$$

Proof. The relative discriminant $|d_{\mathbb{Q}(\zeta)/\mathbb{Q}(i)}|$ is given by $|N_{\mathbb{Q}(\zeta)/\mathbb{Q}(i)}(f'(\zeta))|$ [**41**, p. 49], where f is the minimal polynomial of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(i)$ and $\zeta = \zeta_{2^r}$. Since $f(X) = X^{2^{r-2}} + i$, $f'(\zeta) = 2^{r-2} i \zeta^{-1}$. Thus

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}(i)}(f'(\zeta)) = (2^{r-2} i)^{2^{r-2}} N_{\mathbb{Q}(\zeta)/\mathbb{Q}(i)}(\zeta^{-1}), \tag{41}$$

and we conclude taking the absolute value. □

The minimum product distance of the above ideal lattice Λ^c is then given combining Theorem 5.1 and Proposition 6.3

$$d_{p,min}(\Lambda^c) = (2^{r-2})^{-2^{r-3}}. \tag{42}$$

6.2. Complex constructions from real ones. We show a simple method to derive unitary complex matrices (i.e., rotated $\mathbb{Z}[i]^n$–lattices) from known constructions of rotated $\mathbb{Z}^n$–lattices from totally real number fields. Then we compute their minimum product distance.

Let K be a totally real number field, and L be the compositum of K and $\mathbb{Q}(i)$. We are interested in the extension $L/\mathbb{Q}(i)$. A $\mathbb{Z}[i]$–basis is easily derived.

Lemma 6.1. *(a) Suppose K has an odd discriminant (so that d_K and $d_{\mathbb{Q}(i)}$ are coprime). Let $\mathcal{B}_K = \{\nu_j\}_{j=1}^n$ be a $\mathbb{Z}$–basis of K. Then $\mathcal{B}_K$ is a $\mathbb{Z}[i]$–basis of L.*
(b) Let $\mathcal{B}_L = \{\omega_j\}_{j=1}^n$ be a $\mathbb{Z}[i]$–basis of L. Then $\{i\omega_j\}_{j=1}^n$ is a also a $\mathbb{Z}[i]$–basis of L.

Proof. (a) Let x be in L. Since $(d_K, d_{\mathbb{Q}(i)}) = 1$, a $\mathbb{Z}$–basis of L is given by $\{\nu_1, \dots, \nu_n, i\nu_1, \dots, i\nu_n\}$ [**48**, p. 48]. Thus $x = \sum_{j=1}^n (a_j + ib_j)\nu_j$, $a_j, b_j \in \mathbb{Z}\ \forall j$.
(b) This is clear since i is a unit of $\mathbb{Z}[i]$.

□

The previous Lemma clearly extends to a basis of any ideal of $\mathcal{O}_L$, which may be used to construct an ideal lattice as explained in the following proposition.

Proposition 6.4. *Let $B_{\mathcal{I}} = \{\omega_j = i\nu_j\}_{j=1}^n$ be a $\mathbb{Z}[i]$–basis of an ideal $\mathcal{I} \subseteq \mathcal{O}_L$. We have*

$$Tr_{L/\mathbb{Q}(i)}(\omega_j \overline{\omega_k}) = Tr_{K/\mathbb{Q}}(\nu_j \nu_k). \tag{43}$$

Proof. We have

$$\mathrm{Tr}_{L/\mathbb{Q}(i)}(\omega_j \overline{\omega_k}) = \mathrm{Tr}_{L/\mathbb{Q}(i)}(\nu_j \overline{\nu_k}) = \mathrm{Tr}_{K/\mathbb{Q}}(\nu_j \nu_k)$$

where the last equality holds since $\mathrm{Gal}(L/\mathbb{Q}(i)) = \mathrm{Gal}(K/\mathbb{Q})$ [**48**, p. 47]. □

This construction always yields a purely imaginary lattice generator matrix. In practice, the same rotation may be obtained by directly applying the real generator matrix of Λ, obtained from the field K, to a complex vector in $\mathbb{Z}[i]^n$. However, our point of view enables to evaluate the complex minimum product distance from Corollary 5.1 of Chapter 2

$$d_{p,min}(\Lambda^c) = d_{p,min}(\Lambda) \ . \tag{44}$$

The following example shows how to build a $\mathbb{Z}[i]^n$–lattice using a $\mathbb{Z}^n$–lattice.

Example 6.1. Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ and $\alpha = 2 - (\zeta_7 + \zeta_7^{-1})$. A $\mathbb{Z}^3$–lattice is built using the ideal $\mathcal{I}_K = (\alpha)\mathcal{O}_K$ of $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ as follows. A $\mathbb{Z}$–basis of the ideal $\mathcal{I}_K$ is given by $\{\alpha(\zeta_7^3 + \zeta_7^{-3}), \alpha(\zeta_7^3 + \zeta_7^{-3} + \zeta_7^2 + \zeta_7^{-2}), -\alpha\} = \{\nu_i\}_{i=1}^3$. By direct computation we have

$$\frac{1}{7}\mathrm{Tr}_{K/\mathbb{Q}}(\nu_i \nu_j) = \delta_{ij} \ i, j = 1, 2, 3.$$

The lattice generator matrix of $\Lambda(\mathcal{I}_K)$ can be used to define a $\mathbb{Z}[i]^3$–lattice $\Lambda^c(\mathcal{I}_L)$, where $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, i)$ and $\mathcal{I}_L = (\alpha)\mathcal{O}_L$. Using Proposition 6.4, the lattice generator matrix of $\Lambda^c(\mathcal{I}_L)$, becomes

$$\begin{pmatrix} 0.327985277i & -0.736976229i & -0.591009048i \\ -0.736976229i & -0.591009048i & 0.327985277i \\ -0.591009048i & 0.327985277i & -0.736976229i \end{pmatrix}.$$

Since $d_K = 49$, the complex minimum product distance of this lattice is given by

$$d_{p,min}(\Lambda^c) = 1/7 \ .$$

6.3. Some other constructions. The previous method gives lattice generator matrices that are purely imaginary. One may ask if fully complex coefficients could be obtained. We discuss this question in some particular cases.

As in the previous section, we work with the compositum field $L = K\mathbb{Q}(i)$. Instead of starting from the real $\mathbb{Z}^n$–lattice from K, we attempt to directly construct the $\mathbb{Z}[i]^n$–lattice on a particular ideal $\mathcal{I}$ of $\mathcal{O}_L$. Our approach is the following:

- Consider the ramification in $L/\mathbb{Q}$. The prime factorization of the discriminant $d_{L/\mathbb{Q}} = \prod p_i^{r_i}$ contains the primes which ramify, i.e., $(p_i)\mathcal{O}_L = \prod_j \mathfrak{P}_{ij}^{e_i}$ where $e_i > 1$.
- Considering real lattices, we know that $\mathrm{vol}(\Lambda(\mathcal{O}_L)) = \sqrt{|d_{L/\mathbb{Q}}|}$. We look for a sublattice $\Lambda(\mathcal{I})$ of $\Lambda(\mathcal{O}_L)$, which could be a scaled version of $\mathbb{Z}^{2n}$, i.e., $\Lambda(\mathcal{I}) = (\sqrt{c}\mathbb{Z})^{2n}$ for some integer c.

- Since $\Lambda(\mathcal{I})$ is a sublattice of $\Lambda(\mathcal{O}_L)$, $\mathrm{vol}(\Lambda(\mathcal{O}_L)) = \sqrt{|d_{L/\mathbb{Q}}|}$ must divide $\mathrm{vol}(\Lambda(\mathcal{I})) = c^n$, i.e., $\prod p_i^{r_i}$ divides c^{2n}.
- This gives a necessary condition for the choice of $\mathcal{I}$. In terms of norm of the ideal $\mathcal{I}$ [**41**, p. 69], we need

$$N(\mathcal{I}) = |\mathcal{O}_L/\mathcal{I}| = \frac{\mathrm{vol}(\Lambda(\mathcal{I}))}{\mathrm{vol}(\Lambda(\mathcal{O}_L))} = \frac{c^n}{\sqrt{\prod p_i^{r_i}}}. \tag{45}$$

- In order to satisfy (45), we must find an ideal of the form

$$\mathcal{I} = \prod \mathfrak{P}_{ij}^{s_{ij}} \tag{46}$$

with norm $\prod p_i^{n-r_i/2}$.

From Corollary 5.1 of Chapter 2, the minimum product distance is

$$d_{p,min}(\Lambda^c) = \frac{1}{\sqrt{d_K}}. \tag{47}$$

6.3.1. *Dimension 2.* Denote $\theta = \zeta_5 + \zeta_5^{-1}$ and let $L = \mathbb{Q}(i, \theta)$. The Galois group $\mathrm{Gal}(L/\mathbb{Q}(i))$ is of order 2, generated by σ, that acts on θ as follows: $\sigma(\theta) = -1 - \theta$. We have

$$(5)\mathcal{O}_L = \mathfrak{P}_1^2\mathfrak{P}_2^2 = (1 - i\theta)^2(1 - i\sigma(\theta))^2$$

so that $N(\mathfrak{P}_1) = N(\mathfrak{P}_2) = 5$.

We take the principal ideal $\mathcal{I} = \mathfrak{P}_1 = (\alpha)\mathcal{O}_L$ with $\alpha = 1 - i\theta$, which satisfies (45). A $\mathbb{Z}[i]$–basis of $\mathcal{I}$ is $\{\alpha, \alpha\theta\}$. Using the change of basis given by the matrix

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

we get for $(\alpha)\mathcal{O}_L$ the new $\mathbb{Z}[i]$–basis $\{\nu_i\}_{i=1}^2 = \{1 - i\theta, 1 - i + \theta\}$. Then it is a straightforward computation, to show that

$$\frac{1}{5}\mathrm{Tr}_{L/\mathbb{Q}}(\nu_i\bar{\nu_j}) = \delta_{ij}\ i, j = 1, 2.$$

For example

$$\begin{aligned} \mathrm{Tr}_{L/\mathbb{Q}(i)}((1 - i\theta)\overline{(1 - i\theta)}) &= \mathrm{Tr}_{L/\mathbb{Q}(i)}(1 + \theta^2) \\ &= \mathrm{Tr}_{L/\mathbb{Q}(i)}(2 - \theta) \\ &= \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(2) - \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = 5. \end{aligned}$$

The generator matrix of the lattice is given by

$$\begin{pmatrix} \nu_1 & \sigma(\nu_1) \\ \nu_2 & \sigma(\nu_2) \end{pmatrix} = \begin{pmatrix} 1-i\theta & 1+i+i\theta \\ 1-i+\theta & -i-\theta \end{pmatrix} = \begin{pmatrix} 0.447-0.276i & 0.447+0.723i \\ 0.723-0.447i & -0.276-0.447i \end{pmatrix}.$$

The lattice generator matrix is fully complex as opposed to the one obtained with the method of Section 6.2 using $K=\mathbb{Q}(\theta)$ and $\alpha = 2-\theta$. Its minimum product distance is

$$d_{p,min}(\Lambda^c) = \frac{1}{\sqrt{5}} \ .$$

6.3.2. *Dimension 3.* In Example 6.1 we found a purely imaginary generator matrix for dimension 3, using $K=\mathbb{Q}(\theta)$, $\theta = \zeta_7 + \zeta_7^{-1}$. We have

$$(7)\mathcal{O}_K = \mathfrak{P}^3 = (2-\theta)^3$$

so that $N_{K/\mathbb{Q}}(\mathfrak{P}) = 7$. The prime above 7 in $L=\mathbb{Q}(i,\theta)$ is $(2-\theta)$ and has norm 7. So if we consider $(2-\theta)$ as an element of L, it has norm 49. No other ideal with this norm can be found, hence we only find the $\mathbb{Z}[i]^n$–lattice with a purely imaginary matrix as given in Example 6.1.

6.3.3. *Dimension 4.* Let $\theta = \zeta_{15}+\zeta_{15}^{-1}$ and $L=\mathbb{Q}(\theta,i)$. Consider the ideal $(\alpha) = ((1-3i)+i\theta^2)$ of $\mathcal{O}_L$. A $\mathbb{Z}[i]$–basis of (α) is given by $\{\alpha\theta^i\}_{i=0}^3$. Using the change of basis given by the following matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{pmatrix},$$

one gets a new $\mathbb{Z}[i]$–basis $\{\nu_i\}_{i=1}^4 = \{(1-3i)+i\theta^2, (1-3i)\theta+i\theta^3, -i+(-3+4i)\theta+(1-i)\theta^3, (-1+i)-3\theta+\theta^2+\theta^3\}$. Then by straightforward computation we find

$$\frac{1}{15}\mathrm{Tr}_{L/\mathbb{Q}}(\nu_i\bar{\nu_j}) = \delta_{ij} \ i,j=1,\dots,4$$

using

$$\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = 1,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 9, \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) = 1,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) = 29.$$

n	Section 6.1	Section 6.3
2	0.5	0.44721359
3	-	0.14285714
4	0.0625	0.02981423

TABLE 10. Comparison of $d_{p,min}$ for constructions in Section 6.1 and 6.3

We compute as example the diagonal coefficients to show that they are all equal to 15:

$$\mathrm{Tr}_{L/\mathbb{Q}(i)}(|\nu_i|^2) = \begin{cases} \mathrm{Tr}_{L/\mathbb{Q}(i)}(10 - 6\theta^2 + \theta^4) & \text{if } i = 1 \\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(1 + 3\theta + \theta^2 - \theta^3) & \text{if } i = 2 \\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(5 + 6\theta - \theta^2 - 2\theta^3) & \text{if } i = 3 \\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(-5\theta + 2\theta^2 + 2\theta^3) & \text{if } i = 4 \end{cases}$$

Using the basis $\{\nu_i\}_{i=1}^4$, we find the lattice generator matrix

$$\begin{pmatrix} 0.2582 - 0.3122i & 0.3455 - 0.4178i & -0.4178 + 0.5051i & -0.2136 + 0.2582i \\ 0.2582 + 0.0873i & 0.4718 + 0.1596i & 0.1596 + 0.054i & 0.7633 + 0.2582i \\ 0.2582 + 0.2136i & -0.5051 - 0.4178i & -0.4178 - 0.3455i & 0.3122 + 0.2582i \\ 0.2582 - 0.7633i & -0.054 + 0.1596i & 0.1596 - 0.4718i & -0.0873 + 0.2582i \end{pmatrix}.$$

Its minimum product distance is

$$d_{p,min}(\Lambda^c) = \frac{1}{\sqrt{1125}}.$$

REMARK 6.1. It is an open question whether fully complex matrices can be obtained for dimensions other than 2 and 4.

7. Performance of Complex Lattices

Performance of ideal $\mathbb{Z}[i]$–lattices depends, as in the real case, on both diversity (which is already maximal) and minimum product distance, which has to be maximized.

As shown in Theorem 5.1 of Chapter 2, the minimum product distance of complex lattices depends on a relative discriminant $d_{L/\mathbb{Q}(i)}$. For example, some numerical values of the $d_{p,min}$ for constructions given in the previous section are available in Table 10.

In order to compute relative discriminants, we use a transitivity formula [**48**]:

$$d_{L/\mathbb{Q}} = d^n_{\mathbb{Q}(i)/\mathbb{Q}} N_{\mathbb{Q}(i)/\mathbb{Q}}(d_{L/\mathbb{Q}(i)}) \qquad (48)$$

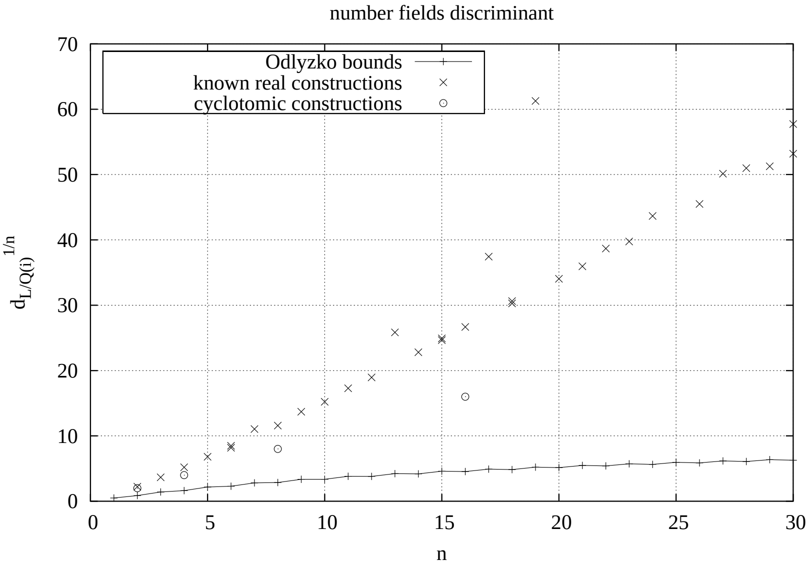

FIGURE 10. Comparison of discriminants among the known constructions and Odlyzko's bounds

where n is the degree of L over $\mathbb{Q}(i)$. Since $N_{\mathbb{Q}(i)/\mathbb{Q}}(d_{L/\mathbb{Q}(i)}) = |d_{L/\mathbb{Q}(i)}|^2$, we get

$$|d_{L/\mathbb{Q}(i)}| = 2^{-n}\sqrt{|d_{L/\mathbb{Q}}|} \tag{49}$$

where L is a totally complex number field.

We already noticed in Corollary 5.1 of Chapter 2 that when d_K is odd, then the relative discriminant is nothing else than d_K itself, i.e., $d_{L/\mathbb{Q}(i)} = d_K$.

As explained in Section 5 of Chapter 2, we can use Odlyzko's bounds to give a lower bound on totally complex number field discriminants. Knowing that $|d_{L/\mathbb{Q}}|^{1/2n} \geq C_{2n}$, we consequently get a bound on the relative discriminant:

$$|d_{L/\mathbb{Q}(i)}|^{1/n} \geq C_{2n}/2 \tag{50}$$

In Figure 10, we compare Odlyzko's bounds for $|d_{L/\mathbb{Q}(i)}|^{1/n}$ to known values of d_K and relative discriminants obtained from cyclotomic constructions. One easily notices that the bound for $|d_{L/\mathbb{Q}(i)}|^{1/n}$ grows very slowly. This can be explained by the fact that discriminants of totally complex number fields are much smaller than the ones of totally real number fields. The large gap from the bound can be explained by the fact that the family of number fields L necessary to produce complex ideal lattices is limited to CM fields containing $\mathbb{Q}(i)$. On the other hand, Odlyzko's bound is valid for arbitrary number fields.

CHAPTER 4

Code Design Criteria for MIMO Channels

In order to achieve high data rate over wireless channels, we need multiple antennas at both transmitter and receiver ends (MIMO stands for multiple input/ multiple output channel). This is a generalization of the model considered in Chapter 1, where there were one transmit and one receive antenna.

1. The MIMO Channel Model

As an example, consider the case in which we have two transmit and three receive antennas (see Fig. 1). The symbols $x_1, \ldots, x_4$ are to be transmitted. The first (resp. the second) antenna has to send the symbols x_1, x_3 (resp. x_2, x_4). First, the two symbols x_1, x_2 are sent over the channel, and are received by the three antennas, which yields the received symbols y_1, y_2, y_3, where each y_i is a combination of x_1, x_2 attenuated, similarly to the case of one antenna, by fading coefficients h_{ij}. Next, the two other symbols x_3, x_4 will be sent, and similarly, we will have at the receiver three received symbols y_4, y_5, y_6. If we summarize, the transmitted codeword can be written as a matrix $\mathbf{X}$ containing the four symbols $x_1, \ldots, x_4$, and the received codeword is a matrix $\mathbf{Y}$ which is of the form

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{Z}, \tag{51}$$

where $\mathbf{H}$ is the channel matrix and $\mathbf{Z}$ is a noise matrix.

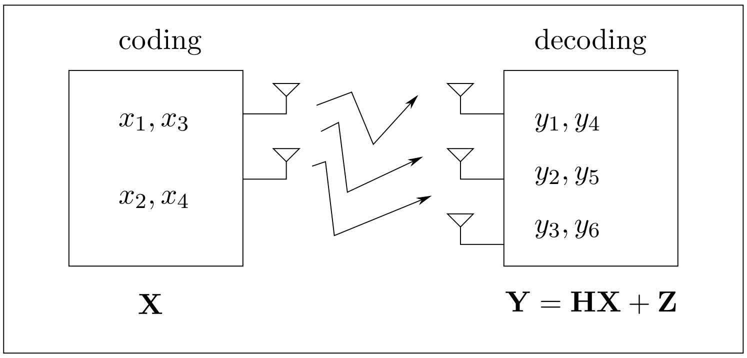

Figure 1. Channel model for two transmit and three receive antennas

This can be generalized for any number of antennas (note that the number of transmit and receive antennas do not need to be the same).

Let the number of transmit antennas be M_t and the number of receive antennas be M_r. If $\mathbf{y}(k) \in \mathbb{C}^{M_r}$ is the received (column) vector at time k, we can write

$$\mathbf{y}(k) = \mathbf{H}(k)\,\mathbf{x}(k) + \mathbf{z}(k)\ , \tag{52}$$

where the matrix $\mathbf{H}(k) \in \mathbb{C}^{M_r \times M_t}$ represents the channel, the column vector $\mathbf{x}(k) \in \mathbb{C}^{M_t}$ is the channel input and $\mathbf{z}(k) \in \mathbb{C}^{M_r}$ is zero mean i.i.d. Gaussian noise with $\mathbb{E}[\mathbf{z}(k)\mathbf{z}(k)^H] = N_0\mathbf{I}$. We assume a Rayleigh flat fading model, i.e. that the elements of $\mathbf{H}(k)$ are i.i.d. with a zero mean complex Gaussian distribution of unit variance. The channel is assumed to be block time-invariant, that is, $\mathbf{H}(k)$ is independent of k over a transmission block of m symbols, say $\mathbf{H}(k) = \mathbf{H}$ (although $\mathbf{H}(k)$ may vary from block to block). Looking at a single block of length m, during which the channel is assumed to be time-invariant, we can write

$$\begin{aligned} \mathbf{Y} &= [\mathbf{y}(1), \ldots, \mathbf{y}(m)] \\ &= \mathbf{H}[\mathbf{x}(1), , \ldots, \mathbf{x}(m)] + [\mathbf{z}(1), \ldots, \mathbf{z}(m)] = \mathbf{HX} + \mathbf{Z}\ , \end{aligned} \tag{53}$$

which is a generalization of (51). The transmitted codeword $\mathbf{X}$ belongs to a codebook (or space-time code) $\mathcal{C}$. Information symbols are taken from a signal constellation (or alphabet) $\mathcal{A}$, and are encoded into the codewords $\mathbf{X}$.

Notice that in the case of MIMO channels, there are two ways of defining the rate of a code.

Definition 1.1. *Let $\mathcal{A}$ be the signal constellation and $\mathcal{C}$ be a codebook. The rate in bits per channel use is defined by*

$$R = \frac{1}{m}\log_{|\mathcal{A}|}(|\mathcal{C}|)$$

where $|\mathcal{C}|$ denotes the cardinality of the codebook.

An alternative definition imitates the classical definition of rate used in the case of linear error correcting codes.

Definition 1.2. *The rate of a $M_t \times M_r$ space-time code $\mathcal{C}$ is given by*

$$R = \frac{\#\{\textit{information symbols}\}}{M_t \cdot M_r}.$$

There is traditionally a distinction depending on whether the receiver knows the channel. The case where the receiver is assumed to know the channel matrix $\mathbf{H}$ is called *coherent*. It is called *non-coherent* otherwise. In the two next sections, we will give the code design criteria for each of these cases.

2. The Coherent Case

We consider the coherent case in which the receiver has perfect knowledge of all the channel coefficients (perfect CSI). Recall that the received signal is:

$$\mathbf{Y}_{M_r \times m} = \mathbf{H}_{M_r \times M_t} \cdot \mathbf{X}_{M_t \times m} + \mathbf{Z}_{M_r \times m} \tag{54}$$

where $\mathbf{X}$ is the transmitted codeword of duration m taken from the codebook $\mathcal{C}$, $\mathbf{H}$ is the channel matrix with i.i.d. Gaussian entries and $\mathbf{Z}$ is the i.i.d. Gaussian noise matrix.

The conditional pairwise error probability is bounded by [**50**]

$$P(\ \mathbf{X} \to \hat{\mathbf{X}} \mid \mathbf{H}\ ) \leq \exp\left(-d^2(\mathbf{X}, \hat{\mathbf{X}}) E_s / 4N_0\right),$$

where E_s is the signal power per transmit antenna. The distance $d^2(\mathbf{X}, \hat{\mathbf{X}})$ is given by

$$d^2(\mathbf{X}, \hat{\mathbf{X}}) = \sum_{j=1}^{M_r} H_j B(\mathbf{X}, \hat{\mathbf{X}}) B(\mathbf{X}, \hat{\mathbf{X}})^H H_j^H,$$

where H_j is the jth column of $\mathbf{H}$ and $B(\mathbf{X}, \hat{\mathbf{X}})_{i,j} = x_{j,i} - \hat{x}_{j,i}$, $i = 1, \ldots, M_t$, $j = 1, \ldots, m$. Expressing $d^2(\mathbf{X}, \hat{\mathbf{X}})$ in terms of the eigenvalues λ_i, $i = 1, \ldots, M_t$, of the matrix $A(\mathbf{X}, \hat{\mathbf{X}}) = B(\mathbf{X}, \hat{\mathbf{X}}) B(\mathbf{X}, \hat{\mathbf{X}})^H$, we get

$$P(\ \mathbf{X} \to \hat{\mathbf{X}} \mid \mathbf{H}\ ) \leq \prod_{j=1}^{M_r} \exp\left(-(E_s/4N_0) \sum_{i=1}^{M_t} \lambda_i |\beta_{i,j}|^2\right)$$

where $|\beta_{i,j}|$ are independent Rayleigh distributed random variables (see [**50**] for more details). An upper bound on the average probability of error is computed by averaging with respect to the independent Rayleigh distributions of $|\beta_{i,j}|$. This yields

$$P(\ \mathbf{X} \to \hat{\mathbf{X}}\ ) \leq \left(\frac{1}{\prod_{i=1}^{M_t} (1 + \lambda_i E_s / 4N_0)}\right)^{M_r}. \tag{55}$$

Let r denote the rank of the matrix $A(\mathbf{X}, \hat{\mathbf{X}})$, and say the nonzero eigenvalues of $A(\mathbf{X}, \hat{\mathbf{X}})$ are $\lambda_1, \ldots, \lambda_r$. Then it follows from Equation (55) that for high SNR

$$P(\ \mathbf{X} \to \hat{\mathbf{X}}\ ) \leq \left(\prod_{i=1}^{r} \lambda_i\right)^{-M_r} (E_s/4N_0)^{-rM_r}, \tag{56}$$

meaning that a *diversity order* of rM_r and a *coding gain* of $(\lambda_1 \cdots \lambda_r)^{M_r}$ are achieved. The coding gain is an approximate measure of the gain over an uncoded system operating with the same diversity order.

Consequently, minimizing the above probability of error requires to consider two criteria.

(1) *The rank criterion*: in order to achieve the maximum diversity M_tM_r, the matrix $B(\mathbf{X}, \hat{\mathbf{X}})$ has to be full rank for any pair of codewords $\mathbf{X}$ and $\hat{\mathbf{X}}$. Codes that achieve the maximal diversity are called *fully diverse*.

(2) *The determinant criterion*: if a diversity of M_tM_r is the design target, then the minimum of the determinant of $A(\mathbf{X}, \hat{\mathbf{X}})$ taken over all pairs of distinct codewords must be maximized.

Note that the diversity order corresponds to the slope of the error probability with respect to SNR in log-log plot.

3. The Noncoherent Case

We assume now that the receiver will not attempt to estimate the channel matrix $\mathbf{H}$, i.e. that we have a noncoherent receiver. Again, a received codeword is given by

$$\mathbf{Y}_{M_r \times m} = \mathbf{H}_{M_r \times M_t} \cdot \mathbf{X}_{M_t \times m} + \mathbf{Z}_{M_r \times m}. \tag{57}$$

It has been shown in [**26**] that

$$P(\mathbf{Y}|\mathbf{X}) = \frac{\exp(-\mathrm{Tr}[\mathbf{Y}\Psi^{-1}\mathbf{Y}^H])}{\det(\pi\Psi)^{M_r}} ,$$

where $\Psi = \mathbf{I}_m + E_s\mathbf{X}^H\mathbf{X}$ is the covariance matrix of the received symbols at a particular antenna and E_s is the signal power per transmit antenna.

In the absence of channel state information at the receiver, Hochwald and Marzetta [**26**] argue that for high SNR, one should use unitary codewords $\mathbf{X}$, that is satisfying $\mathbf{X}\mathbf{X}^H = m\mathbf{I}_{M_t}$. Thus the Maximum Likelihood (ML) detection rule is that we should decode $\mathbf{Y}$ as that codeword $\hat{\mathbf{X}}$ which maximizes

$$\hat{\mathbf{X}} = \arg \max_{\mathbf{X}\mathbf{X}^H = m\mathbf{I}} P(\mathbf{Y}|\mathbf{X}). \tag{58}$$

Using the matrix inversion lemma [**28**, p. 19], it follows that

$$\hat{\mathbf{X}} = \arg \max_{\mathbf{X}\mathbf{X}^H = m\mathbf{I}} \frac{\exp\left(-\mathrm{Tr}\left\{\left[\mathbf{I}_m - \frac{1}{1+1/(mE_s)}\mathbf{X}^H\mathbf{X}\right]\mathbf{Y}^H\mathbf{Y}\right\}\right)}{\pi^{mM_r}(1+mE_s)^{M_tM_r}} \tag{59}$$

so that $\hat{\mathbf{X}}$ should be chosen to maximize

$$\mathrm{Tr}[\mathbf{Y}\mathbf{X}^H\mathbf{X}\mathbf{Y}^H] \ . \tag{60}$$

This implies that the decoder should project the received signal onto the subspace defined by each of the codewords and declare the codeword with the maximal projection to be the winner.

The probability that a transmitted codeword $\mathbf{X}$ is decoded as the codeword $\hat{\mathbf{X}}$ using a ML decoder is

$$P(\mathbf{X} \to \hat{\mathbf{X}}) = P(\mathrm{Tr}(\mathbf{Y}\hat{\mathbf{X}}^H\hat{\mathbf{X}}\mathbf{Y}^H) > \mathrm{Tr}(\mathbf{Y}\mathbf{X}^H\mathbf{X}\mathbf{Y}^H)|\mathbf{X}).$$

Using a Chernoff bound argument, we find that the pairwise error probability is upper bounded by [**26**]

$$\frac{1}{\det(\mathbf{I}_{M_t} + \frac{\rho^2 m^2}{4(1+\rho m)}[\mathbf{I}_{M_t} - \frac{1}{m^2}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}^H])^{M_r}} \ , \tag{61}$$

where $\rho = \frac{E_s}{N_0}$ is the signal-to-noise ratio (SNR). If the SNR is large, this pairwise error probability behaves like

$$\frac{1}{|\frac{\rho m}{4}[\mathbf{I}_{M_t} - \frac{1}{m^2}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}^H]|_+^{M_r}} = (\frac{\Lambda\rho}{4})^{-M_r\nu},$$

where ν is the rank of $[\mathbf{I}_{M_t} - \frac{1}{m^2}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}]$,

$$\Lambda = \Lambda(\mathbf{X}, \hat{\mathbf{X}}) = |m\mathbf{I}_{M_t} - \frac{1}{m}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}^H|_+^{\frac{1}{\nu}} \ ,$$

and $|\cdot|_+$ denotes the product of the nonzero eigenvalues. Note that

$$\begin{aligned} \det\left(\begin{bmatrix} \mathbf{X} \\ \hat{\mathbf{X}} \end{bmatrix}\begin{bmatrix} \mathbf{X}^H & \hat{\mathbf{X}}^H \end{bmatrix}\right) &= \det\begin{pmatrix} m\mathbf{I} & \mathbf{X}\hat{\mathbf{X}}^H \\ \hat{\mathbf{X}}\mathbf{X}^H & m\mathbf{I} \end{pmatrix} \\ &= \det(m^2\mathbf{I}_{M_t} - \hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}^H) \ , \end{aligned} \tag{62}$$

which shows that $\nu = M_t$ is equivalent to the condition that the rows of $\mathbf{X}, \hat{\mathbf{X}}$ are linearly independent [**29**]. For this to happen we must have $m \geq 2M_t$.

Similarly to the coherent case, a way to compare these codes is by using the notion of diversity order (cf. [**50**]). It follows from (61) that the diversity order of the coding scheme is equal to $M_r\nu$. The maximal diversity order that can be achieved is therefore

M_rM_t. Again, we call codes that achieve this bound *fully diverse* codes. The interpretation in terms of the slope of the error probability with respect to SNR is the same as in the coherent case.

CHAPTER 5

Cyclic Division Algebras

This chapter is dedicated to cyclic algebras in general, and to cyclic division algebras in particular. After having reviewed some well known results, we explain how cyclic algebras provide a tool for space-time coding. It will appear that working with cyclic division algebras is a crucial point, and that deciding whether a cyclic algebra is a division algebra reduces to deciding whether a given element is a norm. This requires a tool from Class Field Theory, namely the Hasse norm symbol. We end this chapter by explaining how it can be computed for our purpose.

1. Cyclic Algebras: known Results

Let L/K be a cyclic extension of degree n, i.e., a Galois extension such that the Galois group $G = \mathrm{Gal}(L/K)$ is cyclic, with generator σ. Denote by K^* (resp. L^*) the non-zero elements of K (resp. L). We choose an element $\gamma \in K^*$ and construct a non-commutative K-algebra, denoted $\mathcal{A} = (L/K, \sigma, \gamma)$, by considering the right L-vector space

$$\mathcal{A} = L \oplus eL \oplus \ldots \oplus e^{n-1}L$$

such that e satisfies

$$e^n = \gamma \text{ and } \lambda e = e\sigma(\lambda) \text{ for all } \lambda \in L.$$

Such an algebra is called *a cyclic algebra.* It is a has dimension $(\mathcal{A} : L) = n$.

It will be very useful for the following to know that cyclic algebras belong to the family of central simple algebras.

THEOREM 1.1. [**42**, p. 316] *The cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ is a central simple algebra over K.*

A central simple K-algebra $\mathcal{A}$ has the property that there exists a field extension E of K which *splits* $\mathcal{A}$. This means that there is an isomorphism of E-algebras

$$h : \mathcal{A} \otimes_K E \cong \mathcal{M}_m(E), \text{ where } (\mathcal{A} : K) = m^2,$$

and $\mathcal{M}_m(E)$ denote the m-dimensional matrices with coefficients in E. We call $(\mathcal{A} : K)$ the *dimension* of $\mathcal{A}$ over K and $\sqrt{(\mathcal{A} : K)} = m$ the *degree* of $\mathcal{A}$.

In the particular case of a cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$, where L/K is a cyclic extension of degree n, the degree of $\mathcal{A}$ is equal to n. Moreover, the field extension L of K splits $\mathcal{A}$ and an isomorphism

$$h : A \otimes_K L \to \mathcal{M}_n(L) \tag{63}$$

can be given explicitly. Since each $x \in \mathcal{A}$ is expressible as

$$x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1},\ x_i \in L \text{ for all } i,$$

it is enough to define $h(x_i \otimes 1)$ and $h(e \otimes 1)$. We have that

$$x_i \otimes 1 \mapsto \begin{pmatrix} x_i & 0 & & 0 \\ 0 & \sigma(x_i) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \sigma^{n-1}(x_i) \end{pmatrix} \text{ for all } i,\ e \otimes 1 \mapsto \begin{pmatrix} 0 & 0 & 0 & & \gamma \\ 1 & 0 & 0 & & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & & \ddots & & \\ 0 & & & 1 & 0 \end{pmatrix}.$$

Thus the matrix of $h(x \otimes 1)$ is easily checked to be

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \ldots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \ldots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \ldots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{64}$$

The above isomorphism h will be the key for using cyclic algebras for coding, together with the notion of *reduced norm.*

Definition 1.1. *Let $x \in \mathcal{A}$. With the above notations, we call the* reduced norm *of x, that we denote by $N(x)$, the determinant* $\det(h(x \otimes 1))$ *of the matrix $h(x \otimes 1)$.*

The reduced norm of a cyclic algebra inherits, by Theorem 1.1, of properties of the reduced norm of a central simple algebra.

Proposition 1.1. [**40**, p. 113] *Let $\mathcal{A}$ be a central simple algebra over K. For all $x \in \mathcal{A}$, the reduced norm $N(x)$ of x belongs to the center K of $\mathcal{A}$.*

Finally, we need a criterion to decide whether a cyclic algebra is a division algebra.

Proposition 1.2. [**38**, p. 279] *Let L/K be a cyclic extension of degree n with Galois group Gal$(L/K) =< \sigma >$. If the order of $\gamma \in K^*$ modulo $N_{L/K}(L^*)$ is n, then the cyclic algebra $(L/K, \sigma, \gamma)$ is a division algebra.*

Remark 1.1. Since $N_{L/K}(L^*) \subset K^*$, we consider the quotient group $K^*/N_{L/K}(L^*)$. Obviously, $N_{L/K}(\gamma) = \gamma^n$, so that the order of γ in the quotient group has to divide n. This simplifies the computation, since in order to check that a cyclic algebra is a division algebra, it is enough to check that γ^k is not a norm for $k \mid n$.

2. Cyclic Algebras: a Tool for Space-Time Coding

Based on the previous section, we now explain how to use cyclic algebras to build space-time block codes (STBCs). This application of cyclic algebras has been first thoroughly studied in [**44**].

Again, let L/K be a cyclic extension of degree n, with Galois group Gal$(L/K) =< \sigma >$, where σ is the generator of the cyclic group. Consider $\mathcal{A} = (L/K, \sigma, \gamma)$ its corresponding cyclic algebra.

Via the isomorphism (63), we associate to an element $x \otimes 1$ of the split algebra $\mathcal{A} \otimes_K L$ a matrix representation, as given in (64). Based on the latter, the following space-time block code is then obtained

$$\mathcal{C}_\infty = \left\{ \begin{pmatrix} x_0 & x_1 & \dots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \dots & \sigma(x_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \dots & \sigma^{n-1}(x_0) \end{pmatrix} \mid x_i \in L,\ i = 0, \dots, n-1 \right\}.$$

Let $\mathbf{X} \in \mathcal{C}_\infty$ be a codeword. With the above notations, $\mathbf{X} = h(x \otimes 1)^T$ for some $x \in \mathcal{A}$, thus $\det(\mathbf{X}) = \det(h(x \otimes 1)^T) = \det(h(x \otimes 1)) = N(x)$.

Remark 2.1. By abuse of language, we say that a codeword $\mathbf{X} \in \mathcal{C}_\infty$ is a matrix representation of an element $x \in \mathcal{A}$, and we call $\det(\mathbf{X})$ the reduced norm of x.

The code $\mathcal{C}_\infty$ is obtained by considering a discrete subset of the base field K as information symbols. Following the terminology of [**44**], we may say that the STBC is *over* K. Since L can be seen as a vector space of dimension n over K, the code matrix entries (belonging to L) are linear combinations of n information symbols:

$$x_\ell = \sum_{k=0}^{n-1} u_{\ell,k}\nu_k,\ \ell = 0,\dots,n-1$$

where $\{\nu_k\}_{k=0}^{n-1}$ is a K-basis of L. There are thus n^2 information symbols $u_{\ell,k} \in K$ encoded into a codeword $\mathbf{X} \in \mathcal{C}_\infty$.

In order to build STBCs with "good" properties, we restrict the codebook to a subset of $\mathcal{C}_\infty$, obtained by restricting the coefficients $x_0,\dots,x_{n-1}$, to be in $\mathcal{I} \subseteq \mathcal{O}_L$, an ideal of the ring of integers of L. We denote by $\mathcal{C}_\mathcal{I}$ this codebook:

(65)

$$\mathcal{C}_\mathcal{I} = \left\{ \begin{pmatrix} x_0 & x_1 & \dots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \dots & \sigma(x_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \dots & \sigma^{n-1}(x_0) \end{pmatrix} \mid x_i \in \mathcal{I} \subseteq \mathcal{O}_L,\ i = 0,\dots,n-1 \right\}$$

Note that in order to guarantee all the coefficients to be in $\mathcal{O}_L$, we need to take $\gamma \in K \cap \mathcal{O}_L = \mathcal{O}_K$. This time, we have n^2 information symbols $u_{\ell,k} \in \mathcal{O}_K$ that are encoded into a codeword $\mathbf{X} \in \mathcal{C}_\mathcal{I}$ by

$$x_\ell = \sum_{k=0}^{n-1} u_{\ell,k}\nu_k,\ \ell = 0,\dots,n-1$$

where $\{\nu_k\}_{k=0}^{n-1}$ is a basis of the ideal $\mathcal{I}$.

Remark 2.2. In the following, we will focus on information symbols carved from two different types of constellations: the QAM constellations and the HEX constellations. Since they can be seen as subsets of $\mathbb{Z}[i]$ resp. $\mathbb{Z}[\zeta_3]$ (where ζ_3 is a primitive third root of unity), we will consider number field extensions L/K, where K is either $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$.

The code $\mathcal{C}_\mathcal{I}$ is obviously linear and the information symbols are dispersed in linear combinations over space and time. Such codes are refered to as *Linear Dispersion Space-Time Block Codes* (LD-STBCs) [**24**]. The LD-STBCs built over cyclic algebras have the following two key advantages.

(1) We have a criterion to decide whether the STBC $\mathcal{C}_\infty$ satisfies the rank criterion [**50**]. Namely, when the cyclic algebra is a division algebra, all its elements are invertible hence the codeword matrices have non zero determinant. Proposition

1.2, as already noticed in [**44**], gives a sufficient condition for a cyclic algebra to be a division algebra.

(2) Thanks to linearity, the *minimum determinant* of the infinite code $\mathcal{C}_\infty$ is

$$\delta_{\min}(\mathcal{C}_\infty) = \min_{\mathbf{X}_1,\mathbf{X}_2\in\mathcal{C}_\infty,\mathbf{X}_1\neq\mathbf{X}_2} |\det(\mathbf{X}_1-\mathbf{X}_2)|^2 = \min_{\mathbf{X}\in\mathcal{C}_\infty,\mathbf{X}\neq 0} |\det(\mathbf{X})|^2.$$

Since the rank criterion is fullfilled by considering a division algebra, much of the work will be on deriving a lower bound for the minimum determinant. This is the purpose of the next two sections.

2.1. Discreteness of the determinants. The goal of this section is to investigate the determinant properties of STBCs built over a cyclic algebra $\mathcal{A} = (L/K,\sigma,\gamma)$. We prove that if we restrict the coefficients of the codes to be in $\mathcal{O}_L$, under the assumption that $\gamma \in \mathcal{O}_K$, the determinants are in $\mathcal{O}_K$. When $\mathcal{O}_K = \mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, they are then discrete.

Let us begin with the simplest example.

Example 2.1. Consider a cyclic algebra $\mathcal{A} = (L/K,\sigma,\gamma)$ of degree 2 with $\gamma\in\mathcal{O}_K$. Let $x = x_0 + ex_1$, $x_0, x_1 \in \mathcal{O}_L$, which can be written as

$$\mathbf{X} = \begin{pmatrix} x_0 & x_1 \\ \gamma\sigma(x_1) & \sigma(x_0) \end{pmatrix}.$$

Since x_0 and x_1 are chosen to be in $\mathcal{O}_L$, they are by definition elements of L that satisfy a linear equation with coefficients in $\mathbb{Z}$. Thus $\sigma(x_0)$ and $\sigma(x_1)$ also belong to $\mathcal{O}_L$. The reduced norm of x is given by the determinant of $\mathbf{X}$:

$$\det(\mathbf{X}) = x_0\sigma(x_0) - \gamma x_1\sigma(x_1).$$

Recalling that $\gamma\in\mathcal{O}_K$, $\det(\mathbf{X})\in\mathcal{O}_L$. By Proposition 1.1, $\det(\mathbf{X})\in K$, so that $\det(\mathbf{X})\in K\cap\mathcal{O}_L = \mathcal{O}_K$.

In this example, there are two other ways to obtain the same result. First, notice that $\det(\mathbf{X}) = N_{L/K}(x_0) + \gamma N_{L/K}(x_1)$, as already done in [**4, 5**]. Since $x_0, x_1\in\mathcal{O}_L$, their norms belong to $\mathcal{O}_K$, and we deduce that $\det(\mathbf{X})\in\mathcal{O}_K$. Unfortunately, such a nice expression holds only for dimension 2. Second, it is clear that $\det(\mathbf{X})$ is invariant under the action of σ, that is $\sigma(\det(\mathbf{X})) = \det(\mathbf{X})$. This implies that $\det(\mathbf{X})$ is in K, more precisely in $K\cap\mathcal{O}_L = \mathcal{O}_K$.

Example 2.2. Consider now a cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree 3 with $\gamma \in \mathcal{O}_K$. Let $x = x_0 + ex_1 + e^2x_2$, which can be represented as

$$\mathbf{X} = \begin{pmatrix} x_0 & x_1 & x_2 \\ \gamma\sigma(x_2) & \sigma(x_0) & \sigma(x_1) \\ \gamma\sigma^2(x_1) & \gamma\sigma^2(x_2) & \sigma^2(x_0) \end{pmatrix}.$$

Again the norm of x is given by the determinant of $\mathbf{X}$:

$$\det(\mathbf{X}) = N(x_0) + \gamma N(x_1) + \gamma^2 N(x_2) - \gamma \mathrm{Tr}[x_0\sigma(x_1)\sigma^2(x_2)].$$

Obviously the norm of the algebra cannot be related to the norm of the number field, as in the previous example, though an expression in terms of both norms and traces is enough to conclude that $\det(\mathbf{X}) \in \mathcal{O}_K$.

An explicit computation of the determinant in higher dimensions becomes soon intractable. However, these two examples illustrate the following general result. Since the reduced norm of $\mathcal{A}$ belongs to K (Proposition 1.1), restricting the coefficients $x_0, \ldots, x_n$ to be in $\mathcal{O}_L$ results in the reduced norm to be in $\mathcal{O}_K$. More precisely:

Proposition 2.1. *Let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic algebra with $\gamma \in \mathcal{O}_K$. Denote its basis by $\{1, e, \ldots, e^{n-1}\}$. Let $x \in \mathcal{A}$ be of the form*

$$x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}$$

where $x_k \in \mathcal{O}_L$, $k = 0, \ldots, n-1$. Then, the reduced norm of x belongs to $\mathcal{O}_K$.

Proof. Recall from Definition 1.1 and Remark 2.1 that the reduced norm of x is the determinant of its matrix representation. Since $x_i \in \mathcal{O}_L$ implies $\sigma(x_i) \in \mathcal{O}_L$ for all i and $\gamma \in \mathcal{O}_K$ by hypothesis, all coefficients of the matrix representation belong to $\mathcal{O}_L$, hence so does its determinant. By Proposition 1.1, the reduced norm of x belongs to K, so it belongs to $\mathcal{O}_L \cap K = \mathcal{O}_K$. □

Recall (Remark 2.2) that we are interested in having $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$ as base field. In these cases, we get from Proposition 2.1 that

$$\det(\mathbf{X}) \in \mathbb{Z}[i] \text{ (resp. } \in \mathbb{Z}[\zeta_3]), \text{ for } \mathbf{X} \in \mathcal{C}_{\mathcal{I}}.$$

We thus have discrete determinants.

2.2. The minimum determinant. We discuss now the value of the minimum determinant of the code $\mathcal{C}_{\mathcal{I}}$ in the case where $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$. Recall that

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) = \min_{\mathbf{0}\neq\mathbf{X}\in\mathcal{C}_{\mathcal{I}}} |\det(\mathbf{X})|^2.$$

We show that if $\mathcal{I}$ is principal, then $\delta_{\min}(\mathcal{C}_{\mathcal{I}})$ is easily computed. Otherwise, we give a lower bound on it.

Proposition 2.2. *Let $\mathcal{C}_{\mathcal{I}}$ be a STB code built over the cyclic division algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n where $\gamma \in \mathcal{O}_K$. Let $\mathcal{I} = (\alpha)\mathcal{O}_L$ be a principal ideal of $\mathcal{O}_L$. Then*

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) = N_{L/\mathbb{Q}}(\alpha).$$

Proof. For all $x \in \mathcal{I}$, we have $x = \alpha y$ for some $y \in \mathcal{O}_L$. Thus codewords of $\mathcal{C}_{\mathcal{I}}$ are of the form

$$\mathbf{X} = \begin{bmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \sigma(\alpha) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \sigma^{n-1}(\alpha) \end{bmatrix} \cdot \begin{bmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ \gamma\sigma(y_{n-1}) & \sigma(y_0) & \cdots & \sigma(y_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(y_1) & \gamma\sigma^{n-1}(y_2) & \cdots & \sigma^{n-1}(y_0) \end{bmatrix} \tag{66}$$

where $y_i \in \mathcal{O}_L,\ i = 0, \ldots, n-1$. The determinant of the second matrix is in $\mathcal{O}_K = \mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, so that its square modulus is at least 1. The minimum is achieved by taking $y_0 = 0$ and $y_1 = \ldots = y_{n-1} = 0$ (the corresponding codeword is $x_0 = 1$ and $x_k = 0$ for $k = 1 \ldots n-1$, that is there is a single information symbol $u_{00} = 1$ and all the remaining $n^2 - 1$ equal to 0). We easily deduce that

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) = \min_{\mathbf{0}\neq\mathbf{X}\in\mathcal{C}_{\mathcal{I}}} |\det(\mathbf{X})|^2 = |N_{L/K}(\alpha)|^2 = N_{L/\mathbb{Q}}(\alpha), \tag{67}$$

where last equality holds for $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, since $|x|^2 = N_{K/\mathbb{Q}}(x)$, for $x \in K$. □

We consider now the more general case, where we make no assumption on whether $\mathcal{I}$ is principal. We have the following result.

Proposition 2.3. *Let $\mathcal{C}_{\mathcal{I}}$ be a STB code built over the cyclic division algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n where $\gamma \in \mathcal{O}_K$. Then*

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) \in N(\mathcal{I})\mathbb{Z},$$

where $N(\mathcal{I})$ denotes the norm of $\mathcal{I}$.

Proof. Recall first that

$$\det(\mathbf{X}) = \sum_{s \in S_n} \mathrm{sgn}(s) \prod_{i=1}^{n} (\mathbf{X})_{i,s(i)},$$

where S_n is the group of permutations of n elements. Denote by $\mathcal{I}^\sigma$ the action of the Galois group on $\mathcal{I}$. Since $(\mathbf{X})_{i,s(i)} \in \mathcal{I}^{\sigma^i}$ for all i, we get [**17**, p. 118]

$$\det(\mathbf{X}) \in \prod_{\sigma \in \mathrm{Gal}(L/K)} \mathcal{I}^\sigma = \mathcal{N}_{L/K}(\mathcal{I})\mathcal{O}_L,$$

where $\mathcal{N}_{L/K}(\mathcal{I})$ stands for an ideal of $\mathcal{O}_K$ called the relative norm of the ideal $\mathcal{I}$. By Proposition 2.1, we deduce

$$\det(\mathbf{X}) \in \mathcal{O}_K \cap \mathcal{N}_{L/K}(\mathcal{I})\mathcal{O}_L = \mathcal{N}_{L/K}(\mathcal{I}).$$

Thus $|\det(\mathbf{X})|^2 \in \mathcal{N}_{K/\mathbb{Q}}(\mathcal{N}_{L/K}(\mathcal{I}))$. We conclude using the transitivity of the norm [**17**, p. 99]

$$\min_{\mathbf{X} \in \mathcal{C}_\mathcal{I}, \mathbf{X} \neq 0} |\det(\mathbf{X})|^2 \in \mathcal{N}_{L/\mathbb{Q}}(\mathcal{I}) = N(\mathcal{I})\mathbb{Z}.$$

□

Bounds on $\delta_{\min}(\mathcal{C}_\mathcal{I})$ are easily derived from the above proposition.

Corollary 2.1. *Let $\mathcal{C}_\mathcal{I}$ be a perfect code built over the cyclic division algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n. Then*

$$\min_{x \in \mathcal{I}} N_{L/\mathbb{Q}}(x) \geq \delta_{\min}(\mathcal{C}_\mathcal{I}) \geq N(\mathcal{I}).$$

Proof. The lower bound is immediate from Proposition 2.3. Taking $x_0 \neq 0 \in \mathcal{I}$ and $x_2 = \ldots = x_n = 0$ yields the upper bound. □

The result obtained in Proposition 2.2 for the principal case alternatively follows:

Corollary 2.2. *If $\mathcal{I} = (\alpha)\mathcal{O}_L$ is principal, then*

$$\delta_{\min}(\mathcal{C}_\mathcal{I}) = N_{L/\mathbb{Q}}(\alpha).$$

Proof. If $\mathcal{I}$ is principal, the lower and upper bounds in Corollary 2.1 coincide. □

3. The Hasse Norm Symbol

In this section, we introduce *the Hasse Norm Symbol.* It is a tool derived from Class Field Theory, that allows to compute whether a given element is a norm. We will need it in the next chapter. Our exposition is based on [**22**].

In the following, we consider extensions of number fields L/K that we assume abelian. Denote by L_ν the completion of L with respect to the valuation ν. We denote the *embedding* of L into L_ν by i_ν.

Definition 3.1. [**22**, p. 105] *Let L/K be an abelian extension of number fields with Galois group $Gal(L/K)$. The map*

$$\left(\frac{\bullet\ ,\ L/K}{\nu}\right) : \begin{array}{ccc} L^* & \to & Gal(L/K) \\ x & \mapsto & \left(\frac{i_\nu(x),\ L/K}{\nu}\right) \end{array}$$

is called the Hasse norm symbol*.*

The main property of this symbol is that it gives a way to compute whether an element is a local norm [**22**, p. 106-107].

Theorem 3.1. *We have $\left(\frac{x,\ L/K}{\nu}\right) = 1$ if and only if x is a local norm at ν for L/K.*

In order to compute the Hasse norm symbol, we need to know some of its properties. Let us begin with a property of linearity.

Theorem 3.2. *We have*

$$\left(\frac{xy, L/K}{\nu}\right) = \left(\frac{x, L/K}{\nu}\right)\left(\frac{y, L/K}{\nu}\right).$$

We then know how the symbol behaves at unramified places [**22**, p. 106].

Theorem 3.3. *If ν is unramified in L/K, then we have, for all $x \in K^*$:*

$$\left(\frac{x, L/K}{\nu}\right) = \left(\frac{L/K}{\nu}\right)^{v(x)},$$

where $\left(\frac{L/K}{\nu}\right)$ denotes the Frobenius of ν for L/K, and $v(x)$ denotes the valuation of x.

Corollary 3.1. *At an unramified place, a unit is always a norm.*

Proof. It is straightforward since the valuation of a unit is 0. □

A remarkable property is the *product formula* [**22**, p. 113].

Theorem 3.4. *Let L/K be a finite extension. For any $x \in K^*$ we have:*

$$\prod_{\nu} \left(\frac{x, L/K}{\nu}\right) = 1,$$

where the product is defined over all places ν.

By Corollary 3.1, we know that a unit is always a norm locally if the place is unramified. Since we will be interested in showing that a unit γ is not a norm (see next chapter), we will look for a contradiction at a ramified place. We explain briefly how. The idea is to start from the product formula, and to simplify all the terms except two in the product over all primes, so that we get a product of two terms equal to 1:

$$\left(\frac{\gamma, L/K}{\nu}\right)\left(\frac{x, L/K}{\nu'}\right) = 1, \ x \in K^*.$$

Hopefully, one of the two terms left will involve γ, the other will be shown to be different from 1, so that since the product is 1, we will deduce that the term involving γ is different from 1, thus γ is not a norm. In order to make it easier to simplify the product formula, we introduce an element $y \in L$ such that $y\gamma$ is a unit locally at ramified primes, and we compute the product formula

$$\prod_{\nu} \left(\frac{y\gamma, L/K}{\nu}\right) = 1.$$

CHAPTER 6

Codes for coherent MIMO Channels

Thanks to the tools developped in the previous chapter, we are now ready to concentrate on the space-time block codes construction itself. In this work, we consider square linear dispersion STBCs with full-rate.

As a preliminary, we refine the code design criteria introduced in Chapter 4. This gives rise to the notion of *perfect codes*. In short, we define *perfect* STBCs to have full rate and full diversity, uniform average transmitted energy per antenna, a non-vanishing minimum determinant for increasing spectral efficiency and good shaping. The so-called Golden code [**5**] is the first example of 2×2 perfect codes. In Section 2, we extend it to an infinite family of codes for two transmit antennas. We then give a scheme to generalize the 2×2 constructions to higher dimensions. It allows to build perfect STBCs in dimensions 3, 4 and 6. We conclude by showing that these dimensions are the only ones where perfect codes exist.

1. Code Design Criteria for "Perfect Codes"

As recalled in Chapter 4, the most important code design parameter for coherent MIMO channels is the diversity, which is ensured to be maximal when the rank criterion is satisfied. In previous work such as [**44, 14, 18**], the emphasis is then on having a non-zero minimum determinant.

Here we consider square $M \times M$ LD-STBCs ($M = M_t = M_r$) using cyclic division algebras, so that the maximal diversity is already guaranteed. We thus focus on further requirements, namely we want a lower bound on the *minimum determinant*, and we ask for a *shaping constraint* on the signal constellations, that we consider to be either QAM or HEX symbols.

- **Minimum determinant.** When the minimum determinant is dependent on the spectral efficiency, though it is non-zero, it vanishes when the constellation size increases. This means that the set of determinants of the infinite code is a dense subset of $\mathbb{C}$. We impose here that the minimum determinant of the

STBC is lower-bounded by a constant. Namely, the infinite code $\mathcal{C}_\infty$ must have a non zero minimum determinant $\delta_{\min}(\mathcal{C}_\infty)$ which corresponds to a non vanishing behaviour of this determinant when the spectral efficiency increases.

- **Shaping.** In order to optimize the energy efficiency of the codes, we introduce a shaping constraint on the signal constellation. It is enough to introduce this shaping constraint on each layer as the codes considered all use the layered structure of [**15**].

  Let M be the number of transmit antennas. Since QAM and HEX symbols are finite subsets of $\mathbb{Z}[i]$, resp. $\mathbb{Z}[\zeta_3]$, we need to construct for each layer a $\mathbb{Z}[i]$–lattice $R\mathbb{Z}[i]^M$ (resp. a $\mathbb{Z}[\zeta_3]$–lattice $R\mathbb{Z}[\zeta_3]^M$), where R is a complex unitary matrix ($RR^H = I$), so that there is no shaping loss in the signal constellation. When working over $\mathbb{Z}[\zeta_3]$, the Hermitian transposition uses the conjugation in $\mathbb{Z}[\zeta_3]$, that transforms ζ_3 into ζ_3^2. Note that the matrix R may be viewed as a precoding matrix applied to the information symbols.

  Finally, the $2M^2$–dimensional real lattice generated by the vectorized codewords where real an imaginary components are separated is either $\mathbb{Z}^{2M^2}$ or $A_2^{M^2}$, where A_2 is the hexagonal lattice [**11**], with generator matrix

$$\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}.$$

Finally, it was already noticed in [**44**] that uniform average transmitted energy per antenna in all m time slots is required.

This leads to the definition of a *perfect* STBC code.

Definition 1.1. *A square $M \times M$ STBC is called a* perfect *code if and only if:*

- *it is a full rate (in the sense of Definition 1.2 of Chapter 4) linear dispersion code using M^2 information symbols, either QAM or HEX.*
- *the minimum determinant of the infinite code is non zero (so that in particular the rank criterion is satisfied).*
- *the $2M^2$–dimensional real lattice generated by the vectorized codewords is either $\mathbb{Z}^{2M^2}$ or $A_2^{M^2}$.*
- *it induces uniform average transmitted energy per antenna in all m time slots, i.e., all the coded symbols in the code matrix have the same average energy.*

The 2×2 STBC presented in [**5**] is the first example of perfect STBC. In the next section, we generalize its construction to an infinite family of codes for 2 transmit antennas.

2. An infinite Family of Codes for two Antennas

In this section, we explain how to construct an infinite family of perfect codes for two transmit antennas.

Let p be a prime. Let $K/\mathbb{Q}(i)$ be a relative extension of degree 2 of $\mathbb{Q}(i)$ of the form $K = \mathbb{Q}(i, \sqrt{p})$. We can represent K as a vector space over $\mathbb{Q}(i)$:

$$K = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}(i)\}.$$

Its Galois group $\mathrm{Gal}(K/\mathbb{Q}(i)) = \langle \sigma \rangle$ is generated by $\sigma : \sqrt{p} \mapsto -\sqrt{p}$. Let $\mathcal{A} = (K/\mathbb{Q}(i), \sigma, \gamma)$ be its corresponding cyclic algebra.

We prove that when $p \equiv 5 \pmod 8$, $\gamma = i$, and using a suitable ideal $\mathcal{I}$, we obtain perfect codes as defined in Section 1.

2.1. The lattice $\mathbb{Z}[i]^2$. We first search for the ideal $\mathcal{I}$ giving the rotated $\mathbb{Z}[i]^2$ lattice. Since $\mathbb{Z}[i]^2$ is the only *unimodular* $\mathbb{Z}[i]$–lattice in dimension 2 [**43**], it is enough to find an ideal $\mathcal{I}$ such that the complex lattice $\Lambda^c(\mathcal{I})$ is unimodular. By definition, a unimodular lattice coincides with its *dual* defined as follows.

Definition 2.1. *The dual lattice of the integral lattice (L, b) is defined by*

$$L^{\#} = \{x \in L_{\mathbb{Q}} \mid b(x, y) \in \mathbb{Z} \ \forall \ y \in L\}.$$

Let $\Lambda^c(\mathcal{I})$ be a complex algebraic lattice with basis $\{\mathbf{v}_1, \mathbf{v}_2\} = \{\sigma(\nu_1), \sigma(\nu_2)\}$, following the notation of Section 5 (Chapter 2). Translating the above definition, we get

Definition 2.2. *The dual lattice of $\Lambda^c(\mathcal{I}) = (\mathcal{I}, b)$ is defined by*

$$\Lambda^c(\mathcal{I})^{\#} = \{\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2, a_1, a_2 \in \mathbb{Q}(i) | \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}[i], \forall \mathbf{y} \in \Lambda^c(\mathcal{I})\}$$

where the scalar product between the two vectors can be related to the trace of the corresponding algebraic numbers as

$$\langle \mathbf{x}, \mathbf{y} \rangle = Tr_{L/\mathbb{Q}(i)}(x\overline{y}).$$

The dual of a complex algebraic lattice can be computed explicitly.

LEMMA 2.1. *We have* $\Lambda^c(\mathcal{I})^\# = \Lambda^c\left(\mathcal{I}^\#\right)$ *with*

$$\mathcal{I}^\# = \overline{\mathcal{I}^{-1}\mathcal{D}^{-1}_{L/\mathbb{Q}(i)}}$$

where $\mathcal{D}^{-1}_{L/\mathbb{Q}(i)}$ *denotes the codifferent* [**48**, p. 44],[**3**].

PROOF. Let $x \in \overline{\mathcal{I}^{-1}\mathcal{D}^{-1}_{L/\mathbb{Q}(i)}}$. For all $y \in \mathcal{I}$, we have to show that $\mathrm{Tr}_{L/\mathbb{Q}(i)}(x\overline{y}) \in \mathbb{Z}[i]$. Since $x = \overline{uv}$, with $u \in \mathcal{I}^{-1}$ and $v \in \mathcal{D}^{-1}_{L/\mathbb{Q}(i)}$, we have $x\overline{y} = \overline{uyv}$, with $uy \in \mathcal{O}_L$. The result follows now from the definition of $\mathcal{D}^{-1}_{L/\mathbb{Q}(i)}$. □

Let $L = \mathbb{Q}(i, \sqrt{p})$, with $p \equiv 1 \pmod 4$. The factorization of p in $\mathcal{O}_L$ is

$$(p)\mathcal{O}_L = \mathfrak{P}^2\overline{\mathfrak{P}}^2 \tag{68}$$

where $\mathfrak{P}$, $\overline{\mathfrak{P}}$ are prime conjugate ideals.

PROPOSITION 2.1. *The* $\mathbb{Z}[i]$*–lattice* $\frac{1}{\sqrt{p}}\Lambda^c(\mathfrak{P})$ *is unimodular*

PROOF. Note first that $\mathcal{D}_{L/\mathbb{Q}(i)} = \mathcal{D}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}} = (\sqrt{p})\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = (\sqrt{p})$. Using Lemma 2.1 and (68), we compute the dual of $\mathfrak{P}$,

$$\mathfrak{P}^\# = \overline{\mathfrak{P}^{-1}}(\sqrt{p})^{-1} = \frac{1}{p}\mathfrak{P}.$$

Now the dual lattice is

$$\left(\frac{1}{\sqrt{p}}\Lambda^c(\mathfrak{P})\right)^\# = \sqrt{p}\left(\Lambda^c(\mathfrak{P})^\#\right) = \frac{1}{\sqrt{p}}\Lambda^c(\mathfrak{P})$$

which concludes the proof. □

2.2. A norm condition. We need to prove that the algebra $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ is a division algebra. By Proposition 1.2, it is enough to show that i is not a norm in $L/\mathbb{Q}(i)$.

We first recall the characterization of a square in finite fields. Let p be a prime and denote by $\mathbb{F}_p$ the finite field of p elements.

PROPOSITION 2.2. *Let* $x \in \mathbb{F}_p^*$. *We have*

$$x \text{ is a square} \Longleftrightarrow x^{\frac{p-1}{2}} = 1.$$

PROOF. Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. Let $y \in \overline{\mathbb{F}_p}$ such that $y^2 = x$. We have

$$y \in \mathbb{F}_p^* \iff y^{p-1} = 1 \iff x^{(p-1)/2} = 1.$$

□

COROLLARY 2.1. *If $p \equiv 1$ (mod4) , -1 is a square in $\mathbb{F}_p$.*

Let us come back to our case where p is a prime such that $p \equiv 5 \pmod 8$ and $L = \mathbb{Q}(i, \sqrt{p})$ is a relative extension of $\mathbb{Q}(i)$. Let $x \in L$, $x = a + b\sqrt{p}$, $a, b \in \mathbb{Q}(i)$. Its relative norm is

$$N_{L/\mathbb{Q}(i)}(x) = (a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - pb^2. \tag{69}$$

Our goal is to show that the equation $N_{L/\mathbb{Q}(i)}(x) = i$ has no solution. We prove that this equation has no solution in the field of p-adic numbers $\mathbb{Q}_p$, and thus, no solution for $x \in L$. Let $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | \nu_p(x) \geq 0\}$ be the valuation ring of $\mathbb{Q}_p$, where $\nu_p(x)$ denotes the valuation of x in p. There are embeddings of $\mathbb{Q}(i)$ into $\mathbb{Q}_p$ if $X^2 + 1$, the minimal polynomial of i, has roots in $\mathbb{Z}_p$. Using Hensel's Lemma [**21**, p.75], it is enough to check that -1 is a square in $\mathbb{F}_p$. By assumption, $p \equiv 5 \pmod 8$, thus $p \equiv 1 \,(\mathrm{mod}\, 4)$, then, by Corollary 2.1, -1 is a square in $\mathbb{F}_p$.

PROPOSITION 2.3. *The unit $i \in \mathbb{Z}[i]$ is not a relative norm, i.e., there is no $x \in L$ such that $N_{L/\mathbb{Q}(i)}(x) = i$ where $L = \mathbb{Q}(\sqrt{p}, i)$ with $p \equiv 5$ (mod 8).*

PROOF. This is equivalent, by (69), to prove that

$$a^2 - pb^2 = i, \;\; a, b \in \mathbb{Q}(i) \tag{70}$$

has no solution.
Using the embedding of $\mathbb{Q}(i)$ into $\mathbb{Q}_p$, this equation can be seen in $\mathbb{Q}_p$ as follows:

$$a^2 - pb^2 = y + px, \;\; a, b \in \mathbb{Q}_p, \;\; x, y \in \mathbb{Z}_p, \tag{71}$$

where $y^2 = -1$. If there is a solution to (70), then this solution still holds in $\mathbb{Q}_p$. Thus proving that no solution of (71) exists would conclude the proof. We first show that in (71), a and b are in fact in $\mathbb{Z}_p$. In terms of valuation, we have

$$\nu_p(a^2 - pb^2) = \nu_p(y + px).$$

Since $x \in \mathbb{Z}_p$, the right term yields $\nu_p(y + px) \geq \inf\{\nu_p(y), \nu_p(x) + 1\} = 0$, and we have equality since the valuations are distinct. Now the left term becomes $0 = \nu_p(a^2 - pb^2) = \inf\{2\nu_p(a), 2\nu_p(b) + 1\}$. The only possible case is $\nu_p(a) = 0$, implying $a \in \mathbb{Z}_p$ and consequently $b \in \mathbb{Z}_p$.

We conclude showing that

$$a^2 - pb^2 = y + px, \ \ a, b, x, y \in \mathbb{Z}_p \tag{72}$$

has no solution. Reducing (mod $p\mathbb{Z}_p$), we see that y has to be a square in $\mathbb{F}_p$. Since $y^2 = -1$, $y^{(p-1)/2} = (-1)^{(p-1)/4} = -1$ by choice of $p \equiv 5 \pmod 8$. By Proposition 2.2, y is not a square, which is a contradiction. □

Remark 2.1. This result does not hold for $p \equiv 1 \pmod 8$ since, in this case, $y^{(p-1)/2} = (-1)^{(p-1)/4} = 1$ and we get no contradiction. The fact that this proof does not hold anymore is not enough to restrict ourselves to the case $p \equiv 5 \pmod 8$. We thus give a counterexample.

Example 2.1. Consider $L = \mathbb{Q}\left(\sqrt{17}, i\right)$, and $x = \frac{3(i-1)}{4} - \frac{(i-1)\sqrt{17}}{4}$. It is easy to check that $N_{L/\mathbb{Q}(i)}(x) = i$.

2.3. The minimum determinant. We first show that the ideal $\mathfrak{P}$ in (68) is principal for all $p \equiv 1 \,(\mathrm{mod}\, 4)$. Since $N(\mathfrak{P}) = p$, it is enough to show that there exists an element $\alpha \in \mathfrak{P}$ with absolute norm $N_{L/\mathbb{Q}}(\alpha) = p$. Using the fact that $p = u^2 + v^2$ for some $u, v \in \mathbb{Z}$ [**41**], the element $\alpha = \sqrt{u + iv}$ satisfies the condition and generates $\mathfrak{P}$ (resp. $\overline{\alpha} = \sqrt{u - iv}$ generates $\overline{\mathfrak{P}}$). Now, take $\theta = \frac{1+\sqrt{p}}{2}$ and let $\overline{\theta} = \frac{1-\sqrt{p}}{2}$ be its conjugate. We have $\mathcal{O}_L = \mathbb{Z}[\theta]$. The codewords have the form

$$\mathbf{X} = \frac{1}{\sqrt{p}} \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ i\bar{\alpha}(c + d\bar{\theta}) & \bar{\alpha}(a + b\bar{\theta}) \end{bmatrix}$$

with $a, b, c, d \in \mathbb{Z}[i]$. Each layer of the STBC can be encoded by multiplying the vectors $(a, b)^T$ and $(c, d)^T$ by the matrix

$$\begin{bmatrix} \alpha & \alpha\theta \\ \overline{\alpha} & \overline{\alpha\theta} \end{bmatrix},$$

which generates the $\mathbb{Z}[i]^2$–lattice. We observe that this lattice generator matrix may require basis reduction in order to be unitary.

Determinants are given by

$$\det(\mathbf{X}) \ \ = \tfrac{1}{p} N_{L/\mathbb{Q}(i)}(\alpha) \left(N_{L/\mathbb{Q}(i)}(a + b\theta) - i N_{L/\mathbb{Q}(i)}(c + d\theta) \right). \tag{73}$$

As the second term in (73) only takes values in $\mathbb{Z}[i]$ and its minimum modulus is equal to 1 (take for example $a = 1$ and $b = c = d = 0$), we conclude that

$$\delta_{\min}(\mathcal{C}_\infty) = \frac{1}{p^2}|N_{L/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{p^2}|u + iv|^2 = \frac{1}{p}. \tag{74}$$

Remark 2.2. As $p \equiv 5 \pmod 8$, the largest minimum determinant is given by $p = 5$ corresponding to the Golden code [**5**].

3. Space-Time Codes in higher Dimensions

We are now interested in generalizing perfect codes in higher dimensions.

In this process, the choice of γ in building the cyclic algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ is critical. It determines whether $\mathcal{A}$ is a division algebra and is furthermore constrained by the requirement that $|\gamma| = 1$, so that the average transmitted energy by each antenna in all time slots is equalized. In [**44**, Proposition 12], Sethuraman *et al.* have chosen the element γ to be transcendental, with $|\gamma| = 1$. Hence, they work in the cyclic division algebra $(L(\gamma)/K(\gamma), \sigma, \gamma)$. This is where our approach completely differs. Perfect codes require a non-vanishing minimum determinant. In order to fullfill that condition, we know by Proposition 2.1 that γ has to be in $\mathcal{O}_K$.

Putting together all the constraints to build perfect codes, we obtain the following construction scheme:

(1) We consider QAM or HEX symbols with arbitrary spectral efficiency as information symbols. Since these constellations can be seen as finite subsets of $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\zeta_3]$), we take as base field $K = \mathbb{Q}(i)$ (resp. $K = \mathbb{Q}(\zeta_3)$).

(2) Let M be the number of transmit antennas. We take a cyclic extension L/K of degree $n = M$ with Galois group $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ and build the corresponding cyclic algebra:

$$\mathcal{A} = (L/K, \sigma, \gamma).$$

We choose γ such that $|\gamma| = 1$ in order to satisfy the constraint on the uniform average transmitted energy per antenna.

(3) In order to obtain the non-vanishing determinants, we choose $\gamma \in \mathbb{Z}[i]$, or $\gamma \in \mathbb{Z}[\zeta_3]$ (see Section 2.1 of Chapter 5). Adding the previous constraint $|\gamma| = 1$, we are limited to $\gamma \in \{1, i, -1, -i\} \subset \mathbb{Z}[i]$ or $\gamma \in \{1, \zeta_3, \zeta_3^2, -1, -\zeta_3, \zeta_3^2\} \subset \mathbb{Z}[\zeta_3]$, respectively.

(4) Among all elements of $\mathcal{A}$, we consider those of the form $x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1}$, where $x_i \in \mathcal{I}$, an ideal of $\mathcal{O}_L$. We know by by Proposition 2.1 of Chapter 5 that this guarantees a discrete minimum determinant. Recall that the codebook is given by

(75)
$$\mathcal{C}_\mathcal{I} = \left\{ \begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & \ldots & \sigma(x_{n-2}) \\ \vdots & & & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \mid x_i \in \mathcal{I} \subseteq \mathcal{O}_L,\ i = 0, \ldots, n-1 \right\}.$$

The n^2 information symbols $u_{\ell,k} \in \mathcal{O}_K$ are encoded into a codeword $\mathbf{X} \in \mathcal{C}_\mathcal{I}$ by

$$x_\ell = \sum_{k=0}^{n-1} u_{\ell,k}\nu_k,\ \ \ell = 0, \ldots, n-1$$

where $\{\nu_k\}_{k=0}^{n-1}$ is a basis of the ideal $\mathcal{I}$.

(5) We choose an ideal $\mathcal{I}$ so that the signal constellation on each layer is a finite subset of the rotated versions of the lattices $\mathbb{Z}[i]^n$ or $\mathbb{Z}[\zeta_3]^n$.

(6) We show that $\mathcal{A} = (L/K, \sigma, \gamma)$ is a division algebra by selecting an appropriate field extension L, which reduces to show that $\gamma, \ldots, \gamma^{n-1}$ are not a norm in L^*.

The last point to explain is how to choose the ideal $\mathcal{I}$ so as to get rotated versions of the lattices $\mathbb{Z}[i]^n$ or $\mathbb{Z}[\zeta_3]^n$.

3.1. Construction of the $\mathbb{Z}[i]^n$ and $\mathbb{Z}[\zeta_3]^n$ lattices. In our approach, the cubic shaping constraint requires the construction of rotated versions of $\mathbb{Z}[i]^n$ and $\mathbb{Z}[\zeta_3]^n$ lattices. These can be obtained as complex algebraic lattices (see Section 5 of Chap. 2).

Let L be a relative Galois extension of $K = \mathbb{Q}(i)$ (resp. $K = \mathbb{Q}(\zeta_3)$) of degree n, with $\mathcal{O}_L$ its ring of integers. In the following, we focus on the case where L is the compositum of K and a totally real Galois number field $\mathbb{Q}(\theta)$ of degree n with coprime discriminant, that is $(d_K, d_{\mathbb{Q}(\theta)}) = 1$. We write the compositum as $L = K\mathbb{Q}(\theta)$ (see Fig. 1). This assumption has the convenient consequence that [**48**, p. 48]

$$d_L = d_{\mathbb{Q}(\theta)}^2 d_K^n, \tag{76}$$

where $d_K = -4$ for $K = \mathbb{Q}(i)$ and $d_K = -3$ for $K = \mathbb{Q}(\zeta_3)$. Denote by $\{\sigma_k\}_{k=1}^n$ the Galois group $\mathrm{Gal}(L/K)$.

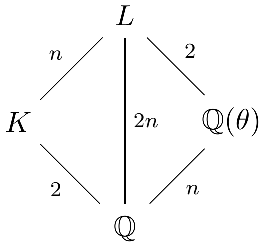

FIGURE 1. The compositum of a totally real field $\mathbb{Q}(\theta)$ and $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$ with coprime discriminants: relative degrees are shown on the branches.

DEFINITION 3.1. *We denote by* $\Lambda^c(\mathcal{I})$ *the* complex algebraic lattice *corresponding to an ideal* $\mathcal{I} \subseteq \mathcal{O}_L$ *obtained by the complex embedding* σ *of* L *into* $\mathbb{C}^n$ *defined as*

$$\begin{array}{rll} \sigma: & L & \to \mathbb{C}^n \\ & x & \mapsto \sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)). \end{array}$$

The basis of $\Lambda^c(\mathcal{I})$ is obtained by embedding the basis $\{\nu_k\}_{k=1}^n$of $\mathcal{I}$. Consequently its Gram matrix G is given by

$$G = \left\{ \begin{array}{l} \left(\mathrm{Tr}_{L/\mathbb{Q}(i)}(\nu_k \overline{\nu_l})\right)_{k,l=1}^n \\ \left(\mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(\nu_k \tau(\nu_l))\right)_{k,l=1}^n \end{array} \right.$$

where the trace form is defined as either

$$\begin{array}{rll} \mathrm{Tr}_{L/\mathbb{Q}(i)}: & L \times L & \to \mathbb{Q}(i) \\ & (x,y) & \mapsto \mathrm{Tr}_{L/\mathbb{Q}(i)}(x\overline{y}) \end{array}$$

where $\overline{x}$ denotes the complex conjugation of x, or as

$$\begin{array}{rll} \mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}: & L \times L & \to \mathbb{Q}(\zeta_3) \\ & (x,y) & \mapsto \mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(x\tau(y)) \end{array}$$

where τ denotes the conjugation in $\mathbb{Q}(\zeta_3)$, i.e., $\tau(\zeta_3) = \zeta_3^2$.

We illustrate now how to choose an ideal $\mathcal{I} \subseteq \mathcal{O}_L$ in order to get the rotated versions of the $\mathbb{Z}[i]^n$ or $\mathbb{Z}[\zeta_3]^n$ lattices. This is the same method as explained in Subsection 6.3 (Chapter 2), but we recall it here for convenience. First consider the real lattice $\Lambda(\mathcal{I})$ obtained from $\Lambda^c(\mathcal{I})$ by vectorizing real and imaginary parts of the complex lattice vectors. We want $\Lambda(\mathcal{I})$ to be a rotated version of $\mathbb{Z}^{2n}$ or A_2^n. The basic idea is that the norm of the ideal $\mathcal{I}$ is closely related to the volume of $\Lambda(\mathcal{I})$. We will thus look for an ideal with the *right* norm.

- Consider the ramification in $L/\mathbb{Q}$. The prime factorization of the discriminant $d_{L/\mathbb{Q}} = \prod p_k^{r_k}$ contains the primes which ramify [**41**, p. 88], i.e., $(p_k)\mathcal{O}_L = \prod_\ell \mathcal{I}_{k\ell}^{e_k}$ where $e_k > 1$ [**41**, p. 86].
- Considering the real lattice $\Lambda(\mathcal{O}_L)$, we know that $\mathrm{vol}(\Lambda(\mathcal{O}_L)) = 2^{-n}\sqrt{|d_L|}$. We look for a sublattice $\Lambda(\mathcal{I})$ of $\Lambda(\mathcal{O}_L)$, which could be a scaled version of $\mathbb{Z}^{2n}$ (resp. A_2^n), i.e., $\Lambda(\mathcal{I}) = (\sqrt{c}\mathbb{Z})^{2n}$ (resp. $(cA_2)^n$) for some integer c.
- Since $\Lambda(\mathcal{I})$ is a sublattice of $\Lambda(\mathcal{O}_L)$, $\mathrm{vol}(\Lambda(\mathcal{O}_L)) = 2^{-n}\sqrt{|d_L|}$ must divide
$$\mathrm{vol}(\Lambda(\mathcal{I})) = \begin{cases} \mathrm{vol}(\sqrt{c}\mathbb{Z})^{2n} = c^n \\ \mathrm{vol}(cA_2)^n = c^n\left(\frac{\sqrt{3}}{2}\right)^n \end{cases}$$
i.e., $d_{L/\mathbb{Q}} = \prod p_k^{r_k}$ divides $2^{2n}c^{2n}$ (resp. $3^n c^{2n}$).
- This gives a necessary condition for the choice of $\mathcal{I}$. In terms of norm of the ideal $\mathcal{I}$, we need
$$N(\mathcal{I}) = |\mathcal{O}_L/\mathcal{I}| = \frac{\mathrm{vol}(\Lambda(\mathcal{I}))}{\mathrm{vol}(\Lambda(\mathcal{O}_L))} = \begin{cases} \frac{(2c)^n}{\sqrt{\prod p_k^{r_k}}} \\ \frac{(\sqrt{3}c)^n}{\sqrt{\prod p_k^{r_k}}} \end{cases} \tag{77}$$
Recall from (76) that $d_L = 2^{2n}d^2_{\mathbb{Q}(\theta)}$, when L is the compositum of $\mathbb{Q}(i)$ and $\mathbb{Q}(\theta)$ with coprime discriminants and that $d_L = 3^n d^2_{\mathbb{Q}(\theta)}$, when L is the compositum of $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\theta)$ with coprime discriminants.
- In order to satisfy (77), we must find an ideal of the form
$$\mathcal{I} = \prod \mathcal{I}_{k\ell}^{s_{k\ell}}$$
with norm $\prod_{p_k \neq 2} p_k^{n-r_k/2}$ (resp. $\prod_{p_k\neq 3} p_k^{n-r_k/2}$).

This procedure helps us in "guessing" what is the right ideal $\mathcal{I}$ to take in order to build a $\mathbb{Z}[i]^n$ or $\mathbb{Z}[\zeta_3]^n$ lattice. To prove that we indeed found the right lattice, it is sufficient to show that

$$\mathrm{Tr}_{L/\mathbb{Q}(i)}(\nu_i\bar{\nu_j}) = \delta_{i,j} \text{ resp. } \mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(\nu_i\tau(\nu_j))) = \delta_{i,j},\ i,j = 1,\dots,n \tag{78}$$

where $\{\nu_i\}_{i,j=1}^n$ denotes the basis of the ideal $\mathcal{I}$, and $\delta_{i,j}$ is the Kronecker delta.

Let us come back to the context of STBCs, and consider $\mathcal{A} = (L/K,\sigma,\gamma)$ a cyclic algebra. In the case where L is the compositum of $K = \mathbb{Q}(i)$ (or $\mathbb{Q}(\zeta_3)$) and a totally real field $\mathbb{Q}(\theta)$, we show that the minimum determinant of the corresponding STBCs $\mathcal{C}_\mathcal{I}$ is linked to the discriminant of the number field $\mathbb{Q}(\theta)$.

Proposition 3.1. *Let $\mathcal{C}_{\mathcal{I}}$ be a perfect code built over the cyclic division algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n where $\gamma \in \mathcal{O}_K$, $L = K\mathbb{Q}(\theta)$ and $\mathcal{I}$ is principal. Then*

$$\delta_{\min}(\mathcal{C}_{\mathcal{I}}) = \frac{1}{d_{\mathbb{Q}(\theta)}},$$

where $d_{\mathbb{Q}(\theta)}$ is the absolute discriminant of $\mathbb{Q}(\theta)$.

Proof. Let $\{\nu_i\}_{i=1}^n$ be a basis of the principal ideal $\mathcal{I} = (\alpha)$ and $\Lambda(\mathcal{I})$ denote the real lattice over $\mathbb{Z}$. Recall that

$$\det(\Lambda(\mathcal{I})) = \mathrm{vol}(\Lambda(\mathcal{I}))^2 = 4^{-n} N(\mathcal{I})^2 d_L, \tag{79}$$

where d_L denotes the absolute discriminant of L. Using (76) and considering the real lattice, we have for $K = \mathbb{Q}(i)$

$$\det(\mathbb{Z}^{2n}) = 1 = 4^{-n} N_{L/\mathbb{Q}}(\alpha)^2 d_{\mathbb{Q}(\theta)}^2 4^n$$

and for $K = \mathbb{Q}(\zeta_3)$

$$\det(A_2^n) = (3/4)^n = 4^{-n} N_{L/\mathbb{Q}}(\alpha)^2 d_{\mathbb{Q}(\theta)}^2 3^n.$$

Both cases reduce to

$$N_{L/\mathbb{Q}}(\alpha) = \frac{1}{d_{\mathbb{Q}(\theta)}},$$

and we conclude using Proposition 2.2 of Chapter 5. □

Corollary 3.1. *Let $\mathcal{C}_{\mathcal{I}}$ be a perfect code built over the cyclic division algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n where $\gamma \in \mathcal{O}_K$ and $L = K\mathbb{Q}(\theta)$. Then*

$$\frac{1}{vol(\Lambda^c(\mathcal{I}))} \min_{x \in \mathcal{I}} N_{L/\mathbb{Q}}(x) \geq \delta_{\min}(\mathcal{C}_{\mathcal{I}}) \geq N(\mathcal{I}) = \frac{1}{d_{\mathbb{Q}(\theta)}}.$$

Proof. The lower bound is immediate from Proposition 2.3 and the equality comes from (79), similarly as in the proof of Proposition 3.1 of Chapter 5.

Taking $x_0 \neq 0 \in \mathcal{I}$ and $x_2 = \ldots = x_n = 0$ and normalizing yields the upper bound. □

4. 4×4 perfect STBC Construction

Let $L = \mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1})$ be the compositum of $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$. The extension $L/\mathbb{Q}(i)$ has degree 4 and cyclic Galois group $\langle\sigma\rangle$, with $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$.

We consider the corresponding cyclic algebra $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ of degree 4 .

4.1. The $\mathbb{Z}[i]^4$ lattice. We search for a complex lattice $R\mathbb{Z}[i]^4$ following the approach given in Subsection 3.1. Since the relative discriminant of L is $d_{L/\mathbb{Q}(i)} = 1125 = 3^2 \cdot 5^3$, a necessary condition to obtain $R\mathbb{Z}[i]^4$ is that there exists an ideal $\mathcal{I} \subseteq \mathcal{O}_L$ with norm $45 = 3^2 \cdot 5$. The geometrical intuition is that the sublattice $\Lambda(\mathcal{I})$ has fundamental volume equal to $2^{-4}\sqrt{d_L}N(\mathcal{I}) = 3^4 \cdot 5^4 = \sqrt{15}^8$, which suggests that the fundamental parallelotope of the lattice $\Lambda(\mathcal{I})$ could be a hypercube of edge length equal to $\sqrt{15}$.

An ideal $\mathcal{I}$ of norm 45 is found from the following ideal factorizations

$$\begin{aligned}(3)\mathcal{O}_L &= \mathfrak{P}_3^2\overline{\mathfrak{P}_3}^2,\\ (5)\mathcal{O}_L &= \mathfrak{P}_5^4\overline{\mathfrak{P}_5}^4.\end{aligned}$$

Let us consider $\mathcal{I} = \mathfrak{P}_3\mathfrak{P}_5$. It is a principal ideal $\mathcal{I} = (\alpha)$ generated by $\alpha = ((1-3i)+i\theta^2)$, where $\theta = \zeta_{15} + \zeta_{15}^{-1}$.

A $\mathbb{Z}[i]$–basis of (α) is given by $\{\alpha\theta^i\}_{i=0}^3$. Using the change of basis given by the following matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & -3 & 0 & 1\\ -1 & -3 & 1 & 1 \end{pmatrix},$$

we get a new $\mathbb{Z}[i]$–basis $\{\nu_i\}_{i=1}^4 = \{(1-3i)+i\theta^2, (1-3i)\theta+i\theta^3, -i+(-3+4i)\theta+(1-i)\theta^3, (-1+i)-3\theta+\theta^2+\theta^3\}$. Then by straightforward computation, we check that

$$\frac{1}{15}\mathrm{Tr}_{L/\mathbb{Q}(i)}(\nu_k\bar{\nu_\ell}) = \delta_{k\ell}\ k,\ell = 1,\ldots,4$$

using

$$\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = 1,\ \ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 9,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3) = 1,\ \ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4) = 29.$$

For example, we compute the diagonal coefficients:

$$\mathrm{Tr}_{L/\mathbb{Q}(i)}(|\nu_k|^2) = \begin{cases} \mathrm{Tr}_{L/\mathbb{Q}(i)}(10-6\theta^2+\theta^4) & \text{if } i=1\\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(1+3\theta+\theta^2-\theta^3) & \text{if } i=2\\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(5+6\theta-\theta^2-2\theta^3) & \text{if } i=3\\ \mathrm{Tr}_{L/\mathbb{Q}(i)}(-5\theta+2\theta^2+2\theta^3) & \text{if } i=4 \end{cases}.$$

We finally get

- **Codeword matrices.** The generator matrix of the lattice is given by

$$\begin{aligned} M &= (\sigma_\ell(\nu_k))_{k,\ell=1}^{n} \\ &= \begin{pmatrix} 0.2582 - 0.3122i & 0.3455 - 0.4178i & -0.4178 + 0.5051i & -0.2136 + 0.2582i \\ 0.2582 + 0.0873i & 0.4718 + 0.1596i & 0.1596 + 0.054i & 0.7633 + 0.2582i \\ 0.2582 + 0.2136i & -0.5051 - 0.4178i & -0.4178 - 0.3455i & 0.3122 + 0.2582i \\ 0.2582 - 0.7633i & -0.054 + 0.1596i & 0.1596 - 0.4718i & -0.0873 + 0.2582i \end{pmatrix}, \end{aligned}$$

so that $\mathbf{X} \in \mathcal{C}_{\mathcal{I}}$ is given by

$$\mathbf{X} = \sum_{k=0}^{3} \operatorname{diag}\left(\frac{1}{\sqrt{15}} M (x_{4k}, x_{4k+1}, x_{4k+2}, x_{4k+3})^T \right) E^k$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 \end{pmatrix}.$$

- **The minimum determinant.** By Proposition 2.2 of Chapter 5, the minimum determinant of the infinite code is equal to

$$\delta_{min}(\mathcal{C}_{\mathcal{I}}) = \frac{1}{15^4} N_{L/\mathbb{Q}}(\alpha) = \frac{45}{15^4} = \frac{1}{1125}.$$

Similarly, Proposition 3.1 gives

$$\delta_{min}(\mathcal{C}_{\mathcal{I}}) = \frac{1}{d_{\mathbb{Q}(\theta)}} = \frac{1}{1125}.$$

4.2. The norm condition. We now show that $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ is a division algebra. By Proposition 1.2 and Remark 1.1 (both of Chapter 5), we have to check that i and -1 are not norms of elements in L.

Proposition 4.1. *The unit -1 is not a norm in $\mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i)$.*

Proof. We consider the field extension $L = \mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i)$. We have

$$5\mathbb{Z}[i] = (i+2)(i-2) = \mathfrak{p}_5 \mathfrak{q}_5 \text{ and } 3\mathbb{Z}[i] = (3) = \mathfrak{p}_3.$$

We show that i is not a norm locally in $\mathfrak{p}_5$, thus i is not a norm in L.
Let $y = 12i - 25$. We have that

$$y \equiv 1 \pmod{i+2} \tag{80}$$

$$-y \equiv 1 \pmod{i-2} \tag{81}$$

$$-y \equiv 1 \pmod{3} \tag{82}$$

and $(y)\mathbb{Z}[\zeta_3] = \mathfrak{p}_{769}$. Let $\left(\frac{x,L/K}{\nu}\right)$ denote the Hasse norm symbol. By the product formula

$$\prod_{\nu}\left(\frac{-y,L/K}{\nu}\right) = 1. \tag{83}$$

The product on the ramified primes yields $\left(\frac{-y,L/K}{\mathfrak{p}_5}\right)\left(\frac{-y,L/K}{\mathfrak{q}_5}\right)\left(\frac{-y,L/K}{\mathfrak{p}_3}\right)$, since the ramification in $L/\mathbb{Q}(i)$ is in 5 and 3 only. Since $y \in \mathfrak{p}_{769}$, its valuation is zero for $\nu \neq \mathfrak{p}_{769}$. The valuation of a unit is zero for all places, so that we get for the product on the unramified primes

$$\prod_{\nu \text{ unramified}}\left(\frac{-y,L/K}{\nu}\right) = \prod_{\nu \text{ unramified}}\left(\frac{-1,L/K}{\nu}\right)\left(\frac{y,L/K}{\nu}\right) = \left(\frac{y,L/K}{\mathfrak{p}_{769}}\right).$$

Thus equation (83) simplifies to

$$\left(\frac{-y,L/K}{\mathfrak{p}_3}\right)\left(\frac{y,L/K}{\mathfrak{p}_5}\right)\left(\frac{-1,L/K}{\mathfrak{p}_5}\right)\left(\frac{-y,L/K}{\mathfrak{q}_5}\right)\left(\frac{y,L/K}{\mathfrak{p}_{769}}\right) = 1.$$

The first, second and fourth terms are 1 by the choice of y (see equations (80), (81) and (82)), so that finally we have

$$\left(\frac{-1,L/K}{\mathfrak{p}_5}\right)\left(\frac{y,L/K}{\mathfrak{p}_{769}}\right) = 1.$$

Since $\mathfrak{p}_{769}$ does not split completely, the second term is different from 1, so that $\left(\frac{-1,L/K}{\mathfrak{p}_5}\right) \neq 1$, which concludes the proof. □

It is left to prove that i is not a norm in L.

Lemma 4.1. *We have the following field extensions:*

$$\mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{5}) \subset L.$$

Proof. We show that $\mathbb{Q}(i,\sqrt{5})$ is the subfield fixed by $\langle\sigma^2\rangle$, the subgroup of order 2 of $\mathrm{Gal}(L/\mathbb{Q}(i)) = \langle\sigma\rangle$. Let $\sigma^2 : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^4 + \zeta_{15}^{-4}$ and $x = \sum_{k=0}^{3} a_k(\zeta_{15} + \zeta_{15}^{-1})^k$,

$a_k \in \mathbb{Q}(i)$ be an element of L. It is a straightforward computation to show that $\sigma^2(x) = x$ implies that x is of the form $x = a_0 + a_3(\zeta_{15}^3 + \zeta_{15}^{-3})$. □

Proposition 4.2. *The algebra $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ is a division algebra.*

Proof. We know by Proposition 4.1 that -1 is not a norm. We now prove by contradiction that i is not a norm either.

Suppose i is a norm in L^*, i.e., there exists $x \in L^*$ such that $N_{L/\mathbb{Q}(i)}(x) = i$. By Lemma 4.1 and transitivity of the norm, we have

$$N_{L/\mathbb{Q}(i)}(x) = N_{\mathbb{Q}(\sqrt{5},i)/\mathbb{Q}(i)}(N_{L/\mathbb{Q}(\sqrt{5},i)}(x)) = i.$$

Thus i has to be a norm in $\mathbb{Q}(\sqrt{5}, i)$. By Proposition 2.3 in the case $p = 5$, we know i is not a norm, which is a contradiction. □

Note that the argument of the previous proof does not apply for -1 since it is clearly a norm in $\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(i)$.

5. 3 × 3 perfect STBC Construction

Let $L = \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})$ be the compositum of K and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. The extension $L/\mathbb{Q}(\zeta_3)$ has degree 3 and cyclic Galois group $\langle\sigma\rangle$ with $\sigma : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$.

Consider the corresponding cyclic algebra $\mathcal{A} = (L/K, \sigma, \zeta_3)$ of degree 3.

5.1. The $\mathbb{Z}[\zeta_3]^3$ lattice. In this case, we look for a complex lattice $R\mathbb{Z}[\zeta_3]^3$, where R is a complex unitary matrix but in the sense of the Hermitian transposition defined with the τ-conjugation. The relative discriminant of L is $d_{L/K} = 49 = 7^2$ while its absolute discriminant is $d_L = -3^3 \cdot 7^4$. A necessary condition to obtain $R\mathbb{Z}[\zeta_3]^3$ is the existence of an ideal $\mathcal{I} \subseteq \mathcal{O}_L$ with norm 7. In fact, the lattice $\Lambda(\mathcal{O}_L)$ has fundamental volume equal to $2^{-3}\sqrt{|d_L|} = 7^2 \left(\frac{\sqrt{3}}{2}\right)^3$ and the sublattice $\Lambda(\mathcal{I})$ has fundamental volume equal to $2^{-3}\sqrt{|d_L|}N(\mathcal{I}) = 7^3 \left(\frac{\sqrt{3}}{2}\right)^3$, where the norm of the ideal $N(\mathcal{I})$ is equal to the sublattice index. This suggests that the algebraic lattice $\Lambda(\mathcal{I})$ could be a homothetic version of A_2^3, namely, $(7A_2)^3$.

An ideal $\mathcal{I}$ of norm 7 is found from the following ideal factorizations

$$(7)\mathcal{O}_L \quad = \quad \mathfrak{P}_7^3\overline{\mathfrak{P}_7}^3.$$

Let us consider $\mathcal{I} = \mathfrak{P}_7$. It is a principal ideal $\mathcal{I} = (\alpha)$ generated by $\alpha = (1+\zeta_3)+\theta$, where $\theta = \zeta_7 + \zeta_7^{-1}$. A $\mathbb{Z}[\zeta_3]$–basis of (α) is given by $\{\alpha\theta^i\}_{i=0}^2 = \{(1+\zeta_3)+\theta, (1+\zeta_3)\theta + \theta^2, 1+2\theta+\zeta_3\theta^2\}$. Using the change of basis given by the following matrix

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

one gets a reduced $\mathbb{Z}[\zeta_3]$–basis $\{\nu_i\}_{i=1}^3 = \{(1+\zeta_3)+\theta, (-1-2\zeta_3)+\zeta_3\theta^2, (-1-2\zeta_3)+(1+\zeta_3)\theta+(1+\zeta_3)\theta^2\}$. Denote by $\tau : \zeta_3 \mapsto \zeta_3^2$, the ζ_3-conjugation. Then by straightforward computation we check that

$$\frac{1}{7}\mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(\nu_k\tau(\nu_l)) = \delta_{kl}\ k,l = 1,2,3$$

using $\mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = 3,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = -1,\ \mathrm{Tr}_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 5.$

We compute, for example, the diagonal coefficients

$$\mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(\nu_k\tau(\nu_k)) = \begin{cases} \mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(1+\theta+\theta^2) = 7 & \text{if } k=1 \\ \mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(2-\theta) = 7 & \text{if } k=2 \\ \mathrm{Tr}_{L/\mathbb{Q}(\zeta_3)}(4-\theta^2) = 7 & \text{if } k=3 \end{cases}$$

We finally get

- **Codeword matrices.** The generator matrix of the lattice is given by

$$\begin{aligned} M &= (\sigma_l(\nu_k))_{k,l=1}^n \\ &= \begin{pmatrix} 1.03826+0.32732i & -0.462069-0.145674i & 0.832620+0.262495i \\ -0.11412+0.32732i & -0.142307+0.408169i & 0.063332-0.181652i \\ 0.39873+0.32732i & -0.718498-0.589822i & -0.895953-0.735496i \end{pmatrix}, \end{aligned}$$

so that $\mathbf{X} \in \mathcal{C}_\mathcal{I}$ is given by

$$\mathbf{X} = \sum_{k=0}^{2} \mathrm{diag}\left(\frac{1}{\sqrt{7}}M(x_{3k}, x_{3k+1}, x_{3k+2})^T\right)E^k$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \gamma & 0 & 0 \end{pmatrix}.$$

- **The minimum determinant.** The ideal $\mathcal{I}$ is principal, so that we can use Proposition 2.2 of Chapter 5 to get

  $$\delta_{min}(\mathcal{C}_{\mathcal{I}}) = \frac{1}{7^3} N_{L/\mathbb{Q}}(\alpha) = \frac{7}{7^3} = \frac{1}{49} = \frac{1}{d_{\mathbb{Q}(\theta)}},$$

  by Proposition 3.1.

5.2. The norm condition. By Proposition 1.2 and Remark 1.1, it is enough to show that the unit ζ_3 is not a norm in $\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\zeta_3)$.

PROPOSITION 5.1. *The cyclic algebra* $\mathcal{A} = (\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})/K, \sigma, \zeta_3)$ *is a division algebra.*

PROOF. We consider the field extension $L = \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\zeta_3)$. We have

$$7\mathbb{Z}[\zeta_3] = (\zeta_3 - 2)(\zeta_3 + 3) = \mathfrak{p}_7\mathfrak{q}_7.$$

We show that ζ_3 is not a norm locally in $\mathfrak{p}_7$, thus ζ_3 is not a norm in L.
Let $y = 7 - 3\zeta_3$. We have that

$$y \equiv 1 \pmod{\zeta_3 - 2} \tag{84}$$

$$\zeta_3 y \equiv 1 \pmod{\zeta_3 + 3} \tag{85}$$

and $(y)\mathbb{Z}[\zeta_3] = \mathfrak{p}_{79}$. Let $\left(\frac{x, L/K}{\nu}\right)$ denote the Hasse norm symbol. By the product formula

$$\prod_{\nu} \left(\frac{\zeta_3 y, L/K}{\nu}\right) = \prod_{\nu \text{ ramified}} \left(\frac{\zeta_3 y, L/K}{\nu}\right) \prod_{\nu \text{ unramified}} \left(\frac{\zeta_3 y, L/K}{\nu}\right) = 1. \tag{86}$$

The product on the ramified primes yields $\left(\frac{\zeta_3 y, L/K}{\mathfrak{p}_7}\right)\left(\frac{\zeta_3 y, L/K}{\mathfrak{q}_7}\right)$, since the ramification in $L/\mathbb{Q}(\zeta_3)$ is in 7 only. Note that $\left(\frac{xy, L/K}{\nu}\right) = \left(\frac{x, L/K}{\nu}\right)\left(\frac{y, L/K}{\nu}\right)$ by linearity. We now look at the product on the unramified primes. Since $y \in \mathfrak{p}_{79}$, its valuation is zero for $\nu \neq \mathfrak{p}_{79}$. The valuation of a unit is zero for all places, so that we get

$$\prod_{\nu \text{ unramified}} \left(\frac{\zeta_3 y, L/K}{\nu}\right) = \prod_{\nu \text{ unramified}} \left(\frac{\zeta_3, L/K}{\nu}\right)\left(\frac{y, L/K}{\nu}\right) = \left(\frac{y, L/K}{\mathfrak{p}_{79}}\right).$$

Thus equation (86) simplifies to

$$\left(\frac{\zeta_3, L/K}{\mathfrak{p}_7}\right)\left(\frac{y, L/K}{\mathfrak{p}_7}\right)\left(\frac{\zeta_3 y, L/K}{\mathfrak{q}_7}\right)\left(\frac{y, L/K}{\mathfrak{p}_{79}}\right) = 1.$$

The second and third terms are 1 by the choice of y (see equations (84) and (85)), so that finally we have

$$\left(\frac{\zeta_3, L/K}{\mathfrak{p}_7}\right)\left(\frac{y, L/K}{\mathfrak{p}_{79}}\right) = 1.$$

Since $\mathfrak{p}_{79}$ is inert, the second term is different from 1, so that $\left(\frac{\zeta_3, L/K}{\mathfrak{p}_7}\right) \neq 1$. In words, ζ_3 is not a norm in $\mathfrak{p}_7$ which concludes the proof. □

6. 6×6 perfect STBC Construction

Let $L = \mathbb{Q}(\zeta_3, \zeta_{28} + \zeta_{28}^{-1})$ be the compositum of K and $\mathbb{Q}(\zeta_{28} + \zeta_{28}^{-1})$. The extension $L/\mathbb{Q}(\zeta_3)$ has degree 6 and cyclic Galois group $\langle\sigma\rangle$ with generator $\sigma : \zeta_{28}+\zeta_{28}^{-1} \mapsto \zeta_{28}^2+\zeta_{28}^{-2}$.

Consider the corresponding cyclic algebra $\mathcal{A} = (L/\mathbb{Q}(\zeta_3), \sigma, -\zeta_3)$ of degree 6.

6.1. The $\mathbb{Z}[\zeta_3]^6$ lattice. First note that the discriminant of L is $d_L = 2^{12} \cdot 3^6 \cdot 7^{10}$. Following the approach given in Subsection 3.1, we need to construct a complex lattice $R\mathbb{Z}[\zeta_3]^6$, where R is a complex unitary matrix (in the sense of the hermitian product defined with the τ-conjugation).

A necessary condition to obtain $R\mathbb{Z}[\zeta_3]^6$ is that there exists an ideal $\mathcal{I} \subseteq \mathcal{O}_L$ with norm 7. In fact, the lattice $\Lambda(\mathcal{O}_L)$ has fundamental volume equal to $2^{-6}\sqrt{|d_L|} = 7^5 \cdot 2^6 \cdot \left(\frac{\sqrt{3}}{2}\right)^6$ and the sublattice $\Lambda(\mathcal{I})$ has fundamental volume equal to $2^{-6}\sqrt{|d_L|}N(\mathcal{I}) = 7^6 \cdot 2^6 \cdot \left(\frac{\sqrt{3}}{2}\right)^6$, where the norm of the ideal $N(\mathcal{I})$ is equal to the sublattice index. This suggests that the algebraic lattice $\Lambda(\mathcal{I})$ could be a homothetic version of A_2^6, namely, $\left(\sqrt{14}A_2\right)^3$, but this needs to be checked explicitly.

An ideal $\mathcal{I}$ of norm 7 can be found from the following ideal factorizations

$$(7)\mathcal{O}_L = \mathfrak{P}_7^6\overline{\mathfrak{P}_7}^6.$$

Let us consider $\mathcal{I} = \mathfrak{P}_7$. Unlike in the preceeding constructions, the ideal $\mathcal{I}$ is not principal. This makes harder the explicit computation of an ideal basis, and in particular of the ideal basis (if any) for which the Gram matrix is the identity. We thus adopt the following alternative approach. We compute numerically a basis of $\mathcal{I}$, from which we compute a Gram matrix of the lattice. We then perform a basis reduction on the Gram matrix, using an LLL reduction algorithm (see Subsection 6.3 for more details). This gives both the Gram matrix in the reduced basis and the matrix of change of basis. We get the following change of basis

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1+\zeta_3 & 0 & 1 & 0 & 0 & 0 \\ -1-2\zeta_3 & 0 & -5 & 0 & 1 & 0 \\ 1+\zeta_3 & 0 & 4 & 0 & -1 & 0 \\ 0 & -3 & 0 & 1 & 0 & 0 \\ 0 & 5 & 0 & -5 & 0 & 1 \end{pmatrix}.$$

The lattice generator matrix in numerical form is given by

$$M = \begin{pmatrix} 1.9498 & 1.3019-0.8660i & -0.0549-0.8660i & -1.7469-0.8660i & 1.5636 & 0.8677 \\ 0.8677 & -1.7469-0.8660i & 1.3019-0.8660i & -0.0549-0.8660i & -1.9498 & 1.5636 \\ 1.5636 & -0.0549-0.8660i & -1.7469-0.8660i & 1.3019-0.8660i & -0.8677 & -1.9498 \\ -1.9498 & 1.3019-0.8660i & -0.0549-0.8660i & -1.7469-0.8660i & -1.5636 & -0.8677 \\ -0.8677 & -1.7469-0.8660i & 1.3019-0.8660i & -0.0549-0.8660i & 1.9498 & -1.5636 \\ -1.5636 & -0.0549-0.8660i & -1.7469-0.8660i & 1.3019-0.8660i & 0.8677 & 1.9498 \end{pmatrix}.$$

This matrix satisfies MM^H is the identity matrix, so that we indeed get a rotated version of the $\mathbb{Z}[\zeta_3]^6$ lattice.

- **Codeword matrices.** Using the lattice generator M above, $\mathbf{X} \in \mathcal{C}_\mathcal{I}$ is given by

$$\mathbf{X} = \sum_{k=0}^{5} \operatorname{diag}\left(\frac{1}{\sqrt{14}} M(x_{6k}, x_{6k+1}, x_{6k+2}, x_{6k+3}, x_{6k+4}, x_{6k+5})^T\right) E^k$$

where

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- **The minimum determinant.** Since the ideal $\mathcal{I}$ is not principal, we use the bounds of Corollary 3.1

$$\frac{1}{14^6} \min_{x \in \mathcal{I}} N(x) = \frac{7^2}{2^6 7^6} \geq \delta_{min}(\mathcal{C}_\mathcal{I}) \geq \frac{1}{14^6} N_{L/\mathbb{Q}}(\mathcal{I}) = \frac{1}{2^6 7^5} = \frac{1}{d_{\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1})}}$$

6.2. The norm condition. By Proposition 1.2 and Remark 1.1, it is enough to show that $\gamma = -\zeta_3$, $\gamma^2 = \zeta_3^2$ and $\gamma^3 = -1$ are not a norm in L.

We first prove that -1 is not a norm in $\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},\zeta_3)/\mathbb{Q}(\zeta_3)$.

PROPOSITION 6.1. *The unit -1 is not a norm in* $\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},\zeta_3)/\mathbb{Q}(\zeta_3)$.

PROOF. We consider the field extension $L = \mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},\zeta_3)/\mathbb{Q}(\zeta_3)$. We have

$$7\mathbb{Z}[\zeta_3] = (\zeta_3-2)(\zeta_3+3) = \mathfrak{p}_7\mathfrak{q}_7 \text{ and } 2\mathbb{Z}[\zeta_3] = (2) = \mathfrak{p}_2.$$

We show that -1 is not a norm locally in $\mathfrak{p}_7$, thus -1 is not a norm in L.
Let $y = 3 - 8\zeta_3$. We have that

$$y \equiv 1 \pmod{\zeta_3 - 2} \tag{87}$$

$$-y \equiv 1 \pmod{3 + \zeta_3} \tag{88}$$

$$-y \equiv 1 \pmod{2} \tag{89}$$

and $(y)\mathbb{Z}[\zeta_3] = \mathfrak{p}_{97}$. Let $\left(\frac{x,L/K}{\nu}\right)$ denote the Hasse norm symbol. By the product formula

$$\prod_{\nu}\left(\frac{-y,L/K}{\nu}\right) = 1. \tag{90}$$

The product on the ramified primes yields $\left(\frac{-y,L/K}{\mathfrak{p}_7}\right)\left(\frac{-y,L/K}{\mathfrak{q}_7}\right)\left(\frac{-y,L/K}{\mathfrak{p}_2}\right)$, since the ramification in $L/\mathbb{Q}(\zeta_3)$ is in 7 and 2 only. Since $y \in \mathfrak{p}_{97}$, its valuation is zero for $\nu \neq \mathfrak{p}_{97}$. The valuation of a unit is zero for all places, so that we get for the product on the unramified primes

$$\prod_{\nu \text{ unramified}}\left(\frac{-y,L/K}{\nu}\right) = \prod_{\nu \text{ unramified}}\left(\frac{-1,L/K}{\nu}\right)\left(\frac{y,L/K}{\nu}\right) = \left(\frac{y,L/K}{\mathfrak{p}_{97}}\right).$$

Thus equation (90) simplifies to

$$\left(\frac{-y,L/K}{\mathfrak{p}_2}\right)\left(\frac{y,L/K}{\mathfrak{p}_7}\right)\left(\frac{-1,L/K}{\mathfrak{p}_7}\right)\left(\frac{-y,L/K}{\mathfrak{q}_7}\right)\left(\frac{y,L/K}{\mathfrak{p}_{97}}\right) = 1.$$

The first, second and fourth terms are 1 by choice of y (see equations (87), (88) and (89)), so that finally we have

$$\left(\frac{-1,L/K}{\mathfrak{p}_7}\right)\left(\frac{y,L/K}{\mathfrak{p}_{97}}\right) = 1.$$

Since $\mathfrak{p}_{97}$ does not split completely, the second term is different from 1, so that $\left(\frac{-1,L/K}{\mathfrak{p}_7}\right) \neq 1$, which concludes the proof. □

Lemma 6.1. *We have the following field extensions:*

$$\mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}) \subset \mathbb{Q}(\zeta_3, \zeta_{28} + \zeta_{28}^{-1})$$

Proof. The proof is similar to that of Lemma 4.1. One has to show that $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_3)$ is the subfield fixed by $\langle \sigma^2 \rangle$, the subgroup of order 2 of $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \zeta_{28}+\zeta_{28}^{-1})/K) = \langle \sigma \rangle$. □

Proposition 6.2. *The algebra $\mathcal{A} = (L/K, \sigma, -\zeta_3)$ is a division algebra.*

Proof. By Proposition 6.1, we know -1 is not a norm. We prove, by contradiction, that $-\zeta_3$ and ζ_3^2 are not a norm in L^*. Suppose that either $-\zeta_3$ or ζ_3^2 are a norm in L^*, i.e., there exists $x \in L^*$ such that $N_{L/K}(x) = -\zeta_3$ (resp. ζ_3^2). By Lemma 6.1 and transitivity of the norm, we have

$$N_{L/K}(x) = N_{\mathbb{Q}(\zeta_3,\zeta_7+\zeta_7^{-1})/K}(N_{L/\mathbb{Q}(\zeta_3,\zeta_7+\zeta_7^{-1})}(x)) = -\zeta_3 \text{ (resp. } \zeta_3^2). \tag{91}$$

Thus ζ_3^2 has to be a norm in $\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\zeta_3)$, which is not the case, by Remark 1.1 (Chapter 5).
For $-\zeta_3$, Equation (91) yields, since $[\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}) : K] = 3$,

$$N_{\mathbb{Q}(\zeta_3,\zeta_7+\zeta_7^{-1})/K}(-N_{L/\mathbb{Q}(\zeta_3,\zeta_7+\zeta_7^{-1})}(x)) = \zeta_3,$$

which contradicts Proposition 5.1. □

6.3. The LLL reduction algorithm over $\mathbb{Z}[\zeta_3]$. The standard LLL reduction algorithm [**23**] over $\mathbb{Z}$ can be easily modified to work over $\mathbb{Z}[\zeta_3]$ [**34**]. The two main points to be careful about are

- the Euclidean division: the quotient of the Euclidean division over $\mathbb{Z}[\zeta_3]$ is defined as follows: let $x = x_1 + \zeta_3 x_2$ and $y = y_1 + \zeta_3 y_2$, $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. The division of x by y yields $\frac{x}{y} = z_1 + \zeta_3 z_2$, with $z_1, z_2 \in \mathbb{Q}$. Then we have that $x = yq + r$, where $q = [z_1] + \zeta_3[z_2]$.
- the conjugation: the usual complex conjugation is replaced by the τ-conjugation, that sends ζ_3 onto ζ_3^2.

7. Existence of Perfect Codes

Perfect space-time block codes must satisfy a large number of constraints. Thus, when they are constructed from cyclic algebras, they do not exist for every value of M (number of transmit antennas). We show here that the only values of M for which they exist are 2, 3, 4 and 6.

In order to have non vanishing determinants when the spectral efficiency increases, determinants of the infinite code $\mathcal{C}_\infty$ must take values in a discrete subset of $\mathbb{C}$. We have shown in Subsection 2.1 (Chapter 5) that the determinants of $\mathcal{C}_\mathcal{I}$ are in $\mathcal{O}_K$, when $\mathcal{I} \subseteq \mathcal{O}_L$ and $\gamma \in \mathcal{O}_K$. But $\mathcal{O}_K$ is discrete in $\mathbb{C}$ if and only if K is a quadratic imaginary field, namely $K = \mathbb{Q}(\sqrt{-d})$, with d a positive square free integer.

Remark 7.1. It is important to note that a base field K of degree higher than 2 yields dense determinants.

We now have the further constraint $|\gamma| = 1$. Since $|\gamma|^2 = N_{\mathbb{Q}(\sqrt{-d})/\mathbb{Q}}(x) = 1$ and $\gamma \in \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, γ is a unit.

Lemma 7.1. [**41**, p.76] *Let d be a positive square free integer. The only units of $K = \mathbb{Q}(\sqrt{-d})$ are ± 1 unless $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\zeta_3)$.*

Finally, we require the algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree M to be a division algebra, i.e., γ^k, $k = 1, 2, \ldots, M-1$ cannot be a norm.

Proposition 7.1. *Perfect codes exist exactly when the number of transmit antennas M is 2, 3, 4 and 6.*

Proof. By Lemma 7.1, the only possible values for γ are -1, $\pm i$, $\pm\zeta_3$ and $\pm\zeta_3^2$. Since they are resp. 2nd, 3rd, 4th and 6th roots of unity, we have $M \leq 6$ antennas.

We then show that there does not exist a perfect code in dimension 5. Since the dimension is 5, we need to choose $\gamma = -\zeta_3$, and thus the base field is $\mathbb{Q}(\zeta_3)$. Consider now a number field extension $L/\mathbb{Q}(\zeta_3)$, where L is any cyclic extension of $\mathbb{Q}(\zeta_3)$. The element $1 + \zeta_3$ belongs to L, and its norm is

$$N_{L/\mathbb{Q}(\zeta_3)}(1 + \zeta_3) = (1 + \zeta_3)^5 = -\zeta_3.$$

Thus we cannot find a cyclic division algebra of degree 5 with base field $\mathbb{Q}(\zeta_3)$. □

CHAPTER 7

Codes for noncoherent MIMO Channels

We finally consider the construction of codes for non-coherent MIMO channels. Note that this chapter is not in the continuity of the others, since the algebraic techniques used here are different from the ones used so far.

The problem of designing codes for non-coherent MIMO channels has been shown (see [**26**],[**55**]) to be equivalent to one of packing subspaces according to a certain notion of distance, as we will briefly recall in Section 1. From that point of view, the diversity order was shown to depend on the dimension of the intersection of the subspaces. Maximal diverse codes are thus obtained by building "nonintersecting" subspaces, that is subspaces which intersect only at the origin. The aim of this chapter is the construction of nonintersecting subspaces, subject to the extra constraint that the codewords are defined using symbols from a fixed, small constellation. We focus on two cases: one in which the symbols are taken from a finite field (Section 2) and the other where they are taken from a PSK arrangement, i.e., are complex roots of unity (Section 3). Our aim is to find constructions that give the largest number of nonintersecting subspaces (i.e., have the highest rate) subject to these constraints.

A similar problem has been studied in the context of designing differential codes for the multiple-antenna channel [**27**], [**29**], [**49**]. An extensive characterization and classification of group differential space-time codes was given in [**45**]. The focus of much of this work is on constructing codes which have the nonintersecting subspace property without imposing any constraints on the number of different symbols used to define the codewords—that is, the codewords are allowed to use a signal constellation that is larger than the minimum possible.

It is worth remarking that a recent paper by Lusina et al. [**36**] discusses an analogous problem for the case of coherent decoders. Another related paper by Lu and Kumar [**32**] explores code constructions with fixed alphabet constraints for achieving different points on the rate-diversity trade-off. Again, only coherent decoders are considered. A very recent paper by Kammoun and Belfiore [**30**] directly addresses the problem of constructing codes for non-coherent systems with a large value of $\Lambda(\mathbf{X},\mathbf{X}')$ between subspaces (see (93) below), though with a different approach.

1. Code Design Criteria: nonintersecting Subspaces

We give here a geometric interpretation of fully diverse codewords in term of nonintersecting subspaces, before formalizing the problem statement, introducing the extra constraint of a fixed alphabet.

1.1. A geometric interpretation of the pairwise error probability. Let M_t (M_r) be the number of transmitting (receiving) antennas, and let m be the block length during which the channel is assumed to be time-invariant. Recall from Chapter 4 that the pairwise error probability when the channel is not known at the receiver is upper bounded as follows:

$$P(\mathbf{X}\rightarrow\hat{\mathbf{X}})\leq\frac{1}{\det(\mathbf{I}_{M_t}+\frac{\rho^2m^2}{4(1+\rho m)}[\mathbf{I}_{M_t}-\frac{1}{m^2}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}^H])^{M_r}}\rightarrow(\frac{\Lambda\rho}{4})^{-M_r\nu},$$

where we consider the behaviour when the signal-to-noise ratio (SNR) $\rho=\frac{E_s}{N_0}$ is large. With our previous notations, ν is the rank of $[\mathbf{I}_{M_t}-\frac{1}{m^2}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}]$, and

$$\Lambda=\Lambda(\mathbf{X},\hat{\mathbf{X}})=|m\mathbf{I}_{M_t}-\frac{1}{m}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}^H|_+^{\frac{1}{\nu}}\ , \tag{92}$$

where $|\cdot|_+$ denotes the product of the nonzero eigenvalues. The diversity of the codes is given by $M_r\nu$, so that fully diverse codes reach a diversity order of M_rM_t.

A geometric interpretation of the pairwise error probability can be given by considering subspaces as corresponding to pairs of codewords. It furthermore requires the notion of *principal angles.* The principal angles between two subspaces $\mathbf{X}$ and $\mathbf{X}'$ are given by $\cos\theta_i=\frac{1}{m}\sigma_i(\mathbf{X}'\mathbf{X}^H)$ where $\sigma_i(\cdot)$ is the i-th singular value of the matrix ([**10**], [**20**]). Using this definition, we rewrite Equation (92) as

$$\Lambda(\mathbf{X},\mathbf{X}')^\nu=m\prod_{i=1}^{\nu}[1-\cos^2\theta_i]=m\prod_{i=1}^{\nu}\sin^2\theta_i\ . \tag{93}$$

Note first that if an eigenvalue of $[\mathbf{I}_{M_t}-\frac{1}{m^2}\hat{\mathbf{X}}\mathbf{X}^H\mathbf{X}\hat{\mathbf{X}}]$ is zero, then there exists a principal angle θ such that $1-\cos^2(\theta)=0$. Thus $\theta\in\{0,\pi\}$ and the codewords intersect. This can be reformulated as: in order to have maximal diversity (that is, no zero eigenvalue), we need to construct subspaces which intersect only at the origin.

Remark 1.1. By a slight abuse of notation, we will say in the following of the chapter that two vector spaces are "nonintersecting" if their only common point is the zero vector.

Equation (93) provides a further measure of how good a code is. Since the error probability will be dominated by the pair of codewords with the smallest rank ν and the smallest "distance" $\Lambda(\mathbf{X}, \mathbf{X}')$, not only should the subspaces be nonintersecting, the value of $\Lambda(\mathbf{X}, \mathbf{X}')$ should be large for every pair $\mathbf{X}$, $\mathbf{X}'$ of distinct subspaces.

In brief, to get a diversity order of M_rM_t, we need to construct nonintersecting subspaces which are far apart in the metric defined by (93).

> The first goal is to obtain maximal diversity order by constructing families of subspaces which are nonintersecting.

In order to further improve performance, we need to maximize $\Lambda(\mathbf{X}, \mathbf{X}')$ over all pairs $\mathbf{X}$, $\mathbf{X}'$ of distinct subspaces.

1.2. Statement of the problem. Let us first formalize our code design criterion in terms of nonintersecting subspaces.

Definition 1.1. *Let $\mathbb{F}$ be a field. A* codeword *or* subspace *will mean an M_t-dimensional subspace of $\mathbb{F}^m$. Two subspaces Π_1 and Π_2 are said to be* nonintersecting *over $\mathbb{F}$ if their intersection is trivial, i.e. if $\Pi_1 \cap \Pi_2 = \{0\}$.*

Suppose Π_1 is generated by (row) vectors $u_1, \ldots, u_{M_t} \in \mathbb{F}^m$, and Π_2 is generated by vectors $v_1, \ldots, v_{M_t} \in \mathbb{F}^m$. Let $P := \begin{bmatrix} \Pi_1 \\ \Pi_2 \end{bmatrix}$ denote the $2M_t \times m$ matrix with rows $u_1, \ldots, u_{M_t}, v_1, \ldots, v_{M_t}$. Then the following lemma is readily established.

Lemma 1.1. *The following properties are equivalent:*

(i) *Π_1 and Π_2 are nonintersecting,*

(ii) *P has rank $2M_t$ over $\mathbb{F}$, and*

(iii) *if $m = 2M_t$ the determinant of P is nonzero.*

Suppose now that instead of allowing the entries in the matrices Π_1 and Π_2 to be arbitrary elements of $\mathbb{F}$, we restrict them to belong to a finite subset $\mathcal{A} \subseteq \mathbb{F}$, called the *alphabet.* In other words, the vectors $u_1, \ldots, u_{M_t}, v_1, \ldots, v_{M_t}$ must belong to $\mathcal{A}^m$. The question that we address is the following:

> Given M_t, m and a finite alphabet $\mathcal{A} \subseteq \mathbb{F}$, how many subspaces can we find which are generated by vectors from $\mathcal{A}^m$ and which are pairwise nonintersecting over $\mathbb{F}$?

Furthermore, if the size of $\mathcal{A}$ is specified in advance, which choice of $\mathcal{A}$ permits the biggest codes? Since the rate of a code $\mathcal{C}$ is $R = \frac{1}{m}\log(|\mathcal{C}|)$, in trying to construct the maximal number of nonintersecting subspaces, we attempt to get the highest rate codes (in the sense of Definition 1.1 of Chapter 4) that achieve maximal diversity order.

We first dispose of the trivial case when $M_t = 1$. Two nonzero vectors u, v are said to be *projectively distinct* over a field $\mathbb{F}$ if there is no $a \in F$ such that $u = av$. Then if $M_t = 1$, the maximum number of nonintersecting subspaces is simply the maximum number of projectively distinct vectors in $\mathcal{A}^m$.

In the following sections, we will investigate the first question for two kinds of alphabets:

(a) $\mathcal{A}$ is a finite field $\mathbb{F}$ (Section 2), and

(b) $M_t = 2$ and $\mathcal{A} \subseteq \mathbb{C}^m$ is a set of complex roots of unity (Section 3).

Of course, for the application to multiple-antenna code design, the subspaces need to be disjoint over $\mathbb{C}$. In Theorem 2.3 of Section 2, we translate the results obtained over $\mathbb{F}$ to this case by "lifting" the subspaces to the complex field.

Remark 1.2. For this application, the case $m = 2M_t$ is the most important. Indeed, as follows from Equation (62), we need $m \geq 2M_t$ in order to get full diversity. But at the same time, we want the highest rate possible. The trade-off is thus to take $m = 2M_t$.

2. Finite Fields

In this section we assume that the alphabet $\mathcal{A}$ and the field $\mathbb{F}$ are both equal to the finite field $GF(q)$, where q is a power of a prime p. At the end of the section, we show how to "lift" these planes to the complex field (see Theorem 2.3). In this case there is an obvious upper bound which can be achieved in infinitely many cases. Let V denote the vector space $GF(q)^m$.

THEOREM 2.1. *The number of pairwise nonintersecting M_t-dimensional subspaces of V is at most*

$$\frac{q^m - 1}{q^{M_t} - 1} \ . \tag{94}$$

PROOF. There are $q^m - 1$ nonzero vectors in V and each subspace contains $q^{M_t} - 1$ of them. No nonzero vector can appear in more than one subspace. □

It is convenient here to use the language of projective geometry, c.f. [**33**, Appendix B]. Recall that the points of the *projective space* $P(s, q)$ are equivalence classes of nonzero vectors from $GF(q)^{s+1}$, where two vectors are regarded as equivalent if one is a nonzero scalar multiple of the other.

A *spread* [**25**] in $PG(s, q)$ is a partition of the points into copies of $PG(r, q)$.

THEOREM 2.2. *Such a spread exists if and only if $r + 1$ divides $s + 1$.*

PROOF. This is a classical result, due to André ([**1**] [**25**, Theorem 4.1.1]). □

COROLLARY 2.1. *The bound (94) can be attained whenever M_t divides m, and only in those cases.*

PROOF. This is immediate from the theorem, since a set of points in a projective space represents a set of projectively distinct lines in the corresponding vector space. □

Note that the condition is independent of q. If a set of nonintersecting subspaces meeting (94) exists over one finite field then it exists over every finite field.

Furthermore, it is straightforward to construct the nonintersecting subspaces meeting the bound in (94), as we now show. The nonzero elements of a finite field $\mathbb{F}$ form a cyclic group which will be denoted by $\mathbb{F}^*$.

Suppose M_t divides m, and consider the fields $F_0 = GF(q)$, $F_1 = GF(q^{M_t})$, $F_2 = GF(q^m)$. Then $F_0 \subseteq F_1 \subseteq F_2$. By regarding $GF(q^m)$ as a vector space of dimension m over $GF(q)$ we can identify F_2 with V. Similarly we can regard F_1 as a M_t-dimensional subspace of V. The desired spread is now obtained by partitioning F_2^* into (multiplicative) cosets of F_1^*.

EXAMPLE 2.1. We consider the case $M_t = 2$, $m = 4$ and $\mathcal{A} = GF(2) = \{0, 1\}$. Then $F_0 = GF(2), F_1 = GF(4), F_2 = GF(16)$. Each plane in $GF(2)^4$ contains three nonzero vectors, and $GF(2)^4$ itself contains 15 nonzero vectors. We wish to find a spread of

$PG(1,2)$'s inside $PG(3,2)$, that is, a partitioning of the 15 vectors into five disjoint sets of three, where each set of three adds to the zero vector.

Let $GF(16) = GF(2)[\alpha]$, where $\alpha^4 + \alpha + 1 = 0$. Then $GF(4)$ is the subfield $\{0, 1, \alpha^5, \alpha^{10}\}$, so $F_1^* = \{1, \alpha^5, \alpha^{10}\}$, and we obtain the desired partition

$$F_2^* = \bigcup_{j=0}^{4} \alpha^j F_1^* \ .$$

Only two of the three vectors are needed to define each plane, so we have the following generators for the five planes:

$$(1, \alpha^5),\ (\alpha, \alpha^6),\ (\alpha^2, \alpha^7),\ (\alpha^3, \alpha^8),\ (\alpha^4, \alpha^9) \ .$$

We convert these to explicit generator matrices for the five nonintersecting planes:

$$\begin{bmatrix} 1000 \\ 0110 \end{bmatrix}, \begin{bmatrix} 0100 \\ 0011 \end{bmatrix}, \begin{bmatrix} 0010 \\ 1101 \end{bmatrix}, \begin{bmatrix} 0001 \\ 1010 \end{bmatrix}, \begin{bmatrix} 1100 \\ 0101 \end{bmatrix} .$$

The problem is therefore essentially solved as long as M_t divides m. If not, we can use partial spreads – see the surveys in [**13**] and [**46**].

We end this section by observing that a set of nonintersecting subspaces over a finite field $\mathcal{A} = GF(q)$, $q = p^k$, p prime, can always be "lifted" to a set of nonintersecting subspaces over a complex alphabet $\bar{\mathcal{A}}$ of the same size.

This can be done as follows. Suppose $GF(q) = GF(p)[\alpha]$, where α is a root of a primitive irreducible polynomial $f(X) \in GF(p)[X]$. Let $n = p^k - 1$ and $\zeta_n = e^{2\pi i/n}$. Let $\mathbb{Q}(\zeta_n)$ be a cyclotomic field , with ring of integers $\mathbb{Z}[\zeta_n]$. It is a classical result from number theory that the ideal (p) in $\mathbb{Z}[\zeta_n]$ factors into $g = \varphi(n)/k$ distinct maximal prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$, where $\varphi(\cdot)$ is the Euler totient function. Furthermore, for each $\mathfrak{p}_j$, the residue class ring $\mathbb{Z}[\zeta_n]/\mathfrak{p}_j \cong GF(q)$ (see for example [**9**, Theorem 10.45], [**54**, Theorem 2.13]). If we choose $\mathfrak{p}_j$ to be the ideal generated by p and $f(\zeta_n)$, then $\mathbb{Z}[\zeta_n]/\mathfrak{p}_j$ is exactly the version of $GF(q)$ that we started with. Note that since $\mathfrak{p}_\mathrm{j}$ contains (p), it acts as reduction mod p on $\mathbb{Z}$. We therefore have a ring homomorphism from $\mathbb{Z}[\zeta_n]$ to $GF(q)$ given by

$$\phi : \mathbb{Z}[\zeta_n] \overset{\text{mod } p}{\to} \mathbb{Z}[\zeta_n]/\mathfrak{p}_\mathrm{j} \overset{\cong}{\to} GF(q) \ . \qquad (95)$$

In this way we can lift vectors over $GF(q)$ to vectors over the alphabet $\bar{\mathcal{A}}$ consisting of 0 and the $q-1$ powers of ζ_n.

Example 2.2. Let $GF(8) = GF(2)[\alpha]$ where α is a root of X^3+X+1. Then $q = 8$, $n = 7$, $\zeta_7 = e^{2\pi i/7}$. To lift $GF(8)$ to $\mathbb{C}$ we write $GF(8) = \{0, 1, \alpha, \alpha^2, \dots, \alpha^6\}$, and lift 0 to 0 and α^j to ζ_7^j for $j = 0, \dots, 6$.

Let Π be an M_t-dimensional subspace of $GF(q)^m$. By lifting each element of a generator matrix we obtain an M_t-dimensional subspace $\bar{\Pi} \subseteq \mathbb{C}^m$, defined over an alphabet $\bar{\mathcal{A}}$ of size q.

Theorem 2.3. *If two subspaces Π_1, Π_2 of $GF(q)^m$ are nonintersecting, so are their lifts $\bar{\Pi}_1, \bar{\Pi}_2$.*

Proof. Let $P := \begin{bmatrix} \Pi_1 \\ \Pi_2 \end{bmatrix}$ and $\bar{P} := \begin{bmatrix} \bar{\Pi}_1 \\ \bar{\Pi}_2 \end{bmatrix}$. By Lemma 1.1, P has a $2M_t \times 2M_t$ invertible submatrix. Since ϕ is a ring homomorphism, the lift of this submatrix is also invertible. □

It follows that the subspaces constructed in Corollary 2.1 are also nonintersecting when lifted to the complex field.

This construction gives full diversity order non-coherent space-time codes when the elements of the codewords are restricted to belong to a finite field. Their rate is

$$R = \frac{1}{m}\log(q^m - 1) - \frac{1}{m}\log(q^{M_t} - 1) < \log(q) \ ,$$

which according to Theorem 2.1 is the maximal achievable rate for diversity order $M_t M_r$. Moreover, the above relationship implies that for fully diverse codes constructed from a finite field, we cannot achieve a rate higher than $\log(|\mathcal{A}|)$.

3. PSK Constellations

Throughout this section we assume that the alphabet $\mathcal{A}$ consists of the set of complex 2^r-th roots of unity, that is, $\mathcal{A} = \{e^{2\pi i j/2^r}, 0 \le j < 2^r\}$, for some $r \ge 1$. Let $\zeta = e^{2\pi i/2^r}$ be a primitive 2^r-th root of unity; $\mathcal{A}$ is a cyclic multiplicative group with generator ζ. In this section we assume that $M_t = 2$, that is, the code consists of a set of pairwise nonintersecting planes.

Example 3.1. Some examples of roots of unity:

(1) If $r = 1$, $\zeta = -1$ and the alphabet is $\mathcal{A} = \{1, -1\}$.

(2) If $r = 2$, $\zeta = i$ and the alphabet is $\mathcal{A} = \{1, i, -1, -i\}$.

(3) If $r = 3$, $\zeta = (1+i)/\sqrt{2}$ and the alphabet is $\mathcal{A} = \{e^{\pi i j/4}, 0 \leq j \leq 7\}$. This is the 8-PSK constellation.

There is a trivial upper bound.

Theorem 3.1. *Let $\mathcal{A}$ be the set of 2^r roots of unity, $r \geq 1$. Then the number of pairwise nonintersecting planes is at most $\frac{1}{2}|\mathcal{A}|^{m-1} = 2^{(m-1)r-1}$.*

Proof. If $v_1, v_2 \in \mathcal{A}^m$ are the generators for a plane, that plane also contains all multiples $\zeta^j v_1$ and $\zeta^j v_2$, a total of $2|\mathcal{A}|$ vectors. Since these sets of vectors must all be disjoint, the number of planes is at most $|\mathcal{A}|^m/(2|\mathcal{A}|)$. □

The same argument shows that there are at most $\frac{1}{M_t}|\mathcal{A}|^{m-1}$ nonintersecting M_t-dimensional subspaces of complex m-dimensional space for any finite alphabet $\mathcal{A}$. The implication of this in terms of rate is that

$$R \leq \frac{m-1}{m}\log(|\mathcal{A}|) - \frac{1}{m}\log(M_t) < \log(|\mathcal{A}|) \ .$$

Hence, for fully diverse codes constructed from PSK constellations, we cannot achieve a rate exceeding $\log(|\mathcal{A}|)$.

Example 3.2. Let $\mathcal{A}$ be the set $\{1, i, -1, -i\}$ and take $m = 4$. The total number of vectors in $\mathcal{A}^4$ is 4^4. Each vector has 4 multiples, so each plane accounts for at least 8 vectors. Therefore there are at most $\frac{4^4}{8} = 32$ planes.

In the other direction we will prove:

Theorem 3.2. *Assume $r \geq 1$ and that $m \geq 2$ is even. There exist $N = |\mathcal{A}|^{m-2} = 2^{(m-2)r}$ pairwise nonintersecting planes in $\mathbb{C}^m$ defined using the complex 2^r-th roots of unity.*

Note that the upper and lower bounds coincide in the case $r = 1$, that is, when $\mathcal{A} = \{1, -1\}$.

The proof is simplified by the use of valuations (cf. [**21**]). If $x \in \mathbb{Q}$, $x = 2^a \frac{b}{c}$ with $a, b, c \in \mathbb{Z}, c \neq 0$, b and c odd, then the 2-adic valuation of x is $\nu_2(x) = a$. Similarly, suppose x belongs to the cyclotomic field $\mathbb{Q}(\zeta)$. Since $1 - \zeta$ is a prime in $\mathbb{Z}[\zeta]$, we can write x uniquely as $(1-\zeta)^a \frac{b}{c}$ with $a \in \mathbb{Z}$, $b, c \in \mathbb{Z}[\zeta], c \neq 0$, b and c relatively prime to $1 - \zeta$. The $(1-\zeta)$-adic valuation of x is then $\nu_{1-\zeta}(x) = a$. It is easy to check that for $k \in \mathbb{Z}$, $k \neq 0$, $\nu_{1-\zeta}(1 - \zeta^k) = 2^{\nu_2(k)}$. In particular, if $k \in \mathbb{Z}$ is odd, $\nu_{1-\zeta}(1-\zeta^k) = 1$.

We will also need a lemma:

Lemma 3.1. *Let* Π *be a plane in* $\mathbb{C}^m$ *generated by vectors* v_1, v_2, *and denote by*

$$\tilde{\Pi}_1 = \begin{bmatrix} v_1 & x_{11} & x_{12} \\ v_2 & x_{21} & x_{22} \end{bmatrix}$$

and

$$\tilde{\Pi}_2 = \begin{bmatrix} v_1 & y_{11} & y_{12} \\ v_2 & y_{21} & y_{22} \end{bmatrix}$$

two different embeddings of Π *into* $\mathbb{C}^{m+2}$. *Then* $\tilde{\Pi}_1 \cap \tilde{\Pi}_2 = \{0\}$ *if and only if*

$$\begin{vmatrix} y_{11} - x_{11} & y_{12} - x_{12} \\ y_{21} - x_{21} & y_{22} - x_{22} \end{vmatrix} \neq 0.$$

Proof. By Lemma 1.1, it is necessary and sufficient that the matrix $P := \begin{bmatrix} \tilde{\Pi}_1 \\ \tilde{\Pi}_2 \end{bmatrix}$ have rank 4. Subtracting the first and second rows of P from the third and fourth rows, we get the matrix

$$\begin{bmatrix} v_1 & x_{11} & x_{12} \\ v_2 & x_{21} & x_{22} \\ 0 & y_{11} - x_{11} & y_{12} - x_{12} \\ 0 & y_{21} - x_{21} & y_{22} - x_{22} \end{bmatrix}.$$

and the result follows. □

We now give the proof of the theorem, for which we use induction on even values of m. For $m = 2$ we take the single plane

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Suppose the result is true for m. For each of the $|\mathcal{A}|^{m-2}$ pairwise nonintersecting planes in $\mathbb{C}^m$ we will construct $|\mathcal{A}|^2$ planes in $\mathbb{C}^{m+2}$, such that full set of planes so obtained is pairwise nonintersecting; this will establish the desired result.

If two planes are nonintersecting in $\mathbb{C}^m$ then they are certainly nonintersecting when embedded in any way in $\mathbb{C}^{m+2}$. So we only need to show that the $|\mathcal{A}|^2$ embeddings of any single plane are pairwise nonintersecting.

Let Π be a plane in $\mathbb{C}^m$ generated by vectors v_1, v_2, and denote by $\tilde{\Pi}(a,b)$ the plane in $\mathbb{C}^{m+2}$ with generator matrix

$$\begin{bmatrix} v_1 & \zeta^a & \zeta^b \\ v_2 & \zeta^{a+b} & \zeta^{a+2b+1} \end{bmatrix},$$

for $a, b = 0, 1, \ldots, 2^r - 1$.

We will use Lemma 3.1 to show that all the planes $\{\tilde{\Pi}(a,b) \mid a \in \mathcal{A},\, b \in \mathcal{A}\}$ are pairwise nonintersecting. For this we must show that

$$\begin{vmatrix} \zeta^c - \zeta^a & \zeta^d - \zeta^b \\ \zeta^{c+d} - \zeta^{a+b} & \zeta^{c+2d+1} - \zeta^{a+2b+1} \end{vmatrix} = 0$$

if and only if $a = c$ and $b = d$.

The above determinant is equal to

$$\zeta^{2c+2d+1}(1-\zeta^{a-c})(1-\zeta^{(a-c)+2(b-d)}) - \zeta^{c+2d}(1-\zeta^{b-d})(1-\zeta^{(a-c)+(b-d)}) \ . \tag{96}$$

If the determinant is zero, the $(1-\zeta)$-adic valuations of the two terms on the right must be equal, that is,

$$2^{\nu_2(a-c)} + 2^{\nu_2(a-c+2(b-d))} = 2^{\nu_2(b-d)} + 2^{\nu_2(a-c+b-d)} \ . \tag{97}$$

We must show that this is true if and only if $a = c$ and $b = d$. We consider four cases, depending on the parity of $a-c$ and $b-d$. If $a-c \equiv 1, b-d \equiv 1 (\text{mod } 2)$ then (96) reads $1+1 = 1+2^{\nu_2(a-c+b-d)} \geq 3$ (since $a-c+b-d$ is even), a contradiction. Similarly, if $a-c \equiv 1, b-d \equiv 0 (\text{mod } 2)$ we get $1+1 = 2^{\nu_2(b-d)}+1$, and if $a-c \equiv 0, b-d \equiv 1 (\text{mod } 2)$ we get $2^{\nu_2(a-c)} + 2^{\nu_2(a-c+2(b-d))} = 1+1$, which are also contradictions. The fourth possibility is $a-c \equiv b-d \equiv 0$ (mod 2). Let $a-c = 2^s x$ and $b-d = 2^t y$, where x and y are odd, $s, t \geq 1$. We have

$$\nu_2(a-c+2(b-d)) = \begin{cases} s & \text{if } s < t \\ s & \text{if } s = t \\ \geq t & \text{if } s > t \end{cases}$$

and

$$\nu_2(a-c+2(b-d)) = \begin{cases} s & \text{if } s < t \\ \geq s & \text{if } s = t \\ t & \text{if } s > t \end{cases}$$

Substituting these valuations in equation (97) again gives a contradiction. This concludes the proof of Theorem 3.2.

4. Summary of the Results

The following table compares the codes constructed in Sections 2 and 3 in the case $M_t = 2$, i.e., codes which are pairwise nonintersecting 2-dimensional subspaces of $\mathbb{C}^m$, for $m = 4, 6$ and 8, and alphabets $\mathcal{A}$ of sizes 2, 4 and 8. The top entry in each cell gives the number of planes obtained from the finite field construction (Corollary 2.1). The bottom entry gives the lower and upper bounds obtained using complex $|\mathcal{A}|$-th roots of unity, from Theorem 3.2 and Theorem 3.1.

	$m = 4$	$m = 6$	$m = 8$
$\lvert\mathcal{A}\rvert = 2$	5 $4 - 4$	21 $16 - 16$	85 $64 - 64$
$\lvert\mathcal{A}\rvert = 4$	17 $16 - 32$	273 $256 - 512$	4369 $4096 - 8192$
$\lvert\mathcal{A}\rvert = 8$	65 $64 - 256$	4161 $4096 - 16384$	266305 $262144 - 1048576$

Table I. Number of pairwise nonintersecting planes in $\mathbb{C}^m$ for various sizes of the alphabet $|\mathcal{A}|$ (see text for details).

Note that the construction via finite fields results in codes for which alphabet consists of 0 and the complex $(|\mathcal{A}| - 1)$-st roots of unity, whereas the construction via PSK constellations produces codes in which the symbols are the complex $|\mathcal{A}|$-th roots of unity (and 0 is not used).

Asymptotically, the rates of the two constructions are very similar. Both satisfy $\log(\text{ number of codewords })/m \approx \log(|\mathcal{A}|)$, for m large, and so both asymptotically achieve the maximal rate possible for fully diverse codes.

Bibliography

[1] J. André. Uber nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60:156–186, 1954.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. PARI/GP-a software package for computer-aided number theory.

[3] E. Bayer-Fluckiger. Lattices and number fields. *Contemporary Mathematics*, 241:69–84, 1999.

[4] J.-C. Belfiore and G. Rekaya. Quaternionic lattices for space-time coding. *Proceedings of ITW2003, Paris*, April 2003.

[5] J.-C. Belfiore, G. Rekaya, and E. Viterbo. The Golden Code: A 2 × 2 Full-Rate Space-Time Code with Non-Vanishing Determinant. *submitted to IEEE Trans. Inform. Theory*, 2004.

[6] G. Berhuy. Réalisation de formes **Z**-bilinéaires symétriques comme formes trace hermitiennes amplifiées. *J. de Théorie des Nombres de Bordeaux*, 12:25–36, 2000.

[7] J. Boutros and E. Viterbo. Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel. *IEEE Transactions on Information Theory*, 44, n. 4:1453–1467, 1998.

[8] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore. Good Lattice Constellations for both Rayleigh Fading and Gaussian Channels. *IEEE Transactions on Information Theory*, 42, n. 2:502–518, 1996.

[9] H. Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer-Verlag, NY, 1978.

[10] J.H. Conway, R.H. Hardin, and N.J.A Sloane. Packing lines, planes, etc.: packings in Grassmannian space. *Experimental Math.*, 5:139–159, 1996.

[11] J.H. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups.* Springer-Verlag, New York, 1988.

[12] M.O. Damen, H. El Gamal, and N.C. Beaulieu. Systematic construction of full diversity algebraic constellations. *IEEE Transactions on Information Theory*, 2003.

[13] J. Eisfeld and L. Storme. (partial) t-spreads and minimal t-covers in finite projective spaces. *Lecture notes from the Socrates Intensive Course on Finite Geometry and its Applications*, 2000.

[14] H. El Gamal and M.O. Damen. Universal space-time coding. *IEEE Trans. Inform. Theory*, 49:1097–1119, May 2003.

[15] H. El Gamal and A. R. Hammons Jr. A new approach to layered space-time coding and signal processing. *IEEE Trans. Inform. Theory*, 47:2321–2334, September 2001.

[16] B. Erez. The Galois Structure of the Trace form in Extensions of Odd Prime Degree. *J. of Algebra*, 118:438–446, 1988.

[17] A. Fröhlich and M.J. Taylor. *Algebraic number theory.* Cambridge University Press, Great Britain, 1991.

[18] S. Galliou and J.-C. Belfiore. A new family of full rate, fully diverse space-time codes based on Galois theory. *Proceedings IEEE International Symposium on Information Theory*, page 419, July 2002.

[19] X. Giraud, E. Boutillon, and J.-C. Belfiore. Algebraic tools to build modulation schemes for fading channels. *IEEE Transactions on Information Theory*, 43, n. 3:938–952, 1997.

[20] G.H. Golub and C.F. Van Loan. *Matrix Computations.* Johns Hopkins Univ. Press, 2nd edition, 1989.

[21] F.Q. Gouvea. *p-adic Numbers: An Introduction.* Springer Verlag, 1993.

[22] G. Gras. *Class Field Theory.* Springer Verlag, 2003.

[23] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization.* New York: Springer-Verlag, 1988.

[24] B. Hassibi and B.M. Hochwald. High-rate codes that are linear in space and time. *IEEE Transactions on Information Theory*, 48:1804–1824, July 2002.

[25] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Oxford Univ. Press, 1979.

[26] B.M. Hochwald and T.L. Marzetta. Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading . *IEEE Transactions on Information Theory*, 46(2):543–564, March 2000.

[27] B.M. Hochwald and W. Sweldens. Differential unitary space-time modulation. *IEEE Transactions on Communications*, 48(12):2041–2052, 2000.

[28] R.A. Horn and C.R. Johnson. *Matrix Analysis.* Cambridge Univ. Press, 1985.

[29] B.L. Hughes. Differential space-time modulation. *IEEE Transactions on Information Theory*, 46(7):2567–2578, November 2000.

[30] I. Kammoun and J.-C. Belfiore. A new family of grassmann space-time codes for non-coherent mimo systems. *IEEE Communications Letters*, 7(11):528–530, 2003.

[31] M. Krüskemper. Algebraic construction of bilinear forms over $\mathbb{Z}$. *Pub.Math. de Besancon, Théorie des nombres*, 1996/97 - 19997/98.

[32] H.-F. Lu and P V. Kumar. Rate-diversity trade-off of space-time codes with fixed alphabet and optimal constructions for psk modulation. *IEEE Transactions on Information Theory*, 49(10):2747–2752, 2003.

[33] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977, 10-th impression, 1998.

[34] H. Napias. A generalization of the LLL algorithm over Euclidean rings or orders . *Journal de Théorie des Nombres de Bordeaux*, 8:387–396, 1996.

[35] A.M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Séminaire de Théorie des Nombres, Bordeaux*, pages 1–15, 1989.

[36] E. M. Gabidulin P. Lusina and M. Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003.

[37] E. Perlis Conner. *A survey of trace forms of algebraic number fields.* 1984.

[38] R.S. Pierce. *Associative Algebras.* Springer-Verlag, New York, 1982.

[39] M. Pohst, J. Martinet, and F. Diaz y Diaz. The minimum discriminant of totally real octic fields. *J.Number Theory*, 36, n. 2:145–159, 1990.

[40] I. Reiner. *Maximal Orders.* Academic Press, 1975.

[41] P. Samuel. *Théorie algébrique des nombres.* Hermann, 1971.

[42] W. Scharlau. *Quadratic and Hermitian Forms.* Springer Verlag, 1985.

[43] A. Schiemann. Classification of hermitian forms with the neighbour method. *J. Symbolic Computation*, 26:487–508, 1998.

[44] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Transactions on Information Theory*, 49(10), October 2003.

[45] A. Shokrollahi, B. Hassibi, B. M. Hochwald, and W. Sweldens. Representation theory for high-rate multiple-antenna code design. *IEEE Transactions on Information Theory*, 47(6):2335–2367, 2001.

[46] L. Soicher. Computation of partial spreads. Published electronically at http://www.maths.qmul.ac.uk/~leonard/partialspreads/.

[47] I.N. Stewart and D.O. Tall. *Algebraic Number Theory.* Chapman and Hall, 1979.

[48] H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory.* University Press of Cambridge, 2001.

[49] V. Tarokh and H. Jafarkhani. A differential detection scheme for transmit diversity. *IEEE Journal of Selected Areas in Communications*, 18(7):1169–1174, 2000.

[50] V. Tarokh, N. Seshadri, and A. R. Calderbank. Space-time codes for high data rate wireless communications: Performance criterion and code construction. *IEEE Transactions on Information Theory*, 44(2):744–765, March 1998.

[51] O. Taussky. On a theorem of Latimer and MacDuffee. *Canad.J.Math.*, 1:300–302, 1949.

[52] O. Taussky. On matrix classes corresponding to an ideal and its inverse. *Illinois Math.J.*, 1:108–113, 1957.

[53] E. Viterbo and J. Boutros. A Universal Lattice Code Decoder for Fading Channels. *IEEE Transactions on Information Theory*, 45, n. 5:1639–1642, 1999.

[54] L.C. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag, NY, 1982.

[55] L. Zheng and D. N. C. Tse. Communication on the Grassmann manifold: a geometric approach to the noncoherent multiple-antenna channel. *IEEE Transactions on Information Theory*, 48(2):359–383, 2002.

Frédérique Oggier

Business address:	Home address:
Institut de Mathématiques Bernoulli	5 rte de la Plaine
EPFL	1022 Chavannes-près-Renens
1015 Lausanne, Switzerland	frederique.oggier@epfl.ch

Research Interests

Mathematics and computer science. I am interested both in pure and applied problems in mathematics, especially when they relate to computer science and to applications to communications system.

Education

- Licence in Mathematics, Université de Genève, 1999
- Diplôme in Mathematics and Computer Science, Université de Genève, November 2000
- Graduate School in communication systems, EPFL, July 2001

Research Experience

- Ecole Polytechnique Fédérale de Lausanne(3/2000-10/2000).
  Diploma student, Laboratoire de Communications Audiovisuelles.
  Research work on the design of codes for delay-constrained communication over networks.
  Supervisor: Sergio Servetto.
- Ecole Polytechnique Fédérale de Lausanne(1/2001-7/2001).
  Graduate student, Laboratoire de Communications Audiovisuelles.
  Implementation of an algorithm for solving semidefinite programming problems.
  Supervisor: Sergio Servetto.
- Ecole Polytechnique Fédérale de Lausanne (9/2001 -).
  PhD student, Institut de Mathématiques Bernoulli.
  Research work on developping algebraic techniques for channel coding.
  Supervisors: Eva Bayer Fluckiger and Rudiger Urbanke.

- Visitor at the School of Electrical and Computer Engineering at Cornell University (February-March 2003).

  Host: Professor Sergio Servetto.
- Visitor at AT&T Shannon Labs, Florham Park, NJ (June-September 2003).

  Host: N.J.A. Sloane.

Teaching-Academic Experience

- Université de Genève(10/99-6/2000).

  Student assistant for the course "Mathémathiques pour informaticiens"
- EPFL(10/2001-3/2002, 10/2003-3/2004 and 10/2004-3/2005).

  Teaching assistant for the course "Algèbre linéaire"
- EPFL(10/2002-3/2003, 10/2003-3/2004 and 10/2004-3/2005).

  Teaching assistant for the course "Algèbre pour les communications numériques"
- Supervisation of student projects:
  (1) Méthodes algébriques pour la construction de codes sur les canaux à évanouissement de Rayleigh, J.F. Crisinel, diploma work, winter 2003-2004.
  (2) Corps finis appliqués au codage, T. Martins, semester project, summer 2004.

Personal information

- Full name: Frédérique Elise Oggier.
- Telephone: +41 21 691 29 93
- Date and Place of Birth: February 28th, 1977, Monthey, Switzerland.

Publications

Papers at Refereed Conferences

(1) F. E. Oggier, S. D. Servetto. "Codes for Delay-Constrained Network Communication". DCC 2001.

(2) F. Oggier, E. Bayer-Fluckiger, E. Viterbo. "New algebraic constructions of rotated cubic lattice constellations for the Rayleigh fading channel". ITW 2003, Paris.

(3) F. Oggier, E. Bayer-Fluckiger."Best rotated cubic lattice constellations for the Rayleigh fading channel". ISIT 2003, Yokohama.

(4) E. Bayer-Fluckiger, F. Oggier and E. Viterbo. "Bounds on the Performance of Rotated Lattice Constellations". ISIT 2004, Chicago.

(5) F. E. Oggier, N. J. A. Sloane, S. N. Diggavi and A. R. Calderbank. "Non-intersecting Subspaces Based on Finite Alphabets", ISIT 2004, Chicago.

(6) F. E. Oggier, G. Rekaya, J.-C. Belfiore and E. Viterbo. "Perfect Space-Time Block Codes". Allerton Conference 2004. Invited paper.

Papers in Refereed Journals

(1) E. Bayer-Fluckiger, F. Oggier, E. Viterbo. "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel", IEEE Transactions on Information Theory, vol. 50, n.4, pp. 702-714, April 2004.

(2) B. D. McKay, F. E. Oggier, G. F. Royle, N. J. A. Sloane, I. M. Wanless and H. S. Wilf. "Acyclic digraphs and eigenvalues of (0,1)-matrices" Journal of Integer Sequences, vol.7, August 2004.

(3) F. E. Oggier, E. Viterbo. "Algebraic number theory and its applications to code design for Rayleigh fading channels", to appear in " Foundations and Trends in Communications and Information Theory".

Submitted Papers

(1) F. E. Oggier, N. J. A. Sloane, S. N. Diggavi and A. R. Calderbank. "Non-intersecting Subspaces Based on Finite Alphabets", submitted to IEEE Transactions on Information Theory , January 2004.

(2) E. Bayer-Fluckiger, F. Oggier, E. Viterbo. "Algebraic lattice constellations: bounds on performance", submitted to IEEE Transactions on Information Theory , April 2004.

(3) F. E. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo."Perfect Space Time Block Codes ", submitted to IEEE Transactions on Information Theory , August 2004.

Invited seminars

(1) "Codes algébriques pour le canal de Rayleigh", November 21 2002, Université Le Mirail, Toulouse, France. Host: Prof. Christian Maire.

(2) "Two problems in coding theory", February 26 2003, Cornell University, NY. Host: Prof. Sergio Servetto.

Research Projects

I) **Design of Codes for Delay-Constrained Communication in Networks.** We are interested in the problem of Multiple Description source coding. We work on a characterization of good codes as the rank-constrained solution of a semidefinite program. This also involves programming a semidefinite solver. (This is joint work with Prof. S. Servetto).

II) **Algebraic lattice codes for channel coding.**

Rotated lattice signal constellations have been proposed as an alternative for transmission over the Rayleigh fading channel. The performance of such modulation schemes depends essentially on two design parameters: the modulation diversity and the minimum product distance. Algebraic lattices, i.e., lattices constructed by the canonical embedding of an algebraic number field, provide an efficient tool for designing such codes, since the design criteria are related to properties of the underlying number field. For example, the maximal diversity is guaranteed when using totally real number fields. Using the notion of *ideal lattice*, we build several infinite families of lattice constellations satisfying a further property of shaping. We are also able to give a bound on the performance of such lattice codes, and we show that with respect to this bound, existing constellations are good enough, in the sense that no significant coding gain can be obtained. (This is joint work with Prof. E. Bayer Fluckiger and Prof. E. Viterbo).

III) **Cyclic Algebras for Coherent Space Time-Coding.**

Cyclic Division algebras for coherent Space-Time Coding have been recently introduced. These non-commutative algebras naturally yields a family of invertible matrices, or in other words, a linear code that fullfills the rank criterion. We further exploit the algebraic structures of cyclic algebras to build Space-Time Block codes that satisfy the following properties: they have full rate, full diversity, non-vanishing constant minimum determinant for increasing spectral efficiency, uniform average transmitted energy per antenna and good shaping. (This is joint work with G. Rekaya , J.-C. Belfiore and E. Viterbo).

IV) **Non-Coherent Space-Time Coding.**

We consider the problem of designing Space-Time Codes in the non-coherent case. Our goal is to construct maximal diversity space-time codewords X, subject to the constraint that the elements of X are taken from a fixed constellation.

Using an interpretation of the well-known pairwise error probability for noncoherent receiver in terms of principal angles between subspaces, we consider the construction of non-intersecting subspaces on finite alphabets. (This is joint work with N.J.A. Sloane and S. Diggavi).