UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Ilha Solteira - SP

CIBELE CRISTINA TRINCA

A CONTRIBUTION TO THE STUDY OF CHANNEL CODING IN WIRELESS COMMUNICATION SYSTEMS

Ilha Solteira
2013

CIBELE CRISTINA TRINCA

A CONTRIBUTION TO THE STUDY OF CHANNEL CODING IN WIRELESS COMMUNICATION SYSTEMS

Tese apresentada à Faculdade de Engenharia do Câmpus de Ilha Solteira - UNESP como parte dos requisitos para obtenção do título de Doutor em Engenharia Elétrica.
Especialidade: Automação.

Prof. Dr. Jozué Vieira Filho
Orientador
Prof. Dr. Edson Donizete de Carvalho
Co-orientador

Ilha Solteira
2013

FICHA CATALOGRÁFICA

Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

Trinca, Cibele Cristina.
T832u A contribuition to the study of channel coding in wireless communication systems / Cibele Cristina Trinca. - Ilha Solteira : [s.n.], 2013
178 f.

Tese (doutorado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de Conhecimento: Automação

Orientador: Jozué Vieira Filho
Co-orientador: Edson Donizete de Carvalho
Inclui bibliografia

1. Cyclotomic felds. 2. Lattice codes. 3. Channel quantization.

unesp **UNIVERSIDADE ESTADUAL PAULISTA**
CAMPUS DE ILHA SOLTEIRA
FACULDADE DE ENGENHARIA DE ILHA SOLTEIRA

CERTIFICADO DE APROVAÇÃO

TÍTULO: A Contribution to the Study of Channel Coding in Wireless Communication Systems

AUTORA: CIBELE CRISTINA TRINCA
ORIENTADOR: Prof. Dr. JOZUE VIEIRA FILHO
CO-ORIENTADOR: Prof. Dr. EDSON DONIZETE DE CARVALHO

Aprovada como parte das exigências para obtenção do Título de DOUTOR EM ENGENHARIA ELÉTRICA , Área: AUTOMAÇÃO, pela Comissão Examinadora:

Prof. Dr. JOZUE VIEIRA FILHO
Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. CARLOS ROBERTO MINUSSI
Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. FRANCISCO VILLARREAL ALVARADO
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. JEAN-CLAUDE BELFIORE
Communications and Electronics / Telecom Paris Tech

Prof. Dr. BARTOLOMEU FERREIRA UCHÔA FILHO
Departamento de Engenharia Elétrica / Universidade Federal de Santa Catarina

Data da realização: 19 de fevereiro de 2013.

I dedicate this work to God and my parents, Eurides Martins Trinca and Nair Queiroz Trinca.

ACKNOWLEDGEMENTS

First of all, I would like to thank God for all the wonderful opportunities that I obtained in my whole life. I learnt a lot during my PhD studying at FEIS (UNESP, campus from Ilha Solteira) and at Télécom ParisTech (Paris-France).

I thank a lot for this great opportunity my advisors, Professor Edson Donizete de Carvalho and Professor Jozué Vieira Filho. Also, I really would like to thank Professor Jean-Claude Belfiore, who collaborated greatly for this work.

I thank greatly my parents, Eurides Martins Trinca and Nair Queiroz Trinca, for the support, love, patience, respect and trust. Unfortunately, my wonderful father is not around us anymore, but he always trusted me and showed me the meaning of the words dignity and persistence.

I thank a lot my whole family, because all of them were present during this stage of my life. They were always encouraging me and guiding me.

I thank greatly all my friends ("miguxos") from FEIS (UNESP-Ilha Solteira) and Télécom ParisTech (Paris-France). They deserve all my respect and admiration, we were always together in good and difficult times.

I also thank all the administrative secretaries from FEIS and Télécom ParisTech for the patience and dedication. I thank greatly, from Télécom ParisTech, the secretaries Zouina and Chantal for all patience, dedication, help and support.

I also would like to thank the jury for accepting to be in the committee.

I thank CAPES, for the funding support.

For all that somehow contributed for the conclusion of this work.

“Any fool can make things bigger, more complex, and more violent. It takes a touch of genius-and a lot of courage-to move in the opposite direction”.

Albert Einstein

“Mais rangez un peu ! Avec le prix qu’on paye, quand même, le minimum c’est qu’il y ait un peu de ménage qui soit fait !”.

Alain Chabat – La Cité de la Peur

RESUMO

Recentemente, códigos perfeitos mínimos e não-mínimos com atraso foram propostos para qualquer canal de dimensão n. A construção destes códigos aparece na literatura como um subconjunto de álgebras de divisão cíclicas sobre $\mathbb{Q}(\xi_3)$ somente para a dimensão $n = 2^s n_1$, onde $s \in \{0,1\}$, n_1 é ímpar e as constelações de sinais são isomorfas a $\mathbb{Z}[\xi_3]^n$. Neste trabalho, revisa-se álgebra de divisão cíclica e propõe-se uma metodologia inovadora para se estender a construção de códigos perfeitos mínimos e não-mínimos com atraso como um subconjunto de álgebras de divisão cíclicas sobre $\mathbb{Q}(\xi_3)$, onde as constelações de sinais são isomorfas ao reticulado rotacionado hexagonal $\mathscr{A}_2^n$, para qualquer canal de qualquer dimensão n tal que $mdc(n,3) = 1$. Também, interferência é geralmente vista como um obstáculo para a comunicação em redes sem fio, portanto desenvolveu-se uma nova metodologia para se quantizar os coeficientes do canal a fim de se realizar o alinhamento de interferência em um reticulado. O modelo de canal usado neste trabalho é o mesmo que o da estratégia compute-and-forward. Nesta nova metodologia, descreve-se uma maneira para se encontrar uma cadeia de partição de reticulados aninhados infinita para qualquer dimensão $n = 2^{r-2}$, onde $r \geq 3$, e faz-se o uso do corpo ciclotômico binário $\mathbb{Q}(\xi_{2^r})$, com $r \geq 3$. Consequentemente, para o caso complexo, desenvolveu-se a generalização para se obter tais cadeias de partição de reticulados aninhados infinitas. Uma metodologia análoga para o caso real também foi desenvolvida. Esta nova metodologia usada para a resolução do problema é original e pode contribuir grandiosamente para a área, ou seja, pode ser muito útil em desenvolvimentos futuros.

Palavras-chave: Corpos ciclotômicos. Códigos reticulados. Quantização de canal.

ABSTRACT

Recently, minimum and non-minimum delay perfect codes were proposed for any channel of dimension n. Their construction appears in the literature as a subset of cyclic division algebras over $\mathbb{Q}(\xi_3)$ only for the dimension $n = 2^s n_1$, where $s \in \{0,1\}$, n_1 is odd and the signal constellations are isomorphic to $\mathbb{Z}[\xi_3]^n$. In this work, we review the cyclic division algebra and we propose an innovative methodology to extend the construction of minimum and non-minimum delay perfect codes as a subset of cyclic division algebras over $\mathbb{Q}(\xi_3)$, where the signal constellations are isomorphic to the hexagonal $\mathscr{A}_2^n$ -rotated lattice, for any channel of any dimension n such that $gcd(n,3) = 1$. Also, interference is usually viewed as an obstacle to communication in wireless networks, so we developed a new methodology to quantize the channel coefficients in order to realize interference alignment onto a lattice. Our channel model is the same from the compute-and-forward strategy. In this new methodology, we have described a way to find an infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$, and we made use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, with $r \geq 3$. Thus, for the complex case, we developed the generalization to obtain such infinite nested lattice partition chains and we also developed a methodology for the real case. This new methodology used to solve the problem is original and can contributes greatly to the area, that is, it can be very useful in future developments.

Keywords: Cyclotomic fields. Lattice codes. Channel quantization.

LIST OF FIGURES

SYMBOLS AND ABBREVIATIONS

$AWGN$	Additive White Gaussian Noise
$MMSE$	Minimum Mean Square Error
QAM	Quadrature Amplitude Modulation
HEX	Hexagonal
$STBC$	Space-Time Block Code
$MIMO$	Multiple Input Multiple Output
SNR	Signal-to-Noise Ratio
$i.i.d.$	Independent and identically distributed

LIST OF SYMBOLS

$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of integer numbers
$\mathbb{Q}$	Set of rational numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers
$\mathbb{N}^*$	Set of nonzero natural numbers
$\partial(f(X))$	Degree of the polynomial $f(X)$
L, M, K	Number fields
L/K	Field extension
$[L/K]$	Degree of L/K
Π	Product
Σ	Sum
$Det(A)$	Determinant of A
O_K	Ring of integers of K
$\# X$	Cardinality of the set X
$\phi(n)$	Euler function for the integer n
$A[X]$	Ring of the polynomials over A in X
ξ^n	Primitive n-th root of unity
d_K	Absolute discriminant of the field K
$Tr_{L/K}$	Trace related to the extension L/K
$N_{L/K}$	Norm related to the extension L/K
$Gal(L/K)$	Galois group of L/K
Λ	Lattice
$V(\Lambda)$	Volume of the lattice Λ
$div(\Lambda)$	Diversity of the lattice Λ
$d_p(x)$	Product distance of x from the origin
$d_{p,min}(\Lambda)$	Minimum product distance of the lattice Λ
Λ^c	Complex lattice
z_m	i.i.d. circularly symmetric complex gaussian noise
$\oplus$	Direct sum

PRESENTATION

This work was motivated by the studies of the Professors Edson Donizete de Carvalho and Jozué Vieira Filho, who is working in cooperation. The initial idea was to work only with Space-Time Codes, the studies related to space-time codes followed up to arise the opportunity of realizing a sandwich stage.

After obtaining a contact with Professor Jean-Claude Belfiore and the confirmation of realizing the stage with him, we established a cooperation that allowed us to continue the work at Télécom ParisTech (Paris-France) on the same line of research, but without restricting new ideas.

Thus, in april/2011 the works started being realized in France. After discussing with Professor Jean-Claude about the work that also would be developed with him, it was decided to study noisy channel models with the support of the algebraic number theory.

In the end, we obtained a work that contributes greatly to the area of channel coding, so it was shown that the collaboration UNESP-Télécom ParisTech via the sandwich doctorate was successful.

CONTENTS

1 INTRODUCTION

Wireless communications appeared in 1897, when Guglielmo Marconi demonstrated the ability to provide radio contact with ships that sailed over the English Channel. During the next hundred years, wireless communications have undergone a remarkable evolution, from the emergence of communication systems AM and FM until the development of cellular systems of last generation. The use of wireless communications has found its largest increase in the last ten years, during which new methods have been introduced and new appliances were invented. Currently, every day of our lives we are surrounded by wireless devices and computing systems: cell phone, wireless INTERNET, walkie-talkie, etc. The ultimate goal of wireless communications is to allow people to communicate from anywhere, anytime, with anyone.

With the increase in applications with wireless communications, the demand for bandwidth or transmission capacity has increased considerably, but there are still basic constraints of power and complexity of systems. This means that no one can increase the capacity by simply increasing the transmitted power. The current communication systems are predominantly systems with a single antenna. Due to multipath propagation in wireless channels, the capacity of a single wireless channel can be very low. Researches in this area have enabled more efficient use of this limited capacity and achieved exceptional progresses. The challenge is to reduce the error rate, which can be significant in systems based on a single antenna.

New communication systems that are superior in capacity and lower error rate should occur based on new communication theories that exploit multiple antennas.

Recently emerged the digital communication systems that use wireless connections with multiple input and multiple output (MIMO), that is, that use multiple antennas at the transmitter and receiver. This is one of the most significant techniques developed recently in modern communications. The main characteristic of a system with multiple antennas is its ability to make multiple propagation paths, which is traditionally considered as a disadvantage for wireless communications, however beneficial to the users.

In 1996 and 1999, Foschini and Telatar proved in (FOSCHINI, 1996) and (TELATAR, 1999) that communication systems with multiple antennas have a much greater capacity than systems with single antenna. They showed that the improved capacity is almost linear to the number of transmit antennas and the number of receiving antennas, which is smaller. This result indicated the superiority of systems with multiple antennas and promoted the great interest in this area.

In this work, we make use of rotated lattices constructed through extension fields to construct perfect codes from cyclic division algebras over $\mathbb{Q}(\xi_3)$ for the family of dimension n, where n is any even degree such that 3 does not divide n, and develop a new methodology to perform the channel approximation in order to realize interference alignment onto a lattice.

Over the last years new coding techniques have been proposed to combat fading effects in wireless communication channels. Most of them have been proposed by considering multiple-input and multiple-output (MIMO) channels. The main goal is to maximize the spectral efficiency by using diversity techniques, in which the same information is transmitted over different and independent channels.

These techniques increase the diversity gain and the probability that, at least, one copy of the original information will arrive to the receiver. As a consequence, data rate and channel performance are improved with no extra cost of spectrum. The advantage of the systems based on multiple antennas (or multiple channels) arises because of the ability of exploiting the multiple-path propagation to the benefit of the users, where the multiple-path propagation is traditionally considered a disadvantage to the wireless communication channels.

A MIMO channel with n_t transmit and n_r receive antennas is modeled by the following matrix equation

$$Y_{n_r \times l} = H_{n_r \times n_t} X_{n_t \times l} + W_{n_r \times l}, \tag{1}$$

where $Y_{n_r \times l}$ is the receive matrix over l channels, $X_{n_t \times l}$ is the transmit matrix, $H_{n_r \times n_t}$ is the channel matrix and $W_{n_r \times l}$ is the additive noise matrix, the subscripts denote the dimension of the matrices. The entries of the matrices $H_{n_r \times n_t}$ and $W_{n_r \times l}$ are independent and Gaussian distributed. The set $\mathscr{C}$ of all transmit codewords $X_{n_t \times l}$ form a STBC. We focus on square STBCs, that is, space-time codes $\mathscr{C}$ with $l = n_t$, and we will use the symbol $n = n_t = l$ to denote the common dimension.

A STBC is called a *linear dispersion code* (HASSIBI; HOCHWALD, 2002) over a constellation $\mathscr{U}$ if every code matrix X has a unique expansion as it follows

$$X = \sum_{k=1}^{K} a_k \Lambda_k, \ a_k \in \mathscr{U}, \tag{2}$$

where the matrices Λ_k are fixed, independent of the message and every matrix of the form on the right is a code matrix. A linear dispersion code (HASSIBI; HOCHWALD, 2002) over a constellation $\mathscr{U}$ is said to be *full-rate* over the constellation $\mathscr{U}$ if $K = n^2$.

Division algebras have been proposed by (OGGIER et al., 2006; SETHURAMAN; RAJAN; SHASHIDHAR, 2003; BELFIORE; REKAYA; VITERBO, 2005; HOLLANTI et al., 2009) as a new tool for constructing STBCs, since they are non-commutative algebras that naturally yield

linear fully diverse codes. However, the determination of these algebras is a nontrivial problem.

Several works (BELFIORE; REKAYA; VITERBO, 2005; KIRAN; RAJAN, 2005; ELIA; SETHURAMAN; KUMAR, 2007; HOLLANTI et al., 2009; OGGIER et al., 2006) have considered the case of adaptive modulation schemes that requires the transmission of different sizes of constellation. It is very important that the coding gain does not depend on the constellation size. It is necessary that the STBCs satisfy the property of *non-vanishing determinant*, that is, the property that the set of all determinants associated to each code matrix of the code $\mathscr{C}$ forms a discrete subset of the complex number $\mathbb{C}$.

We will focus only on signals based on *QAM* or *HEX* constellation. We consider *QAM* signal constellations identified by the elements of the *Gaussian integers* $\mathbb{Z}[i]$, that is, the integer ring of the number field $F = \mathbb{Q}(i)$. Similarly, we consider *HEX* signal constellations identified by the elements of the *Eisenstein integers* $\mathbb{Z}[\xi_3]$, that is, the integer ring of the number field $F = \mathbb{Q}(\xi_3)$, where ξ_3 is a third root of unity.

Perfect codes form the class of STBCs, whose construction is based on cyclic division algebras and vectorized code matrices such that they are associated to the cubic lattices in $2n$-dimensional Euclidean space. Algebraically, it is equivalent to consider $\mathbb{Z}[i]^n$ or $\mathscr{A}_2^n$-rotated lattices. In the context of STBCs, the Golden code (BELFIORE; REKAYA; VITERBO, 2005; DAYAL; VARANASI, 2003) was the first perfect code found.

In (OGGIER et al., 2006) perfect codes have been built algebraically by using cyclic division algebras and their existence is shown in dimensions $2,4$ and $3,6$. The considered codes are subsets of cyclic division algebras over the number fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\xi_3)$, respectively.

(ELIA; SETHURAMAN; KUMAR, 2007) generalized the procedure of the construction of perfect codes and showed their existence for any dimension when the considered codes are subsets of cyclic division algebras over the number field $\mathbb{Q}(i)$. However, in (ELIA; SETHURAMAN; KUMAR, 2007), the authors proposed a construction of perfect codes from cyclic division algebras over the number field $\mathbb{Q}(\xi_3)$ only for the dimension $n = 2^s n_1$, with $s \in \{0,1\}$ and n_1 is odd. For doing such a generalization we have the concept of perfect space-time codes that was introduced in (OGGIER et al., 2006) by the following definition:

Definition 1. (OGGIER et al., 2006) *A square $n_t \times n_t$ STBC is called a perfect code if and only if*

1. *the code is a full-rate linear dispersion code, where the $(n_t l)$ coefficients that representing the message symbols are drawn from the QAM or HEX constellations;*
2. *for every pair X_1, X_2 of distinct code matrices, the determinant $det(\Delta X \Delta X^t)$, where $\Delta X = X_1 - X_2$, prior to SNR normalization, is lower bounded by a constant that is greater than zero and independent of the code size;*

3. *the energy required to send the linear combination of the information symbols on each layer is similar to the energy used for sending the symbols themselves (we do not increase the energy of the system in encoding the information symbols);*

4. *it induces uniform average transmitted energy per antenna in all l time slots, i.e., all the coded symbols in the code matrix have the same average energy.*

On the constructions of perfect codes in (ELIA; SETHURAMAN; KUMAR, 2007), the authors meet the property (3) by ensuring that the signalling set, obtained by the code matrix vectorization, is isometric to either QAM^{n^2} (isomorphic to the $\mathbb{Z}[i]^n$-rotated lattice) or HEX^{n^2} (isomorphic to the $\mathscr{A}_2^n$-rotated lattice). The procedure of the construction of perfect codes in (ELIA; SETHURAMAN; KUMAR, 2007) is a consequence of the existence of $\mathbb{Z}^n$-rotated lattices (BAYER-FLUCKIGER; OGGIER; VITERBO, 2004) from cyclic extensions of $\mathbb{Q}$ with odd degree n.

Also, Andrade and Carvalho (ANDRADE; CARVALHO, 2011) presented cyclic constructions of full diversity rotated $\mathbb{Z}^n$-lattice constellations based on algebraic number theory constructions using the theory of ideal lattices (BAYER-FLUCKIGER; OGGIER; VITERBO, 2006), where n is any dimension. These rotated lattices were constructed through cyclic extension fields of prime degree based on cyclotomic fields (WASHINGTON, 1997).

So, in (TRINCA et al., 2012), we extended the procedure of the construction of perfect codes from cyclic division algebras over $\mathbb{Q}(\xi_3)$ for the family of dimension n, where n is any even degree such that 3 does not divide n.

In a wireless network, a transmission from a single node is heard not only by the intended receiver, but also by all other nearby nodes; by analogy, any receiver not only captures the signal from its designated transmitter, but from all other nearby transmitters. The resulting interference is usually viewed as highly undesirable and clever algorithms and protocols have been devised to avoid interference between transmitters.

Although interference is usually viewed as an obstacle to communication in wireless networks, in (NAZER; GASTPAR, 2011) the authors proposed a new strategy called *compute-and-forward*, which exploits interference to obtain significantly higher rates between users in a network.

The idea is that compute-and-forward enables relays to decode linear equations of the transmitted messages using the noisy linear combinations provided by the channel, that is, they do not ignore the interference as a noise. After the relays decode these linear equations, they simply send them to the destinations, which given enough equations, can recover their desired messages. The strategy is based on nested lattice codes, which are codes with a linear structure. Such structure ensures that integer combinations of codewords can be decoded reliably.

Each relay, indexed by $m = 1, 2, \ldots, M$, observes a noisy linear combination of the transmitted signals through the channel,

$$y_m = \sum_{l=1}^{L} h_{ml} x_l + z_m, \tag{3}$$

where $h_{ml} \in \mathbb{C}$ are complex-valued channel coefficients, $x_l \in \mathbb{C}^n$ such that $\|x_l\|^2 \leq nP$ (in (NAZER; GASTPAR, 2011), Appendix C, they argue that there exist fixed dithers that meet the power constraint) and z_m is i.i.d. circularly symmetric complex Gaussian noise, $z_m \sim \mathscr{CN}(\mathbf{0}, \mathbf{I}^{M \times M})$. Let $h_m = [h_{m1} \cdots h_{mL}]^T$ denote the vector of channel coefficients to relay m and let $H = \{h_{ml}\}$ denote the entire channel matrix, where T denotes the transpose. Note that by this convention the m^{th} row of H is h_m^T.

The coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself. Specifically, relay m only needs to know h_m. Each transmitter only needs to know the desired message rate, not the realization of the channel.

However, in (NAZER; GASTPAR, 2011) we also have an equivalent channel induced by the modulo-Λ transformation. In this "virtual" channel model each relay observes a $\mathbb{Z}[i]$-combination $\sum a_{ml} t_l$ of the lattice points corrupted by effective noise $z_{eq,m}$, that is,

$$y_m = \sum_{l=1}^{L} a_{ml} t_l + z_{eq,m}. \tag{4}$$

Transmitters send messages that take values in a prime-sized finite field and relays recover linear equations of the messages over the same field, thus we have and ideal physical layer interface for network coding. Even if the transmitters lack channel state information, this scheme can be applied.

The relaying strategy of the compute-and-forward is applicable to any configuration of sources, relays and destinations that are linked through linear channels with additive white Gaussian noise (AWGN). We refer to such configurations as AWGN networks.

There is a great number of works based on lattice codes and their applications in communications. It is not possible to discuss all of them here, but the reference (ZAMIR, ITA, 2009) is a great indication for the interested reader. The basic insight is that nested lattice codes can approach, for a great amount of AWGN networks of interest, the performance of standard random coding arguments.

An important result by Erez and Zamir showed that nested lattice codes, combined with lattice decoding, can achieve the capacity of the point-to-point AWGN channel (EREZ; ZAMIR, 2004). They showed that capacity may also be achieved by using nested lattice codes, the coarse lattice serving for shaping via the modulo-lattice transformation, the fine lattice for channel

coding. (EREZ; ZAMIR, 2004) also showed that such pairs exist for any desired nesting ratio, i.e., for any signal-to-noise ratio (SNR). Furthermore, for the modulo-lattice additive noise channel lattice decoding is optimal.

So we developed a new methodology to quantize the channel coefficients in order to realize interference alignment onto a lattice. Our channel model is the same from the compute-and-forward strategy, given by the equation (4).

In this new methodology, we have described a way to find an infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$, and we made use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, with $r \geq 3$, $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{(r-1)}$, where ϕ is the Euler function, and $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$. So we developed, for the complex case, the generalization to obtain such infinite nested lattice partition chains. We also developed a methodology for the real case.

After that, by using the MMSE criterion, we showed, in a probabilistic sense, that the error between the desired quantity and our estimate of it goes to zero, when n goes to the infinity.

The generalization to obtain these infinite nested lattice partition chains shows us the construction A of the corresponding lattices of each infinite nested lattice partition chain.

With this new methodology, for further work, we want to obtain the distributed computation, that is, the non-linearity for the compute-and-forward strategy and, at the same time, we want to achieve the AWGN channel capacity. For that, the goal is to find finite number fields that give us right commutative orders, i.e., by using the Minkowski embedding we want to associate such commutative orders with the lattices in (EREZ; ZAMIR, 2004), where we can obtain the AWGN channel capacity. Since orders are rings, we have the multiplication operation and, by using the Minkowski embedding, we can associate the multiplication of two elements that belong to the commutative order with an element of the lattice. So we can perform the non-linearity for the compute-and-forward strategy.

Also, we can apply this new methodology in communication interference (JAFARIAN; VISHWANATH, 2012). The compute-and-forward strategy (NAZER; GASTPAR, 2011) and the communication interference are related to the communications engineering. This methodology applied in communication interference should hold a precoder and the respective precoding is given as it follows: each channel coefficient is approximated to a generator of an ideal, suppose $(1+\xi_{2^r})^k$, where $r \geq 3$ and $k \geq 0$. So we will make use of the residue operation, that is, we make k modulo $n = 2^{r-2}$, thus we have $k = 1, 2, 3, \ldots, n-1$. We know that each channel coefficient h is approximated to a diagonal matrix, so when k is a multiple of n, we have that h is directly approximated because the set of the elements of such a matrix is the same. When $k = 1, 2, \ldots, n-1$, suppose that the best approximation for h is $\sigma_i(\mu)^k$, which is one of the elements of the diagonal matrix, where $\mu = 1+\xi_{2^r}$ and $i = 1, 2, \ldots, n$. Therefore $\frac{n}{2}$ bits will send

to the transmitter the information that $k \neq n$ and so for all the other elements of such a matrix, each of them will be multiplied by $\sigma_i(\mu)^k$ divided by itself.

Another possible application is related to the computer science, it might be possible to apply the theory developed in this work in homomorphic encryption schemes.

Therefore, this work was organized specifically as it follows: in chapter 1, we present basic concepts and results from the lattice and algebraic number theory and the goal of this chapter is to provide the theoretical basis for the development of the work.

In chapter 2, the authors in (ELIA; SETHURAMAN; KUMAR, 2007) proposed a construction of perfect codes from cyclic division algebras over the number field $\mathbb{Q}(\xi_3)$ only for the dimension $n = 2^s n_1$, with $s \in \{0,1\}$ and n_1 is odd. Also, Andrade and Carvalho (ANDRADE; CARVALHO, 2011) presented cyclic constructions of full diversity rotated $\mathbb{Z}^n$-lattice constellations based on algebraic number theory constructions using the theory of ideal lattices (BAYER-FLUCKIGER; OGGIER; VITERBO, 2006), where n is any dimension. These rotated lattices were constructed through cyclic extension field of prime degree based on cyclotomic fields (WASHINGTON, 1997).

Thus, we extend the procedure of the construction of perfect codes from cyclic division algebras over $\mathbb{Q}(\xi_3)$ for the family of dimension n, where n is any even degree such that 3 does not divide n.

In chapter 3, we develop a new methodology to quantize the channel coefficients in (4) in order to realize interference alignment onto a lattice. In this chapter, we explain two examples of channel quantization, these examples are related to the dimensions 4 and 8 (real) or 2 and 4 (complex) and we make use of the binary cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{16})$, respectively.

In this new methodology, we describe a way to find an infinite nested lattice partition chain for the dimensions 4 and 8 (real) or 2 and 4 (complex).

In chapter 4, this new methodology is generalized for any dimension $n = 2^{r-2}$, where $r \geq 3$. In this chapter, we describe a way to find an infinite nested lattice partition chain, for any $r \geq 3$, in order to quantize the channel coefficients. For that, we make use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, with $r \geq 3$, $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{(r-1)}$, where ϕ is the Euler function, and $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$.

In chapter 5, we suppose that our interference channel is real-valued, specifically $a_{ml} \in \mathbb{R}$ in (4), and we describe a way to find an infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$, in order to quantize the channel coefficients. For that, we make use of the maximal real subfield K of $L = \mathbb{Q}(\xi_{2^r})$, where $r \geq 3$, $\xi = \xi_{2^r}$ is the 2^r-th root of unity and $K = \mathbb{Q}(\theta)$, with $\theta = \xi + \xi^{-1}$.

In this chapter, we have a program that gives us, for each $r \geq 3$, a nested lattice partition

chain, which is extended by periodicity so that it is a doubly infinite chain. This program presents the generator and Gram matrices of the lattices in each nested lattice partition chain. We can observe that each nested lattice partition chain is extended by periodicity and such a periodicity is equal to $n = 2^{r-2}$.

In chapter 6, we introduce an error criterion that measures, in a probabilistic sense, the error between the desired quantity and our estimate of it. In this chapter, we focus on choosing our estimate to minimize the expected or mean value of the square of the error, referred to as a minimum mean-square-error (MMSE) criterion.

Thus, in this chapter, for the case $a_{ml} \in \mathbb{R}$ and $n = 1$ or $n = 2^{r-2}$ ($r \geq 3$), we minimize the expected or mean value of the square of the error, referred to as a minimum mean-square-error (MMSE) criterion. But we can also observe that the theory developed in chapter 6 is analogous to the complex case.

In chapter 7, we present the construction of nested lattices from ideals via binary cyclotomic fields. We show the construction A of these nested lattices and, in this case, the linear codes associated to this construction are cyclic codes. So we observe that nested lattices from ideals via binary cyclotomic fields can also be obtained from the construction A, whose the associated codes, in this case, are cyclic codes.

We also show, in chapter 7, that the dense lattices D_4 and E_8 can be constructed from ideals via the cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{24})$, respectively. We explain the construction A of the lattice E_8 and, in this case, the linear code associated to this construction is a negacyclic code called Tetracode.

This work had a grand collaboration of the Professor Jean-Claude Belfiore, who is associated to the university Télécom ParisTech (Paris-France).

2 BACKGROUND ON LATTICE AND ALGEBRAIC NUMBER THEORY

2.1 Introduction

In this chapter, we present basic concepts and results from the lattice and algebraic number theory. We will also introduce cyclotomic fields and decomposition of prime ideals.

The goal of this chapter is to provide the theoretical basis for the development of the work. By assuming more general backgrounds, we will leave out the proofs and we will cite the sources where we can find them. In this way, we tried to make a concise work.

Works which contain on a complementary way the topics presented here are, for instance, (STEWART; TALL, 2002; FORNEY, 1988; OGGIER, 2005).

This chapter will present two sections, the first one is related to the algebraic number theory and the last one is related to the lattice theory.

2.2 Background on Algebraic Number Theory

This section introduces, on a concise way, basic concepts and results from the algebraic number theory, which are necessary for this work.

In this work, by using the algebraic number theory, we construct perfect codes from cyclic division algebras over $\mathbb{Q}(\xi_3)$ and develop a new methodology to perform the channel approximation in order to realize interference alignment onto a lattice.

Let K and L be subfields of the complex numbers $\mathbb{C}$. We say that L is an extension of K, or that L/K is a *field extension*, if K is a subfield of L.

The dimension of the K-space L is denoted by $[L:K]$ and is called the *degree* of L/K. We say that L/K is a *finite extension* if $[L:K] < \infty$.

Let L/K be a field extension and $\alpha \in L$. If there exists a monic irreducible polynomial $f(X) \in (K[X] - \{0\})$ such that $f(\alpha) = 0$, we say that α is an *algebraic number* over K. Such a polynomial is called *minimal polynomial* of α over K.

We say that an extension L of K is an *algebraic extension* if all element $\alpha \in L$ is a root of some non-zero polynomial $f \in K[X]$.

The set of the algebraic numbers of K over $\mathbb{Q}$ is a ring, called the *ring of algebraic integers* of K, and is denoted by O_K.

Let K and O_K be a finite extension of $\mathbb{Q}$ and the ring of algebraic integers of K, respectively, we have that O_K is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$, whose basis is called *integral basis*.

A *number field* is a finite extension of $\mathbb{Q}$. If the dimension of K as a vector $\mathbb{Q}$-space is n, we say that K is a number field of degree n.

Every number field K has the form $K = \mathbb{Q}(\theta)$, for some algebraic number $\theta \in K$. So K is a vector $\mathbb{Q}$-space generated by powers of θ. If K has degree n, then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of K and the degree of the minimal polynomial of θ over $\mathbb{Q}$ is n, that is, $\partial(f(X)) = n$.

If the minimal polynomial of θ over $\mathbb{Q}$ has all your roots in K, we say that K is a *Galois extension* of $\mathbb{Q}$. The set of the automorphisms of the field $Gal(K/\mathbb{Q}) = \{\sigma : K \to K \mid \sigma(x) = x,\ \forall x \in \mathbb{Q}\}$ is a group, called *Galois group* of K over $\mathbb{Q}$. If the Galois group is Abelian (cyclic), the Galois extension is called Abelian (cyclic).

Definition 2. *Let K and L be two extensions of a field E. A field homomorphism $\varphi : K \to L$ is said to be a E-homomorphism if for all $a \in E$ we have $\varphi(a) = a$ (that is, $\varphi|_E$ is the identity of E).*

Remark 1. *All homomorphism $\varphi : K \to L$ of subfields of $\mathbb{C}$ is a $\mathbb{Q}$-homomorphism and if φ is injective we can call it embedding.*

The next theorem is related to an homomorphism between such fields.

Theorem 1. (SAMUEL, 2008) *Let K and L be subfields of $\mathbb{C}$, where L is an extension of K and $[L:K] = n < \infty$. Then exists $\theta \in L$ such that $L = K(\theta)$ and exist exactly n K-homomorphisms $\sigma_i : L \to \mathbb{C}$, $i = 1, \ldots, n$, such that $\sigma_i(\theta) = \theta_i$, where θ_i are the distinct roots in $\mathbb{C}$ of the minimal polynomial of θ over K.*

If we take $\theta = \theta_1$, we can note that $\sigma_1(\theta) = \theta_1 = \theta$, so σ_1 is the identity map $\sigma_1(l) = l$, for all $l \in L$. When we apply the embedding σ_i to an arbitrary element $x \in L$, $x = \sum_{k=1}^{n} a_k \theta^k$, $a_k \in K$, using the K-homomorphism properties, we have

$$\sigma_i(x) = \sigma_i(\sum_{k=1}^{n} a_k \theta^k) = \sum_{k=1}^{n} \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^{n} a_k \theta_i^k \in \mathbb{C}$$

and the image of x over σ_i is univocally identified by θ_i.

The elements $\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)$ are called the *K-conjugated* of x and

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x) \text{ and } Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

are called, respectively, *norm* and *trace* of x of the extension L/K.

Let $K \subset L$ be fields. Let $[L:K] = n$, $x, y \in L$ and $a \in K$. Then we have the following properties:

1. $Tr_{L/K}(x+y) = Tr_{L/K}(x) + Tr_{L/K}(y)$;
2. $Tr_{L/K}(ax) = aTr_{L/K}(x)$;
3. $Tr_{L/K}(a) = na$;
4. $N_{L/K}(xy) = N_{L/K}(x) \cdot N_{L/K}(y)$;
5. $N_{L/K}(a) = a^n$.

In case that $K \subseteq L \subseteq M$, given $x \in M$, we have:

1. $Tr_{M/K}(x) = Tr_{L/K}(Tr_{M/L}(x))$;
2. $N_{M/K}(x) = N_{L/K}(N_{M/L}(x))$.

In particular, if $x \in L$, then

1. $Tr_{M/K}(x) = [M:L]Tr_{L/K}(x)$;
2. $N_{M/K}(x) = N_{L/K}(x)^{[M:L]}$.

Lemma 1. (ESMONDE; MURTY, 2005) *For all $x \in K$, we have $N(x)$ and $Tr(x) \in \mathbb{Q}$. If $x \in O_K$, we have $N(x)$ and $Tr(x) \in \mathbb{Z}$.*

Definition 3. *Let $\{w_1, \ldots, w_n\}$ be an integral basis of O_K. The discriminant of K is defined as $d_K = Det[\sigma_j(w_i)]^2$, where $i, j = 1, 2, \ldots, n$.*

Remark 2. *The discriminant is independent of the choice of the basis.*

Let m and n be the degrees of the extensions K and L over $\mathbb{Q}$, respectively, and let $d = mdc(d_K, d_L)$, where d_K and d_L are the discriminants of K and L, respectively.

Theorem 2. (MARCUS, 1977) *If $[KL:\mathbb{Q}] = mn$, then $O_{KL} \subset \frac{1}{d} O_K O_L$, where KL is the composition of the fields K and L and $KL/\mathbb{Q}$ is the corresponding composite extension.*

Corollary 1. (MARCUS, 1977) *If $[KL:\mathbb{Q}] = mn$ and $d = 1$, then $O_{KL} = O_K O_L$, where KL is the composition of the fields K and L and $KL/\mathbb{Q}$ is the corresponding composite extension.*

Example 1. *Consider the set of rational numbers $\mathbb{Q}$, which is easily checked to be a field. Other fields can be built starting from $\mathbb{Q}$. Take, for example, the element i such that $i^2 = -1$, which is not an element of $\mathbb{Q}$. One can build a new field by "adding" i to $\mathbb{Q}$. In the same way i is added to $\mathbb{R}$ to create $\mathbb{C}$. Note that, in order to make this new set a field, we have to add all the multiples and powers of i. We thus get a new field that contains both $\mathbb{Q}$ and i, and only $\mathbb{Q}$- linear combination of i, that we denote it by $\mathbb{Q}(i)$. We call it a field extension of $\mathbb{Q}$. Note that we can iterate this procedure and start with the field $\mathbb{Q}(i)$. Then, by adding, for example, the element $\sqrt{5}$ (which does not belong to $\mathbb{Q}(i)$), its multiples and powers, we get a new field, denoted by $\mathbb{Q}(i,\sqrt{5})$. Thus $\mathbb{Q}(i,\sqrt{5})$ is an extension of $\mathbb{Q}(i)$, which is itself an extension of $\mathbb{Q}$.*

It is useful to note that if L/K is a field extension, then L has a natural structure of vector space over K, where vector addition is addition in L and scalar multiplication of $a \in K$ on $v \in L$ is just $av \in L$. For example, an element $x \in \mathbb{Q}(i)$ can be written as $x = a + ib$, where $\{1, i\}$ are the basis "vectors" and $a, b \in \mathbb{Q}$ are the scalars. The dimension of $\mathbb{Q}(i)$ as vector space over $\mathbb{Q}$ is 2. Similarly, an element of $\mathbb{Q}(i,\sqrt{5})$ can be written as $w = x + y\sqrt{5}$, with $x, y \in \mathbb{Q}(i)$, or also as $w = (a+ib) + \sqrt{5}(c+id)$, where $a, b, c, d \in \mathbb{Q}$. Thus, $\mathbb{Q}(i,\sqrt{5})$ is a vector space of dimension 2 over $\mathbb{Q}(i)$, or of dimension 4 over $\mathbb{Q}$.

In our example, the polynomial $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$. The number i is algebraic over $\mathbb{Q}$. Similarly, $x^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(i)$.

Consider $\mathbb{Q}(i,\sqrt{5})$ a field extension of degree 2 of $\mathbb{Q}(i)$. It can be defined, as already pointed out, by the polynomial $x^2 - 5$ over $\mathbb{Q}(i)$. Since $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$, both $\pm\sqrt{5} \in \mathbb{Q}(i,\sqrt{5})$, and we can define two automorphisms of $\mathbb{Q}(i,\sqrt{5})$ as it follows: let $a, b \in \mathbb{Q}(i)$,

$$\sigma_1 : \mathbb{Q}(i,\sqrt{5}) \to \mathbb{C}, \text{ where } \sigma_1(a + b\sqrt{5}) = a + b\sqrt{5}$$

and

$$\sigma_2 : \mathbb{Q}(i,\sqrt{5}) \to \mathbb{C}, \text{ where } \sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}.$$

So notice that σ_1 and σ_2 are $\mathbb{Q}(i)$-automorphisms of $\mathbb{Q}(i,\sqrt{5})$, that is, they satisfy $\sigma_j(x) = x$, $j = 1, 2$, for all $x \in \mathbb{Q}(i)$.

2.2.1 Cyclotomic fields

A very important class of the number fields is the class of the cyclotomic fields. Our goal in this section is to present the ring of the algebraic integers, the integral basis and the discriminant of the cyclotomic fields.

An element $\xi \in \mathbb{C}$ is called an n-th root of unity if $\xi^n = 1$, $n \geq 1$ an integer, and is called

a primitive n-th root of unity if $\xi^n = 1$, but $\xi^d \neq 1$, for $1 \leq d < n$. The n-th roots of unity are roots of the polynomial $x^n - 1$.

The complex number ξ^m is a primitive n-th root of unity if, and only if, $mdc(m,n) = 1$, that is, the number of primitive n-th roots of unity is given by

$$\phi(n) = \#\{0 < m < n \mid mdc(m,n) = 1,\ m \in \mathbb{Z}\},$$

where ϕ is the Euler function.

Definition 4. *We say that L is the n-th cyclotomic field if L is the result of the addition of $\mathbb{Q}$ and a primitive n-th root of unity, $L = \mathbb{Q}(\xi_n)$.*

As $L = \mathbb{Q}(\xi_n)$, where ξ_n is a primitive n-th root of unity, we have $[L : \mathbb{Q}] = \phi(n)$.

Theorem 3. (MARCUS, 1977) *The ring of integers of $L = \mathbb{Q}(\xi_n)$ is $O_L = \mathbb{Z}[\xi_n]$ and*

$$\{1, \xi_n, \ldots, \xi_n^{\phi(n)-1}\}$$

is an integral basis of O_L.

Theorem 4. (ENDLER, 2006) *Let $\xi_n \in \mathbb{C}$ be a primitive n-th root of unity. Then $L = \mathbb{Q}(\xi_n)$ is a Galois extension of $\mathbb{Q}$, whose Galois group $Aut(L/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}_n)^*$, so is abelian with order $\phi(n)$.*

Then we have the isomorphism $Aut(L/\mathbb{Q}) \simeq (\mathbb{Z}_n)^*$. It is clear that $(\mathbb{Z}_n)^*$ is abelian, but it is not always cyclic. We have that $(\mathbb{Z}_n)^*$ is cyclic if, and only if, $n = 2, 4, p^r$ or $2p^r$, where p is an odd prime and $r \geq 1$.

The Galois group $Aut(L/\mathbb{Q})$ consists of $\phi(n)$ automorphisms σ_j, where $mdc(j,n) = 1$, $j = 1, \ldots, \phi(n)$, and σ_j is univocally determined by $\sigma_j(\xi_n) = \xi_n^j$; in particular, σ_1 is the identity of L.

Let L be a field, the subfield of L fixed point-to-point by the complex conjugation is called the *maximal real subfield* of L.

Proposition 1. (JESUS, 2007) *Let $L = \mathbb{Q}(\xi_n)$, where ξ_n is a primitive n-th root of unity, we have*

1. *$K = \mathbb{Q}(\alpha)$, $\alpha = \xi_n + \xi_n^{-1}$, is the maximal real subfield of L;*
2. *The ring of algebraic integers of K is $\mathbb{Z}[\alpha]$;*
3. *$1, \alpha, \ldots, \alpha^{\frac{\phi(n)}{2}-1}$ form an integral basis of K.*

An outcome involving cyclotomic fields and the concept of abelian number fields due to Kronecker and Weber is the following:

Theorem 5. (JESUS, 2007) *Let K be a finite and abelian extension of the rational numbers (that is, a Galois extension with abelian Galois group). Then K is contained in some cyclotomic field.*

The main invariant of the algebraic number fields is characterized on the cyclotomic fields by the following theorem:

Theorem 6. (WASHINGTON, 1997) *The discriminant of $L = \mathbb{Q}(\xi_n)$ over $\mathbb{Q}$ is given by*

$$d_L = d_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(1, \xi_n, \ldots, \xi_n^{\phi(n)-1}) = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

As a consequence, we have

1. if $n = p$, then $d_L = (-1)^{\frac{(p-1)}{2}} p^{(p-2)}$;
2. if $n = p^r$, then $d_L = (-1)^{\frac{(p-1)p^{r-1}}{2}} p^{p^{r-1}(r(p-1)-1)}$, where r is a positive integer.

Theorem 7. (JESUS, 2007) *The discriminant of $K = \mathbb{Q}(\xi_n + \xi_n^{-1})$ over $\mathbb{Q}$ is given by:*

1. $d_K = p^{\frac{(p-3)}{2}}$, *if* $n = p \geq 5$;
2. $d_K = 2^{(r-1)2^{r-2}-1}$, *if* $n = 2^r$;
3. $d_K = p^{\frac{(r+1)(p-1)p^{r-1}-p^r-1}{2}}$, *if* $n = p^r$, $p \neq 2$, $r > 1$.

Now let $\mathbb{Q}(\xi)$, where $\xi = \xi_{2^r}$. We have the following important results:

Proposition 2. (OGGIER, 2005) *We have that $O_L = \mathbb{Z}[\xi]$ is a free $\mathbb{Z}[i]$-module of rank 2^{r-2} and a $\mathbb{Z}[i]$-basis is given by $\{1, \xi, \xi^2, \ldots, \xi^{2^{r-2}-1}\}$.*

Proposition 3. (OGGIER, 2005) *The relative discriminant $d_{\mathbb{Q}(\xi)/\mathbb{Q}(i)}$ satisfies*

$$|d_{\mathbb{Q}(\xi)/\mathbb{Q}(i)}| = (2^{r-2})^{2^{r-2}}.$$

Thus, we have the following example:

Example 2. *As seen previously, a cyclotomic field is a number field K given by $K = \mathbb{Q}(\xi_n)$, where $\xi_n = e^{\frac{2\pi i}{n}}$, for some integer $n \geq 3$, that is, ξ_n is a primitive n-th root of unity. It can be shown that the field extension K/F is cyclic and $[K : F] = \frac{1}{2}[K : \mathbb{Q}]$, where $[K : \mathbb{Q}] = \phi(n)$ and ϕ denotes the Euler function. This field extension is Galois, with*

$$Gal(K/\mathbb{Q}) = \{\sigma_j : \sigma_j(\xi_n) = \xi_n^j | gcd(n, j) = 1\},$$

which is isomorphic to the group of units in $\mathbb{Z}/\mathbb{Z}_n$ and denoted as $U(\mathbb{Z}/\mathbb{Z}_n)$. The ring of algebraic integers of K is denoted by $\mathcal{O}_K = \mathbb{Z}[\xi_n]$ and its integral basis is given by

$$\{1, \xi_n, \xi_n^2, \ldots, \xi_n^{\phi(n)-1}\}.$$

However,

1. *if $F = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\xi_{2^{s+2}})$, for $s \geq 1$, then the field extension $K/\mathbb{Q}$ is cyclic, with $[K : \mathbb{Q}] = \phi(2^{s+2}) = 2 \times 2^s$ and the Galois group $Gal(K/\mathbb{Q}) \simeq U(\mathbb{Z}/2^{s+2}\mathbb{Z})$. Also $[K : F] = \frac{\phi(2^{s+1})}{2} = 2^s$ and, therefore, the subfield $F = \mathbb{Q}(i)$ of K is fixed by the cyclic group $\mathbb{Z}/2^s\mathbb{Z}$.*

2. *if $F = \mathbb{Q}(\xi_3)$ and $K = \mathbb{Q}(\xi_{3^{s+1}})$, for $s \geq 1$, then the field extension $K/\mathbb{Q}$ is cyclic, with $[K : \mathbb{Q}] = \phi(3^{s+1}) = 2 \times 3^s$ and the Galois group $Gal(K/\mathbb{Q}) \simeq U(\mathbb{Z}/(3^{s+1})\mathbb{Z})$. Also $[K : F] = \frac{\phi(3^{s+1})}{2} = 3^s$ and, therefore, the subfield $F = \mathbb{Q}(\xi_3)$ of K is fixed by the cyclic group $\mathbb{Z}/3^s\mathbb{Z}$.*

2.2.2 Decomposition of prime ideals

In this section, we will see that every ideal in the ring of integers of a number field can be factored uniquely as the product of prime ideals.

Definition 5. *An ideal I of a commutative ring R is an additive subgroup of R, which is stable over the multiplication by R, that is, $aI \subset I$, for all $a \in R$. An ideal I is principal if it is of the form $I = (x) = xR = \{xy,\ y \in R\}$, $x \in I$.*

Definition 6. *We say that an ideal is prime if it satisfies the following property: if $xy \in I$, then $x \in I$ or $y \in I$.*

Definition 7. *Let I_1 and I_2 be ideals of a ring R. The sum and product of ideals are defined as it follows:*

$$I_1 + I_2 := \{a + b \mid a \in I_1 \text{ and } b \in I_2\} \text{ and}$$

$$I_1 I_2 := \{a_1 b_1 + \ldots + a_n b_n \mid a_i \in I_1 \text{ and } b_i \in I_2,\ i = 1, 2, \ldots, n;\ \text{for } n = 1, 2, 3, \ldots\},$$

i.e., the product of two ideals I_1 and I_2 is defined to be the ideal $I_1 I_2$ generated by all products of the form ab, with $a \in I_1$ and $b \in I_2$. The product $I_1 I_2$ is contained in the intersection of I_1 and I_2.

Proposition 4. *Let I be an ideal of a commutative ring with identity R and assume that I is a principal ideal, that is, $I = (a)$, $a \in I$. Then I^k (the product), $k \geq 2$ integer, is the principal ideal generated by a^k.*

Proof. We will prove it by induction over k. For $k = 2$, it follows

$$I^2 = I \cdot I = \{a_1b_1 + \ldots + a_nb_n \mid a_i, b_i \in I,\ i = 1,2,\ldots,n;\ \text{for } n = 1,2,3,\ldots\}.$$

If $x \in I^2$, then $x = (ar_{11})(ar_{12}) + \ldots + (ar_{n1})(ar_{n2})$, with $r_{ij} \in R$, $i = 1,2,\ldots,n$ and $j = 1,2$. As the ring is commutative, we have $x = a^2\gamma$, with $\gamma = r_{11}r_{12} + \ldots + r_{n1}r_{n2}$, so $x \in (a^2)$ and then $I^2 \subset (a^2)$.

Now if $x \in (a^2)$, then $x = a^2\gamma$, with $\gamma \in R$. So $\gamma = \delta_1 + \ldots + \delta_n$, for some n, and $\delta_i \in R$, $i = 1,2,\ldots,n$. But δ_i can be written as $\delta_i = r_{i1}r_{i2}$, with $r_{ij} \in R$, $i = 1,2,\ldots,n$ and $j = 1,2$. Then we have (R is commutative)

$$x = a^2\gamma = a^2(r_{11}r_{12} + \ldots + r_{n1}r_{n2}) = (ar_{11})(ar_{12}) + \ldots + (ar_{n1})(ar_{n2}) \in I^2.$$

Therefore $(a^2) \subset I^2$, so $I^2 = (a^2)$. We will assume now that it is true for k and we will prove it for $k+1$, so $I^k = (a^k)$. We have

$$I^{k+1} = I^k \cdot I = \{a_1b_1 + \ldots + a_nb_n \mid a_i \in I^k \text{ and } b_i \in I,\ i = 1,2,\ldots,n;\ \text{for } n = 1,2,3,\ldots\}.$$

If $x \in I^{k+1}$, then $x = (a^kr_{11})(ar_{12}) + \ldots + (a^kr_{n1})(ar_{n2})$, with $r_{ij} \in R$, $i = 1,2,\ldots,n$ and $j = 1,2$. As the ring is commutative, we have $x = a^{k+1}\gamma$, with $\gamma = r_{11}r_{12} + \ldots + r_{n1}r_{n2}$, so $x \in (a^{k+1})$ and then $I^{k+1} \subset (a^{k+1})$.

Now if $x \in (a^{k+1})$, then $x = a^{k+1}\gamma$, with $\gamma \in R$. So $\gamma = \delta_1 + \ldots + \delta_n$, for some n, and $\delta_i \in R$, $i = 1,2,\ldots,n$. But δ_i can be written as $\delta_i = r_{i1}r_{i2}$, with $r_{ij} \in R$, $i = 1,2,\ldots,n$ and $j = 1,2$. Then we have (R is commutative)

$$x = a^{k+1}\gamma = a^{k+1}(r_{11}r_{12} + \ldots + r_{n1}r_{n2}) = (a^kr_{11})(ar_{12}) + \ldots + (a^kr_{n1})(ar_{n2}) \in I^{k+1}.$$

Therefore $(a^{k+1}) \subset I^{k+1}$, so $I^{k+1} = (a^{k+1})$. Then $I^k = (a^k)$. □

The notion of ideal can be extended as it follows:

Definition 8. *A fractional ideal I is a O_K-submodule of K such that there exists $d \in O_K \setminus \{0\}$ with $I \subset d^{-1}O_K$.*

Theorem 8. (STEWART; TALL, 2002) *Every ideal $I \neq 0$ of O_K has a free $\mathbb{Z}$-basis $\{v_1,\ldots,v_n\}$, where n is the degree of K.*

Definition 9. *Let I be an ideal of O_K. The norm of I is defined by $N(I) = |O_K/I|$.*

Remark 3. *It follows directly that if $I = aO_K$ is principal, then $N(I) = |N_{K/\mathbb{Q}}(a)|$.*

We know that for all $n \in \mathbb{Z}$, there exists a unique factorization into prime numbers. This notion of factoring is replaced similarly to ideals.

Theorem 9. (SAMUEL, 2008) *Every ideal I of O_K can be written uniquely as a product of powers of prime ideals:*

$$I = \prod_{i=1}^{m} B_i^{e_i}.$$

Example 3. *If p is a prime number and O_K is the ring of algebraic integers of $K = \mathbb{Q}(\xi_p)$, then the ideal pO_K has the form $pO_K = (1-\xi_p)^{p-1}O_K$. In fact, if $1 \leq k,\ j \leq p-1$, then there exists an integer t, where $1 \leq t \leq p-1$, such that $j \equiv kt \pmod p$. So*

$$1 - \xi_p^j = 1 - (\xi_p^k)^t = (1-\xi_p^k)(1+\xi_p^k + \ldots + (\xi_p^k)^{t-1}) \tag{5}$$

and then $(1-\xi_p^k)|(1-\xi_p^j)$. Analogously $(1-\xi_p^j)|(1-\xi_p^k)$. So $1-\xi_p^j$ and $1-\xi_p^k$ are associated in O_K. As the minimal polynomial of $\mathbb{Q}(\xi_p)$, $X^{p-1}+\ldots+X+1$, is equal to the p-th cyclotomic polynomial $\phi_p(X) = \prod_{k=1}^{p-1}(X-\xi^k)$, it follows that, evaluating the polynomial at $X=1$, we have $p = \prod_{k=1}^{p-1}(1-\xi^k)$. Then there exists an invertible element $\beta \in O_K$ such that $p = (1-\xi_p)^{p-1}\beta$. Therefore $pO_K = (1-\xi_p)^{p-1}O_K$.

Definition 10. *The set $D_{K/\mathbb{Q}}^{-1} = \{x \in K \mid \forall \alpha \in O_K,\ Tr_{K/\mathbb{Q}}(x\alpha) \in \mathbb{Z}\}$ is a fractional ideal of O_K called codifferent. Its inverse ideal $D_{K/\mathbb{Q}}$ is an integer ideal of D_K called different.*

Now we remember the basic results of factorization into irreducible elements of the ring of algebraic integers of a cyclotomic number field. Let L be a cyclotomic number field such that L is a finite algebraic extension of F, where F is a number field. If $\mathscr{P}$ is a prime ideal in $\mathscr{O}_F$, then $\mathscr{P}$ is factorized uniquely into a product of prime ideals given by

$$\mathscr{P}\mathscr{O}_L = \beta_1^{e_1}\beta_2^{e_2}\ldots\beta_n^{e_n}. \tag{6}$$

Notice that $\beta_i \cap \mathscr{O}_F = \mathscr{P}$. The exponent of any β_i that appears in the factorization of $\mathscr{P}\mathscr{O}_L$ is called the ramification index of β_i over $\mathscr{P}$ and denoted by $e(\beta_i|\mathscr{P}) = e_i$. The inertial degree of β_i over $\mathscr{P}$ is given by the degree associated to the field extension $\mathscr{O}_L/\beta_i$ over $\mathscr{O}_L/\mathscr{P}$ and denoted by $f(\beta_i|\mathscr{P}) = f_i$. In other words, the norm of the ideal β_i is given by $N_{L/\mathbb{Q}}(\beta_i) = (N_{L/F}(\mathscr{P}))^{f_i}$. The ramification indices and the inertial degrees satisfy the relations given by $\sum_{i=1}^{r} e_i f_i = [L:F]$, $f(\beta_i|p) = f(\beta_i|\mathscr{P})f(\mathscr{P}|p)$ and $e(\beta_i|p) = e(\beta_i|\mathscr{P})e(\mathscr{P}|p)$.

We call the primes p, $\mathscr{P}$ and β_i that lie one below the other as a prime triplet $(p;\mathscr{P};\beta_i)$. When we work with the cyclic Galois extension such that L is Galois over F, if β_i, where $1 \leq i \leq r$, are all the prime ideals that lie over $\mathscr{P}$ (with the same form that they appear in Equation (6)), then the ramification indices of all the prime ideals are equal and so are the

inertial degrees. Therefore if e and f denote these common values, then we find the relations $efr = [L:F]$ and $N_{L/\mathbb{Q}}(\beta_i) = (N_{L/F}(\mathscr{P}))^f$, for all $i = 1,\ldots,n$.

Definition 11. *Let $F \subseteq L$ be fields such that $[L:F] = m$. Let $\mathscr{O}_F$ and $\mathscr{O}_L$ be their respective ring of algebraic integers. We say that the ideal $\mathscr{P}$ of $\mathscr{O}_F$ is:*

1. *totally decomposed in L, if $n = m$ and so $e_i = f_i = 1$, for all $i = 1,2,...,n$;*
2. *inert in L, if $n = 1$, $e_1 = 1$ and so $f_1 = m$;*
3. *totally ramified in L, if $n = 1$ and so $f_1 = 1$ and $e_1 = m$.*

2.3 Background on Lattice Theory

Lattices have been very useful in applications in communication theory and, in this work, we used lattices in order to realize interference alignment. In this section, we present basic concepts and results from the lattice theory, which are very useful for this work. An important reference related to the lattice theory used for the development of this work is (FORNEY, 1988). For more details in lattice theory, see (CONWAY; SLOANE, 1999).

2.3.1 A lattice primer

In this section, most of the concepts of lattice presented here can be found in (FORNEY, 1988), which is one of the fundamental references for the development of this work.

Definition 12. *Let $v_1, v_2, \ldots, v_m$ be a set of linearly independent vectors in $\mathbb{R}^N$ such that $m \leq N$. The set of the points*

$$\Lambda = \{x = \sum_{i=1}^{m} \lambda_i v_i, \text{ where } \lambda_i \in \mathbb{Z}\}$$

*is called a **lattice** of rank m and $\{v_1, v_2, \ldots, v_m\}$ is called a basis of the lattice.*

So we have that a real *lattice* Λ is simply a discrete set of vectors (points (N-tuples)) in real Euclidean N-space $\mathbb{R}^N$ that forms a group under ordinary vector addition, i.e., the sum or difference of any two vectors in Λ is in Λ. Thus Λ necessarily includes the all-zero N-tuple $\mathbf{0}$, and if λ is in Λ, then so is its additive inverse $-\lambda$.

As an example, the set $\mathbb{Z}$ of all integers is the only one-dimensional real lattice, up to scaling, and the prototype of all lattices. The set $\mathbb{Z}^N$ of all integer N-tuples is an N-dimensional real lattice, for any N.

Definition 13. *The parallelotope formed by the points*

$$\theta_1 v_1 + \ldots + \theta_m v_m, \text{ where } 0 \leq \theta_i < 1,\ i = 1, \ldots, m,$$

is called a ***fundamental parallelotope*** *or* ***fundamental region*** *of the lattice.*

Lattices have only two principal structural characteristics. Algebraically, a lattice is a group; this property leads to the study of subgroups (sublattices) and partitions (coset decompositions) induced by such subgroups. Geometrically, a lattice is endowed with the properties of the space in which it is embedded, such as the Euclidean distance metric and the notion of volume in $\mathbb{R}^N$.

Definition 14. *Let* $\{v_1, v_2, \ldots, v_m\}$ *be a basis of the lattice* Λ*. If* $v_i = (v_{i1}, v_{i2}, \ldots, v_{iN})$*, for* $i = 1, 2, \ldots, m$*, the matrix*

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1N} \\ v_{21} & v_{22} & \cdots & v_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mN} \end{pmatrix}$$

is called a ***generator matrix*** *for the lattice* Λ*. The matrix* $G = MM^T$ *is called a* ***Gram matrix*** *for the lattice* Λ*, where* T *denotes the transpose.*

By using the fact that M contains the vectors of the lattice basis $\{v_i\}_{i=1}^m$, the (i, j)-th entry of the matrix G is the inner product $\langle v_i, v_j \rangle = v_i \cdot v_j^T$, where T denotes the transpose.

The points of the lattice Λ are formed by

$$\Lambda = \{x = \lambda M \mid \lambda \in \mathbb{Z}^m\}.$$

Definition 15. *The* ***determinant of the lattice*** Λ *is defined as the determinant of the matrix G, that is,*

$$Det(\Lambda) = Det(G).$$

If $m = N$, a lattice is said to have *maximal rank* and, in this case, M is a square matrix. Then

$$Det(\Lambda) = (Det(M))^2.$$

Definition 16. *For lattices which have maximal rank, the square root of the determinant of the lattice is the volume of the fundamental parallelotope, also called* ***volume of the lattice*** *and denoted by* $V(\Lambda)$.

The volume of a lattice is independent of the chosen basis, so we can define the volume of the lattice Λ as the volume of a fundamental region.

Lattices closely related to a given real N-dimensional lattice Λ are obtained by the following operations:

1. *Scaling:* If r is any real number, then $r\Lambda$ is the lattice consisting of all multiples $r\Lambda$ of vectors λ in Λ by the scalar r;

2. *Orthogonal Transformation:* More generally, if T is any scaled orthogonal transformation of N-space, then $T\Lambda$ is the lattice consisting of all transformations $T\lambda$ of vectors λ in Λ by T. We say that $T\Lambda$ is a *version* of Λ;

3. *Cartesian Product:* The M-fold Cartesian product of Λ with itself, i.e., the set of all MN-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_M)$ where each λ_j is in Λ, is an MN-dimensional lattice denoted by Λ^M.

For example, $\mathbb{Z}^N$ is the N-fold Cartesian product of $\mathbb{Z}$ with itself, and $r\mathbb{Z}^N$ is a scaled version of $\mathbb{Z}^N$, for any r and N.

The most important scaled orthogonal transformation four our purposes is the *rotation operator* R, defined by the 2×2 matrix

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

$R\mathbb{Z}^2$ is a version of $\mathbb{Z}^2$ obtained by rotating $\mathbb{Z}^2$ by 45° and scaling by $2^{\frac{1}{2}}$. The points in $R\mathbb{Z}^2$ are a subset of the points in $\mathbb{Z}^2$, meaning that $R\mathbb{Z}^2$ is a sublattice of $\mathbb{Z}^2$. Note that $R^2 = 2I$, where I is the identity operator (in two dimensions), so that $R^2\mathbb{Z}^2 = 2\mathbb{Z}^2$.

We can define a $2N$-dimensional rotation operator by letting R operate on each pair of coordinates in a $2N$-tuple; with a slight abuse of notation, we denote by R any such rotation operator. For instance, in four dimensions,

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

Note that $R^2 = 2I$, for any N, where I is the identity operator in $2N$ dimensions, so that $R^2\Lambda = 2\Lambda$, for any real $2N$-dimensional lattice Λ.

Definition 17. *If a lattice can be obtained from another lattice by using a rotation, reflection or scaling, we say that these lattices are equivalent.*

Thus, two generator matrices M and M' define equivalent lattices if, and only if, they are described by $M' = cUMB$, where c is a non-zero constant, U is a matrix with integer entries and

determinant equal to ± 1 and B is an orthogonal real matrix. The corresponding Gram matrices are related by $G' = c^2 UGU^T$, where T denotes the transpose. If U has the determinant equal to ± 1 and $c = 1$, then M and M' define congruent lattices.

Then we have to keep in mind that the same lattice can be represented in a few different ways.

Definition 18. *Let Λ, β and V be a lattice, a basis of the lattice Λ and the vector space generated by β, respectively. We define the* ***Voronoi region*** *of $v \in \Lambda$ as the region that contains all the points of V which are closer to v than any other point u of the lattice, that is, $V(v) = \{x \in V \mid \| x - v \| \leq \| x - u \|, \forall u \in \Lambda\}$.*

2.3.2 Group and geometric properties

The author in (FORNEY, 1988) discusses the group and geometric properties as it follows: a *coset* of a lattice Λ, denoted by $\Lambda + c$, is the set of all N-tuples of the form $\lambda + c$, where λ is any point in Λ and c is some constant N-tuple that specifies the coset. Geometrically, the coset $\Lambda + c$ is therefore a *translate* of Λ by c (if c is in Λ, then $\Lambda + c = \Lambda$). Two N-tuples are *equivalent modulo* Λ if their difference is a point in Λ. So the coset $\Lambda + c$ is the set of all points equivalent to c modulo Λ.

We have that a sublattice Λ' of a lattice Λ is a subset of the elements of Λ that is itself a lattice, i.e., Λ' is a subgroup of the additive group Λ. Thus, by elementary group theory, a sublattice Λ' induces a *partition* (denoted by Λ/Λ') of Λ into equivalence classes modulo Λ' (the equivalence classes may be added modulo Λ' and form the *quotient group* Λ/Λ'). We shall say that the *order* of the partition (or quotient group) Λ/Λ' is the number $|\Lambda/\Lambda'|$ of such equivalence classes (in the mathematical literature, $|\Lambda/\Lambda'|$ is usually called the *index* of Λ' in Λ). Each equivalence class is a coset of Λ' (one being Λ' itself), or, geometrically, a translate of Λ'. For example, the partition $\mathbb{Z}^2/R\mathbb{Z}^2$ has order $|\mathbb{Z}^2/R\mathbb{Z}^2| = 2$, that is, $\mathbb{Z}^2$ is the union of two cosets of $R\mathbb{Z}^2$. Of course, any N-dimensional integer lattice Λ is a sublattice of $\mathbb{Z}^N$.

If we take one element from each equivalence class, we obtain a system of *coset representatives* for the partition Λ/Λ', denoted by $[\Lambda/\Lambda']$. (In general, there are many ways of selecting such a system $[\Lambda/\Lambda']$, so the notation does not entirely specify the system.) Then every element of Λ can be written uniquely as a sum $\lambda = \lambda' + c$, where $c \in [\Lambda/\Lambda']$ is the coset representative of the equivalence class in which λ lies, and $\lambda' = \lambda - c$ is an element of Λ' (because $\lambda \equiv c \bmod \Lambda'$). This is called a *coset decomposition* of Λ and will be written here as

$$\Lambda = \Lambda' + [\Lambda/\Lambda'].$$

For instance, the two 2-tuples $(0,0)$ and $(1,0)$ are a system of coset representatives for

the partition $\mathbb{Z}^2/R\mathbb{Z}^2$, and every element of $\mathbb{Z}^2$ may be written as the sum of one of these two 2-tuples with an element of $R\mathbb{Z}^2$, i.e., $\mathbb{Z}^2$ is the union of $R\mathbb{Z}^2+(0,0)=R\mathbb{Z}^2$ and $R\mathbb{Z}^2+(1,0)$.

As another example, if m is any integer, the lattice $m\mathbb{Z}$ of integer multiples of m is a sublattice of $\mathbb{Z}$. The partition $\mathbb{Z}/m\mathbb{Z}$ is the partition of the integers into m equivalence classes modulo $m\mathbb{Z}$ (modulo m), and the order of the partition is m. The integers $\{0,1,\ldots,m-1\}$ form a system of coset representatives for the partition $\mathbb{Z}/m\mathbb{Z}$, and every integer n can be written uniquely as $n=am+c$, where am is an element of $m\mathbb{Z}$ and $c\in\{0,1,\ldots,m-1\}=[\mathbb{Z}/m\mathbb{Z}]$ (thus $[\mathbb{Z}/m\mathbb{Z}]$ is essentially the ring $\mathbb{Z}_m$ of integers modulo m). In particular, the partition $[\mathbb{Z}/2\mathbb{Z}]$ has order 2 and divides the integers into two subsets, $2\mathbb{Z}$ (the even integers) and $2\mathbb{Z}+1$ (the odd integers).

More generally, for any $m\in\mathbb{Z}$, the lattice $m\mathbb{Z}^N$ of all N-tuples of integers multiples of m is a sublattice of $\mathbb{Z}^N$ of order m^N, and $[\mathbb{Z}/m\mathbb{Z}]^N$ is a system of coset representatives for $\mathbb{Z}^N/m\mathbb{Z}^N$; hence $\mathbb{Z}^N=m\mathbb{Z}^N+[\mathbb{Z}/m\mathbb{Z}]^N$.

A partition Λ/Λ' also induces a coset decomposition of any coset of Λ, say $\Lambda+c$; for $\Lambda+c=\Lambda'+[\Lambda/\Lambda']+c$.

A *partition chain* $\Lambda/\Lambda'/\Lambda''/\cdots$ is a sequence of lattices such that each is a sublattice of the previous one (in other words, $\Lambda\supseteq\Lambda'\supseteq\Lambda''\supseteq\cdots$). For example, $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}/\cdots$ is an infinite sequence of two-way partitions of the integers. A partition chain induces a multiterm coset decomposition chain, with a term corresponding to each partition; e.g., if $\Lambda/\Lambda'/\Lambda''$ is a partition chain, then

$$\Lambda=\Lambda''+[\Lambda'/\Lambda'']+[\Lambda/\Lambda'],$$

meaning that every element of Λ can be expressed as an element of Λ'' plus a coset representative from $[\Lambda'/\Lambda'']$ plus a coset representative from $[\Lambda/\Lambda']$. For example, the chain $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}/\cdots$ leads to the *standard binary representation* of an integer m:

$$m=a_0+2a_1+4a_2+\cdots,$$

where $a_0,a_1,a_2,\ldots\in\{0,1\}$, and a_0 specifies the coset in the partition $\mathbb{Z}/2\mathbb{Z}$, $2a_1$ specifies the coset in the partition $2\mathbb{Z}/4\mathbb{Z}$, and so forth. That is,

$$\mathbb{Z}=[\mathbb{Z}/2\mathbb{Z}]+[2\mathbb{Z}/4\mathbb{Z}]+[4\mathbb{Z}/8\mathbb{Z}]+\cdots.$$

We have that the geometry of a real lattice Λ arises from the geometry of a real Euclidean N-space $\mathbb{R}^N$. The two principal geometrical parameters of Λ are the minimum squared distance $d^2_{min}(\Lambda)$ between its points and its fundamental volume $V(\Lambda)$; these determine its fundamental coding gain.

The *norm* $\|x\|^2$ of a vector x in $\mathbb{R}^N$ is the sum of the squares of its coordinates. Norms are

non-negative and in fact non-zero unless $x = 0$. The *squared distance* between two vectors x and y is the norm of their difference $\|x-y\|^2$.

By the fact that a lattice Λ consists of discrete points, the norms of all lattice points are an infinite set of discrete values that can be enumerated in ascending order. We call this the *weight distribution* of the lattice (*theta series*, in the lattice literature). The weight distribution is also the squared distance distribution between any point in the lattice and all other points, since any point λ in Λ can be taken as the origin $\mathbf{0}$ by translation of Λ by λ (looking out from any point in Λ, the lattice looks the same).

The minimum non-zero norm is thus the *minimum squared distance* $d^2_{min}(\Lambda)$ between any two points in Λ. The number of elements of Λ with this norm is the number of nearest neighbors of any lattice point (also called the *kissing number* or *multiplicity*), and will be called here the *error coefficient* $N_0(\Lambda)$.

For example, for any N, the integer lattice $\mathbb{Z}^N$ has $d^2_{min}(\mathbb{Z}^N) = 1$. The set of all integer N-tuples of norm 1 is the set of all permutations and sign changes of the vector $(1,0,\ldots,0)$, so $N_0(\mathbb{Z}^N) = 2N$.

Loosely, the *fundamental volume* $V(\Lambda)$ is the volume of N-space per lattice point, or the reciprocal of the number of lattice points per unit volume. More precisely, if we can partition N-space into regions of equal volume, one associated with each lattice point, then $V(\Lambda)$ is the volume of each such region. For example, it is easy to see that we may partition N-space into N-cubes of side 1, one associated with each point of $\mathbb{Z}^N$, so $V(\mathbb{Z}^N) = 1$.

Lemma 2. (FORNEY, 1988) *If Λ' is a sublattice of Λ of order $|\Lambda/\Lambda'|$, then $V(\Lambda') = |\Lambda/\Lambda'|V(\Lambda)$.*

Corollary 2. (FORNEY, 1988) *If Λ is an integer lattice, then $V(\Lambda) = |\mathbb{Z}^N/\Lambda|$.*

From the two geometrical parameters $d^2_{min}(\Lambda)$ and $V(\Lambda)$, we define the *fundamental coding gain* $\gamma(\Lambda)$ of a lattice Λ as it follows:

$$\gamma(\Lambda) \triangleq d^2_{min}(\Lambda)/V(\Lambda)^{2/N}.$$

We have in the mathematical literature that this is called Hermite's parameter and is also denoted by the symbol γ. The fundamental coding gain is a normalized measure of the density of a lattice.

2.3.3 Complex lattices and Gaussian integers

The author in (FORNEY, 1988) discusses complex lattices and Gaussian integers as it follows: a complex lattice Λ is a discrete set of points in complex Euclidean N-space $\mathbb{C}^N$ that forms a group under ordinary (complex) vector addition. Again, we stipulate that the only such

lattices to be considered here will actually span N dimensions, so we shall feel free to call such a Λ an *N-dimensional* complex lattice.

We have that an obvious isomorphism (written $\Lambda_r \simeq \Lambda_c$) exists between any $2N$-dimensional real lattice Λ_r and a corresponding N-dimensional complex lattice Λ_c, formed by taking each pair of coordinates of Λ_r to specify the real and imaginary parts of each coordinate of Λ_c, or vice versa. Addition of two points gives the same result in either case. Sublattices, cosets and all such group properties carry over. Even the norm of two corresponding vectors is the same, so distances are not affected. Thus for most purposes it makes no difference whether we consider a lattice to be real or complex.

The only difference of any significance arises when we consider multiplicative operations, such as scaling or the taking of inner product. The inner product (x,y) of two real vectors x and y is the sum of the products of their coordinates and must be real; the (Hermitian) inner product (x,y) of two complex vectors x and y is the sum of the products of the coordinates of x with the complex conjugates of the coordinates of y and may be complex. Thus there may arise differences in definitions of orthogonality, duality and so forth.

The simplest example of a complex lattice is the one-dimensional complex lattice G corresponding to the two-dimensional real lattice $\mathbb{Z}^2$. The point (a,b) in $\mathbb{Z}^2$ corresponds to the point $a+bi$ in G, where a and b may be any pair of integers. The set G is called the set of *Gaussian integers*.

The Gaussian integers G actually form a system of complex integers analogous to the ordinary real integers $\mathbb{Z}$. Multiplication of two elements of G (using complex arithmetic) yields another element of G, which cannot be 0 unless one of the two elements is 0 (in fact, their norms multiply as real integers). Thus G is a ring and, in fact, an integral domain. Indeed, we have unique factorization in G: every element of G can be expressed uniquely as a product of primes, up to units, where the units (invertible elements) are ± 1 and $\pm i$, and the primes are the elements that have no divisors other than themselves, up to units. The primes of G, in order of increasing norm, are $1+i, 2\pm i, 3, \ldots$, with norms $2, 5, 9, \ldots$ We denote the prime of least norm by $\phi \triangleq 1+i$. (Note that $|\phi|^2 = \phi\phi^* = 2$ and thus two is not a prime in G)

We may scale G by any element $g \in G$ and obtain a sublattice gG of G. The partition G/gG have order $|g|^2$ (the norm of g). There are thus $|g|^2$ equivalence classes of G modulo g.

For example, ϕG is a sublattice of G of order $|g|^2 = 2$ and, in fact, is the complex lattice corresponding to the real lattice $R\mathbb{Z}^2$. As with $R\mathbb{Z}^2$, ϕG consists of all the elements of G with even norm, its coset $\phi G + 1$ consists of all the elements of G with odd norm, and the union of ϕG and $\phi G + 1$ is G. The coset representatives $[G/\phi G]$ may thus be taken as $\{0,1\}$, and are isomorphic to $\mathbb{Z}_2 = GF(2)$ using modulo ϕ arithmetic (since $2 \equiv 0 \bmod \phi$).

More generally, $\phi^\mu G$ is a sublattice of G of order $|\phi|^{2\mu} = 2^\mu$ and, in fact, is the com-

plex lattice corresponding to the real lattice $R^\mu\mathbb{Z}^2$, which is equal to $2^{\mu/2}\mathbb{Z}^2$, for μ even, and $2^{(\mu-1)/2}R\mathbb{Z}^2$, for μ odd. As with $R^\mu\mathbb{Z}^2$, $\phi^\mu G$ consists of all the elements of G whose norms are multiples of 2^μ, and thus $d^2_{min}(\phi^\mu G) = 2^\mu$. There is then an infinite chain

$$G/\phi G/\phi^2 G/\phi^3 G/\phi^4 G/\cdots$$

of two-way partitions, with distances $1/2/4/8/16/\cdots$, corresponding to the real chain

$$\mathbb{Z}^2/R\mathbb{Z}^2/2\mathbb{Z}^2/2R\mathbb{Z}^2/4\mathbb{Z}^2/\cdots.$$

In analogy to the chain $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}/\cdots$, this chain suggests a *complex binary representation* of a Gaussian integer g:

$$g = a_0 + \phi a_1 + \phi^2 a_2 + \cdots,$$

where $a_0, a_1, a_2, \ldots \in \{0,1\}$, and a_0 specifies the coset of ϕG in the partition $G/\phi G$, ϕa_1 specifies the coset of $\phi^2 G$ in the partition $\phi G/\phi^2 G$ and so forth. That is, the complex binary representation is based on the coset decomposition

$$G = [G/\phi G] + [\phi G/\phi^2 G] + [\phi^2 G/\phi^3 G] + \cdots.$$

For any lattice Λ, if λ is any lattice point and m is any integer, then $\pm m\lambda = \pm(\lambda + \lambda + \cdots + \lambda)$ is a lattice point, so $m\Lambda$ is a sublattice of Λ and Λ (like any additive group) is a module over the ring $\mathbb{Z}$ of ordinary integers. However, a complex lattice Λ is not necessarily a module over the ring G of Gaussian integers (for example, the two-dimensional hexagonal lattice is not). It is so if, and only if, $\lambda \in \Lambda$ implies $i\lambda \in \Lambda$; for then if $g = a + bi$ is any Gaussian integer, $g\lambda = a\lambda + b(i\lambda)$ is a lattice point. Then $g\Lambda$ is a sublattice of Λ, for any $g \in G$. In particular, $i\Lambda$ is a sublattice of Λ; but since $i(i\Lambda) = -\Lambda = \Lambda$ is a sublattice of $i\Lambda$, in fact $i\Lambda = \Lambda$. When necessary, we shall call such a complex lattice a *G-lattice*.

2.3.4 Binary lattices

The author in (FORNEY, 1988) discusses binary lattices as it follows: a real N-dimensional lattice Λ is a *binary lattice* if it is an integer lattice that has $2^m\mathbb{Z}^N$ as sublattice, for some m. The least such m is called the *2-depth* of the lattice. Thus $\mathbb{Z}^N/\Lambda/2^m\mathbb{Z}^N$ is a partition chain. It turns out that all of the binary lattices that have proved to be useful to date have 2-depth equal to one or two; we shall call such lattices mod-2 and mod-4 lattices, respectively.

A complex N-dimensional lattice Λ is a *binary lattice* if it is a Gaussian integer G-lattice that has $\phi^\mu G^N$ as a sublattice, for some μ. The least such μ is called the *ϕ-depth* of the lattice. Thus $G^N/\Lambda/\phi^\mu G^N$ is a partition chain.

If Λ is a $2N$-dimensional real binary lattice, then the corresponding N-dimensional complex lattice is also a complex binary lattice (if it is a G-lattice), and vice versa, since $2^m\mathbb{Z}^{2N} \simeq \phi^{2m}G^N \subset \phi^{2m-1}G^N$. So we may speak of the ϕ-depth of a real $2N$-dimensional binary lattice. A real $2N$-dimensional binary lattice with 2-depth m has ϕ-depth $2m$ or $2m-1$; thus the ϕ-depth is twice as fine-grained a parameter and we shall henceforth call it simply the *depth* μ of a binary lattice. A mod-2 binary lattice thus has depth 1 or 2, and a mod-4 binary lattice has depth 3 or 4. For example, since $\mathbb{Z}^4/D_4/R\mathbb{Z}^4 \simeq G^2/D_4/\phi G^2$ is a partition chain, where D_4 is defined as the four-dimensional integer lattice consisting of all integer 4-tuples with an even number of odd coordinates or, equivalently, with even norm, D_4 is a mod-2 binary lattice with depth $\mu = 1$.

Since the order of the partition $\mathbb{Z}^N/2^m\mathbb{Z}^N$ (resp. $G^N/\phi^\mu G^N$) is a power of two, the orders of $\mathbb{Z}^N/\Lambda$ and $\Lambda/2^m\mathbb{Z}^N$ (resp. G^N/Λ and $\Lambda/\phi^\mu G^N$) must be powers of two, since their product is $|\mathbb{Z}^N/2^m\mathbb{Z}^N|$ (resp. $|G^N/\phi^\mu G^N|$). The *redundancy* $r(\Lambda)$ of a binary lattice Λ is defined as the binary logarithm of $|\mathbb{Z}^N/\Lambda|$, so that $|\mathbb{Z}^N/\Lambda| = 2^{r(\Lambda)}$. The fundamental volume of a binary lattice is $V(\Lambda) = 2^{r(\Lambda)}$.

2.3.5 Ideal lattices

We will present, in this section, the concepts of ideal lattice, diversity and product distance.

Definition 19. *Let K be a totally real number field of degree n. An ideal lattice is a lattice $(\mathscr{A}, q_\alpha)$, where $\mathscr{A} \subseteq O_K$ is an ideal,*

$$q_\alpha : \mathscr{A} \times \mathscr{A} \to \mathbb{Z}, \text{ with } q_\alpha(x,y) = Tr_{K/\mathbb{Q}}(\alpha xy), \text{ for all } x,y \in \mathscr{A},$$

and $\alpha \in K$ is totally positive, i.e., $\sigma_j(\alpha) > 0$, for all $j = 1,2,\ldots,n$, where $n = [K/\mathbb{Q}]$ and $\{\sigma_1,\ldots,\sigma_n\}$ denotes the n embeddings of the extension $K/\mathbb{Q}$.

If $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is a basis of $\mathscr{A}$ over $\mathbb{Z}$, then the generator matrix R of the lattice $\Lambda = \{x = \lambda R \mid \lambda \in \mathbb{Z}^n\}$ is given by

$$R = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(\alpha_1) & \ldots & \sqrt{\sigma_n(\alpha)}\sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\alpha_n) & \ldots & \sqrt{\sigma_n(\alpha)}\sigma_n(\alpha_n) \end{pmatrix}. \tag{7}$$

In this case, we have that the Gram matrix RR^T coincides with the trace form

$$Tr_{K/\mathbb{Q}}(\alpha\alpha_i\alpha_j)_{i,j=1}^n,$$

where T denotes the transpose.

Definition 20. *Let $\Lambda \subseteq \mathbb{R}^N$ be a lattice and let $x = (x_1, \ldots, x_N) \in \Lambda$. The diversity of Λ is defined as*

$$div(\Lambda) = min_{0 \neq x \in \Lambda} \#\{i \mid x_i \neq 0,\ i = 1, 2, \ldots, N\}.$$

Definition 21. *Let Λ be an n-dimensional lattice with full diversity, that is, the diversity of Λ is equal to n, and let $x = (x_1, \ldots, x_n) \in \Lambda$. The product distance of x from the origin is defined as*

$$d_p(x) = \prod_{i=1}^{n} | x_i |,$$

and the minimum product distance of Λ is defined as

$$d_{p,min}(\Lambda) = min_{x \in \Lambda} d_p(x).$$

The following theorem gives us a relation between the minimum product distance of an ideal lattice Λ and its determinant:

Theorem 10. (OGGIER, 2005) *Let $\mathscr{A}$ be a principal ideal of O_K. The minimum product distance of an ideal lattice Λ, with determinant $D = Det(\Lambda)$, defined over $\mathscr{A}$ is*

$$d_{p,min}(\Lambda) = \sqrt{\frac{D}{d_K}},$$

where d_K is the discriminant related to K.

Now let $\mathbb{Q}(\xi)$, where $\xi = \xi_{2^r}$. We have the following important result:

Proposition 5. (OGGIER, 2005) *Consider the ideal lattice $\Lambda^c = (O_L, b)$, where $L = \mathbb{Q}(\xi)$ 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 $x, y \in O_L$. Then Λ^c is isomorphic to the $\mathbb{Z}[i]^n$-lattice.*

2.3.6 Complex ideal lattices

We have that all the theory explained by considering lattices over $\mathbb{Z}$ is also applied to lattices over $\mathbb{Z}[i]$.

A *complex lattice* is given by

$$\Lambda^c = \{x = \lambda M \mid \lambda \in \mathbb{Z}[i]^n\},$$

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

Definition 22. *Let K and $^- : K \to K$ be a number field and an additive and multiplicative map,*

respectively. We say that the map $^- : K \to K$ *is a* $\mathbb{Q}$*-linear involution of* K *if* $\bar{\bar{x}} = x$*, 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 L be an extension of degree n over $\mathbb{Q}(i)$ endowed with an involution given by complex conjugation. Let O_L be the ring of integers of L. Since $\mathbb{Z}[i]$ is principal, O_L is a free $\mathbb{Z}[i]$-module of rank n.

Definition 23. *A complex ideal lattice is a* $\mathbb{Z}[i]$*-lattice* $\Lambda^c = (I, b)$*, where* I *is an* O_L*-ideal and*

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

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

We denote by $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ 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

$$\sigma : L \Rightarrow \mathbb{C}^n, \text{ with } \sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)).$$

Let $\{w_1, \ldots, w_n\}$ be a $\mathbb{Z}[i]$-basis of $I \subset O_L$. The generator matrix of the complex algebraic lattice $\sigma(I)$ is

$$M = \begin{pmatrix} \sigma_1(w_1) & \ldots & \sigma_n(w_1) \\ \vdots & & \vdots \\ \sigma_1(w_n) & \ldots & \sigma_n(w_n) \end{pmatrix}. \tag{8}$$

The following lemma shows us that complex ideal lattices are well-defined via their generator matrix M:

Lemma 3. (OGGIER, 2005) *The matrix* M *as defined in* (8) *is the generator matrix of a complex ideal lattice if, and only if, complex conjugation commutes with all* $\sigma_j,\ j = 1, 2, \ldots, n$*.*

Definition 24. *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*.*

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

Remark 4. (OGGIER, 2005) *If we take* L *a CM field, then complex conjugation commutes with all* $\sigma_j,\ j = 1, 2, \ldots, n$*.*

3 ON THE CONSTRUCTION OF PERFECT CODES FROM *HEX* SIGNAL CONSTELLATIONS

3.1 Introduction

Recently, minimum and non-minimum delay perfect codes were proposed for any channel of dimension n. Their construction appears in the literature (ELIA; SETHURAMAN; KUMAR, 2007) as a subset of cyclic division algebras over $\mathbb{Q}(\xi_3)$ only for the dimension $n = 2^s n_1$, where $s \in \{0,1\}$, n_1 is odd and the signal constellations are isomorphic to $\mathbb{Z}[\xi_3]^n$.

In this chapter, we review the cyclic division algebra and we propose an innovative methodology to extend the construction of minimum and non-minimum delay perfect codes as a subset of cyclic division algebras over $\mathbb{Q}(\xi_3)$, where the signal constellations are isomorphic to the hexagonal $\mathscr{A}_2^n$ -rotated lattice, for any channel of any dimension n such that $gcd(n,3) = 1$, where $\mathscr{A}_2 = \mathbb{Z}[\xi_3]$.

In (OGGIER et al., 2006), perfect codes have been built algebraically by using cyclic division algebras and their existence is shown in dimensions $2,4$ and $3,6$. The considered codes are subsets of cyclic division algebras over the number fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\xi_3)$, respectively.

(ELIA; SETHURAMAN; KUMAR, 2007) generalized the procedure of the construction of perfect codes and showed their existence for any dimension when the considered codes are subsets of cyclic division algebras over the number field $\mathbb{Q}(i)$. However, in (ELIA; SETHURAMAN; KUMAR, 2007), the authors proposed a construction of perfect codes from cyclic division algebras over the number field $\mathbb{Q}(\xi_3)$ only for the dimension $n = 2^s n_1$, with $s \in \{0,1\}$ and n_1 is odd. For doing such a generalization we have the concept of perfect space-time codes that was introduced in (OGGIER et al., 2006) by the following definition:

Definition 25. (OGGIER et al., 2006) *A square $n_t \times n_t$ STBC is called a perfect code if and only if*

1. *the code is a full-rate linear dispersion code, where the $(n_t l)$ coefficients that representing the message symbols are drawn from the QAM or HEX constellations;*
2. *for every pair X_1, X_2 of distinct code matrices, the determinant $det(\Delta X \Delta X^t, \Delta X = X_1 - X_2)$, prior to SNR normalization, is lower bounded by a constant that is greater than zero and independent of the code size;*
3. *the energy required to send the linear combination of the information symbols on each layer is similar to the energy used for sending the symbols themselves (we do not increase*

the energy of the system in encoding the information symbols);

4. *it induces uniform average transmitted energy per antenna in all l time slots, i.e., all the coded symbols in the code matrix have the same average energy.*

In the constructions of perfect codes in (ELIA; SETHURAMAN; KUMAR, 2007), the authors meet the property (3) by ensuring that the signalling set, obtained by the code matrix vectorization, is isometric to either QAM^{n^2} (isomorphic to the $\mathbb{Z}[i]^n$-rotated lattice) or HEX^{n^2} (isomorphic to the $\mathscr{A}_2^n$-rotated lattice, where $\mathscr{A}_2 = \mathbb{Z}[\xi_3]$). The procedure of the construction of perfect codes in (ELIA; SETHURAMAN; KUMAR, 2007) is a consequence of the existence of $\mathbb{Z}^n$-rotated lattices (BAYER-FLUCKIGER; OGGIER; VITERBO, 2004) from cyclic extensions of $\mathbb{Q}$ with odd degree n.

Andrade and Carvalho (ANDRADE; CARVALHO, 2011) presented cyclic constructions of full diversity rotated $\mathbb{Z}^n$-lattice constellations based on algebraic number theory constructions using the theory of ideal lattices (BAYER-FLUCKIGER; OGGIER; VITERBO, 2006), where n is any dimension. These rotated lattices were constructed through cyclic extension field of prime degree based on cyclotomic fields (WASHINGTON, 1997). So we extended the procedure of the construction of perfect codes from cyclic division algebras over $\mathbb{Q}(\xi_3)$ for the family of dimension n, where n is any even degree such that 3 does not divide n.

3.2 Cyclic algebras and space-time codes

Let K/F be a cyclic extension of degree n with Galois group $G =< \sigma >$, where σ is the generator of the cyclic group and $\mathscr{A} = (K/F, \sigma, \gamma)$ is its corresponding cyclic algebra of degree n, that is,

$$\mathscr{A} = 1 \cdot K \oplus e \cdot K \oplus \cdots \oplus e^{n-1} \cdot K,$$

with $e \in \mathscr{A}$ such that $le = e\sigma(l)$, for all $l \in K$ and $e^n = \gamma \in F^* = F - \{0\}$.

Cyclic algebras provide families of matrices by associating an element $x \in \mathscr{A}$ to the matrix of multiplication by x. For all $x_k \in K$, it follows that

$$x_k \leftrightarrow \begin{pmatrix} x_k & 0 & \cdots & 0 \\ 0 & \sigma(x_k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma^{n-1}(x_k) \end{pmatrix}$$

and

$$e \leftrightarrow \Gamma = \begin{pmatrix} 0 & 0 & \cdots & 0 & \gamma \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Formally we can associate a matrix to any element $x \in \mathscr{A}$ by using the map $\lambda_x : \mathscr{A} \to \mathscr{A}$ defined by $\lambda_x(y) = xy$, where $y \in \mathscr{A}$. The matrix related to λ_x, with $x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1}$, is given by

$$X = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{9}$$

Therefore, via λ_x, we have a matrix representation of an element $x \in \mathscr{A}$.

Remark 5. *The definition of the norm can also be calculated for any element of a cyclic algebra $\mathscr{A}$, i.e., if $x \in \mathscr{A}$, then the reduced norm of x is given by the determinant of its corresponding matrix X (*68*).*

For the purpose of constructing STBCs as a subset of a cyclic algebra $\mathscr{A}$ with the property of the rank criterion, we consider $\mathscr{A}$ as a cyclic division algebra, that is, a cyclic algebra that satisfies the property of division algebra, i.e, when all its non-zero elements are invertible and hence the codeword matrices have nonzero determinants.

Thus the following proposition is a criterion to decide whether the STBCs satisfy the rank criterion:

Proposition 6. (ALBERT, 1961; SETHURAMAN; RAJAN; SHASHIDHAR, 2003) *The algebra $\mathscr{A} = (K/F, \sigma, \gamma)$ of degree n is a division algebra if the smallest positive integer t such that γ^t is the norm of some element in $K^* = K - \{0\}$ is n.*

Example 4. *Let $\{1, i, j, k\}$ be a basis for a vector space of dimension* 4 *over $\mathbb{R}$. These elements satisfy the rules $i^2 = -1$, $j^2 = -1$, $k^2 = -1$ and $k = ij = -ji$. The Hamilton's quaternions is the set $\mathscr{H}$ defined by*

$$\mathscr{H} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}.$$

It has a structure of ring, since addition and multiplication are well-defined, though one has to be careful about the noncommutativity when doing computations.

Let us now prove that the Hamilton's quaternions are a division algebra, that is, every nonzero element $q \in \mathscr{H}$ is invertible. Like for complex numbers, one can define the conjugate

of a quaternion $q = x + yi + zj + wk$ *as*

$$\overline{q} = x - yi - zj - wk.$$

It is a straightforward computation to check that

$$q\overline{q} = x^2 + y^2 + z^2 + w^2.$$

We call $\overline{q}q = q\overline{q} = |q|^2 = N(q)$ *the norm of a quaternion. Since* $x, y, z, w \in \mathbb{R}$, $q\overline{q} > 0$, *unless* $x = y = z = w = 0$. *Thus the inverse of a quaternion* q *is given by*

$$q^{-1} = \frac{\overline{q}}{q\overline{q}},$$

and all nonzero elements have an inverse.

The most famous example of noncommutative field is the Hamilton's quaternions

Other important results for the study of the norm of any element of a cyclic algebra $\mathscr{A}$ are given by the following proposition and its corresponding corollary:

Proposition 7. (OGGIER et al., 2006) *If* $\mathscr{A} = (K/F, \sigma, \gamma)$ *is a cyclic algebra, then the reduced norm of an element of* $\mathscr{A}$ *belongs to* F.

Corollary 3. (OGGIER et al., 2006) *Let* $\mathscr{A} = (K/F, \sigma, \gamma)$ *be a cyclic algebra. If* $x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1}$, *where* $x_0, \ldots, x_{n-1} \in \mathscr{O}_K$ *and* $\gamma \in \mathscr{O}_K$, *then the reduced norm of* x *belongs to* $\mathscr{O}_F$.

Based on the concept of factorization of an ideal $p\mathscr{O}_F$ in cyclotomic number fields K, we will give some examples of constructions of cyclic division algebras $(K/F, \sigma, \gamma)$. For that we present the following results:

Lemma 4. (KIRAN; RAJAN, 2005) *Let* K *be a degree-*n *Galois extension of a number field* F. *If* $\mathscr{P}$ *is a prime ideal in* $\mathscr{O}_F$ *such that the ideal* $\beta = \mathscr{P}\mathscr{O}_K$ *is a prime ideal in* $\mathscr{O}_K$, *then* $N_{K/\mathbb{Q}}(\beta) = (N_{K/F}(\mathscr{P}))^n$.

Theorem 11. (KIRAN; RAJAN, 2005) *Let* K *be a degree-*n *Galois extension of a number field* F *and let* $\mathscr{P}$ *be a prime ideal in* $\mathscr{O}_F$ *that is below the prime ideal* $\beta \subset \mathscr{O}_K$ *such that* $N_{K/\mathbb{Q}}(\beta) = (N_{K/F}(\mathscr{P}))^f$. *If* γ *is any element of* $\mathscr{P} \setminus \mathscr{P}^2$, *then* $\gamma^j \neq N_{K/F}(x)$, *for all* $x \in K^* = K - \{0\}$ *and* $j = 1, 2, \ldots, f-1$.

Theorem 12. (KIRAN; RAJAN, 2005) *If* $gcd(p, m) = 1$, *then the ideal* $p\mathbb{Z}[\xi_m]$ *split into* $\varphi(m)/f$ *distinct prime ideals in* $\mathbb{Z}[\xi_m]$, *where* f *is the multiplicative order of* p *modulo* m.

Remark 6. *Kiran and Rajan* (KIRAN; RAJAN, 2005) *showed that if* $Gal(K/F) = \langle\sigma\rangle$, *with* $[K : F] = n$, *then the cyclic algebra* $(K/F, \sigma, \gamma)$ *is a division algebra if* $\gamma \in \mathscr{P} \setminus \mathscr{P}^2$, *for some*

prime triplet $(p, \mathscr{P}, \beta)$*, with* $f(\beta|\mathscr{P}) = n$*, where* p *is and integer prime,* $\mathscr{P}$ *is a prime ideal in* $\mathscr{O}_F$ *and* β *is a prime ideal in* $\mathscr{O}_K$*.*

Now we have the following example of construction of cyclic division algebras:

Example 5. *Let* K *be the cyclotomic number field given by* $K = \mathbb{Q}(\xi_{2^{s+2}})$*, for* $s \geq 1$ *and* $F = \mathbb{Q}(i)$*. Let* β_1 *be one of the primes in* $\mathbb{Z}[\xi_{2^{s+2}}]$*, which lies above* $p = 5$*. The multiplicative order of* 5 *module* 2^{s+2} *is equal to* $f(\beta_1|p) = 2^s$*. Since* $gcd(5, 2^{s+2}) = 1$ *in* $\mathbb{Z}[\xi_{2^{s+2}}]$*, by Theorem 12, it follows that the ideal* $5\mathbb{Z}[\xi_{2^{s+2}}]$ *splits into* $\varphi(2^{s+2})/f(\beta_1|p) = 2$ *distinct prime ideals,* β_1 *and* β_2 *(see,* (KIRAN; RAJAN, 2005)*, p. 2989 for details). If* $\mathscr{P} = \beta_1 \cap \mathbb{Z}[i]$ *is the unique prime ideal in* $\mathbb{Z}[i]$ *below* β_1 *and since* $5 = (2+i)(2-i)$ *in* $\mathbb{Z}[i]$*, then* $\mathscr{P}$ *is equal to either* $(2+i)\mathbb{Z}[i]$ *or* $(2-i)\mathbb{Z}[i]$*. Without loss of generality, we assume* $\mathscr{P} = (2+i)\mathbb{Z}[i]$*. Further, since* 5 *splits into two factors and* $[\mathbb{Q}(i) : \mathbb{Q}] = 2$*, it follows that* $f(\mathscr{P}|p) = 1$*. From Theorem 11 and Remark 6 we have that* $(5; (2+i)\mathbb{Z}[i]; \beta_1)$ *is a prime triplet with* $f(\beta_1|\mathscr{P}) = f(\beta_1|p)/f(\mathscr{P}|p) = 2^s/1 = 2^s$*. Therefore, for each* $s \geq 1$*, there are families of cyclic division algebras given by* $(K/F, \sigma, \gamma)$ *(see* (KIRAN; RAJAN, 2005) *for details).*

Based on Theorem 11 and Remark 6 we will find, in the following proposition, a new family of cyclic division algebras:

Proposition 8. *Let* K *be a cyclotomic number field given by* $K = \mathbb{Q}(\xi_{3^{s+1}})$*, for* $s \geq 1$*. If* $F = \mathbb{Q}(\xi_3)$*, then there is a* $\gamma \in \mathscr{O}_F$ *such that* $\gamma^j \neq N_{K/F}(x)$*, for all* $x \in K^* = K - \{0\}$ *and* $j = 1, 2, \ldots, 3^s - 1$*, and there is a family of cyclic division algebras* $(K/F, \sigma, \gamma)$*.*

Proof. Let β_1 be one of the primes in $\mathbb{Z}[\xi_{3^{s+1}}]$ which lies above $p = 7$. The multiplicative order of 7 module 3^{s+1} is equal to $f(\beta_1|p) = 3^s$ (see (KIRAN; RAJAN, 2005), p. 2990 for details). Since $gcd(7, 3^{s+1}) = 1$ in $\mathbb{Z}[\xi_{3^{s+1}}]$, by Theorem 12, it follows that the ideal $7\mathbb{Z}[\xi_{3^{s+1}}]$ splits into $\varphi(3^{s+1})/f(\beta_1|p) = 2$ distinct prime ideals β_1 and β_2 (see (KIRAN; RAJAN, 2005), p. 2990 for details). If $\mathscr{P} = \beta_1 \cap \mathbb{Z}[\xi_3]$ is the unique prime in $\mathbb{Z}[\xi_3]$ below β_1, since $7 = (3+\xi_3)(2-\xi_3)$ in $\mathbb{Z}[\xi_3]$, then $\mathscr{P}$ is equal to either $(3+\xi_3)\mathbb{Z}[\xi_3]$ or $(2-\xi_3)\mathbb{Z}[\xi_3]$. Without loss of generality we assume $\mathscr{P}\mathbb{Z}[\xi_3] = (3+\xi_3)\mathbb{Z}[\xi_3]$. Further, since 7 splits into two factors and $[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2$, it follows that $f(\mathscr{P}|p) = 1$. From Theorem 11 and Remark 6 we have that $(7; (3+\xi_3)\mathbb{Z}[\xi_3]; \beta_1)$ is a prime triplet with $f(\beta_1|\mathscr{P}) = f(\beta_1|p)/f(\mathscr{P}|p) = 3^s/1 = 3^s$. Therefore, for each $s \geq 1$, we find families of cyclic division algebras $(K/F, \sigma, \gamma)$. □

Based on the construction given by Example 5, (ELIA; SETHURAMAN; KUMAR, 2007) proposed a new family of cyclic division algebras given by the following example:

Example 6. *Let* K *be a cyclotomic number field given by* $K = \mathbb{Q}(\xi_{2^{s+2}})$*, for* $s \geq 1$ *and* $F = \mathbb{Q}(i)$*. By Example 2 we have that* K/F *is a cyclic field extension of degree* 2^s*. By Example 5, for each* s*, it follows that* $\beta_1 = 2+i$ *and* $\beta_2 = 2-i$ *are distinct primes ideals in* $\mathbb{Z}[\xi_{2^{s+2}}]$ *such that* β_1^j *and*

$\beta_2^j \neq N_{K/F}(x)$, for all $x \in K-\{0\}$ and $j = 1,2,\ldots,2^s-1$, and, for each integer s, we find γ given by $\gamma = \frac{\beta_1}{\beta_2}$ such that $|\gamma| = 1$ and $\gamma = (\frac{\beta_1}{\beta_2})^j \neq N_{K/F}(x)$, for all $x \in K-\{0\}$ and $j = 1,2,\ldots,2^s-1$. Therefore, for each $s \geq 1$, we find a family of cyclic division algebras $(K/F,\sigma,\gamma)$.

3.2.1 Space-time codes from cyclic division algebras

Let $F = \mathbb{Q}(i)$ or $F = \mathbb{Q}(\xi_3)$. Let K and σ be a n-degree cyclic Galois extension of F and a generator of the Galois group $Gal(K/F)$, respectively.

Now let $\{\beta_1,\ldots,\beta_n\}$ form an integral basis for $\mathscr{O}_K/\mathscr{O}_F$ and define the sets

$$\mathscr{A}_{QAM}(\beta_1,\ldots,\beta_n) = \{\sum_i a_i\beta_i \mid a_i \in \mathscr{A}_{QAM}\}$$

and

$$\mathscr{A}_{HEX}(\beta_1,\ldots,\beta_n) = \{\sum_i a_i\beta_i \mid a_i \in \mathscr{A}_{HEX}\},$$

where $\mathscr{A}_{QAM}$ and $\mathscr{A}_{HEX}$ are the *QAM* and *HEX* constellations, respectively.

Notice that the sets $\mathscr{A}_{QAM}(\beta_1,\ldots,\beta_n)$ and $\mathscr{A}_{HEX}(\beta_1,\ldots,\beta_n)$ are linear combinations of the basis elements β_i with coefficients lying in $\mathscr{A}_{QAM}$ and $\mathscr{A}_{HEX}$, respectively.

By (SETHURAMAN; RAJAN; SHASHIDHAR, 2003), a STBC can be obtained as

$$\mathscr{C} = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix} : \text{ for all } x_i \in K \right\}. \tag{10}$$

Now since each codeword X contains n coefficients x_i and each one of them being a linear combination of n information symbols, it follows that cyclic algebras naturally yields full-rate STBCs.

All the coefficients of such matrices are in K, thus each x_i is a linear combination of n elements in F, therefore the information symbols are chosen to be in F.

Oggier et al. (OGGIER et al., 2006) showed that the STBCs obtained as the subset of the space matrices (70) are linear-dispersion space-time codes and can be seen from the expansion below

$$X = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_{ij}\Gamma^i diag(\beta_j,\sigma(\beta_j),\ldots,\sigma^{n-1}(\beta_j)), \tag{11}$$

where $f_{ij} \in \mathscr{A}_{QAM}$ or $f_{ij} \in \mathscr{A}_{HEX}$ and the cyclic-shift-and-multiply-at-end- by-γ matrix Γ is given by

$$\Gamma = \begin{pmatrix} 0 & 0 & \cdots & 0 & \gamma \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Developing the sum on j, we obtain

$$X = \sum_{i=0}^{n-1} \Gamma^i diag(l_i, \sigma(l_i), \ldots, \sigma^{n-1}(l_i)), \tag{12}$$

where $l_i = \sum_{j=0}^{n-1} f_{ij}\beta_j$.

In order to show that the signal constellation has the property of good shaping, (ELIA; SETHURAMAN; KUMAR, 2007) used the fact that the sets $\{lay(X)|,\ X \in \mathscr{A}_{QAM}\}$ and $\{lay(X)|,\ X \in \mathscr{A}_{HEX}\}$ are isometric to the sets $\mathscr{A}_{QAM}^{n^2}$ and $\mathscr{A}_{HEX}^{n^2}$, respectively. We can rearrange the entries of the code matrix X in a layer by layer fashion to form a vector $lay(X) = \lambda f$, where $lay(X)$ is given by the matrix

$$\begin{pmatrix} l_0 \\ \sigma(l_0) \\ \sigma^2(l_0) \\ \vdots \\ l_{n-1} \\ \gamma\sigma(l_{n-1}) \\ \gamma\sigma^2(l_{n-1}) \\ \vdots \end{pmatrix} \tag{13}$$

and we also have

$$\lambda f = \begin{pmatrix} B_0 G & & \\ & \ddots & \\ & & B_{n-1} G \end{pmatrix}, \tag{14}$$

where

$$G = \begin{pmatrix} \beta_0 & \cdots & \beta_{n-1} \\ \sigma(\beta_0) & \cdots & \sigma(\beta_{n-1}) \\ & \vdots & \\ \sigma^{n-1}(\beta_0) & \cdots & \sigma^{n-1}(\beta_{n-1}) \end{pmatrix} \tag{15}$$

and B_i is given by

$$B_i = diag(1, \ldots, 1, \gamma, \ldots, \gamma),$$

where 1 appears in the first $n-i$ entries and γ appears in the next i entries, for $i = 0, 1, \ldots, n-1$.

It is possible to choose an integral basis $\{\beta_1,\ldots,\beta_n\}$ such that the normalized matrix is given by

$$U(G)=\kappa G,$$

where $\kappa\in F$.

3.2.2 Non-vanishing determinant property

In (ELIA; SETHURAMAN; KUMAR, 2007) we have that the determinant of every matrix that represents an element of a cyclic algebra lies in $F=\mathbb{Q}(i)$ or $\mathbb{Q}(\xi_3)$. They also showed that if $\gamma=\frac{a}{b}$, where $a,b\in\mathscr{O}_F$, by scaling the entries of the columns $2,3,\ldots,n$ of a code matrix in the space-time code $\mathscr{C}$ by the element $b\in\mathscr{O}_F$, then the entries in the scaled matrix lies in $\mathscr{O}_K$. Thus the determinant of a scaled matrix lies in $\mathscr{O}_K\cap F=\mathscr{O}_F$.

Therefore the determinant of the unscaled matrices lies in the set $\frac{1}{b^{n-1}}\mathscr{O}_F$ and, in this set, the magnitude of every element is bounded below by $\frac{1}{|b|^{n-1}}$. So the non-vanishing determinant property of the STBCs constructed follows since the difference of any two elements is in the cyclic division algebra.

We can see that the main difference between the works (OGGIER et al., 2006; ELIA; SETHURAMAN; KUMAR, 2007) is that (OGGIER et al., 2006) only chooses the non-norm element γ to be a root of unity in $\mathscr{O}_K$, while (ELIA; SETHURAMAN; KUMAR, 2007) uses elements with denominators. If one fixes the constraint that γ is indeed a root of unity, then the codes cannot exist in other dimensions than $2,3,4,6$, as shown by Berhuy et al. (BERHUY; OGGIER, 2009).

3.2.3 Constellation shaping and uniform energy property

In this section, we extend the procedure of the construction of perfect codes given in (ELIA; SETHURAMAN; KUMAR, 2007). Notice that if we want to construct a perfect code $\mathscr{C}$ such that $\mathscr{C}$ is isometric to either the set $\mathscr{A}_{QAM}^{n^2}$ or the set $\mathscr{A}_{HEX}^{n^2}$, then by Equations (12), (13), (14), (15) and Proposition 6 it is necessary to consider the unitary matrix $U(G)$ and the element $\gamma\in F^*$ such that $|\gamma|=1$ and $\gamma^i\neq N_{K/F}(x)$, for all $x\in K^*=K-\{0\}$ and $i=1,\ldots,n-1$, where K/F is a n-degree cyclic extension. So, after that, we consider the cyclic division algebra $\mathscr{A}=(K/F,\sigma,\gamma)$ associated to this construction.

Boutros and Viterbo (BOUTROS; VITERBO, 1998) proposed a procedure to construct unitary matrices isomorphic to the $\mathbb{Z}[i]^n$- lattice (cubic form) for the dimension $n=2^{s_1}3^{s_2}$, where $s_1,s_2\in\{0,1,\cdots\}$. Based on this construction, Elia et al. proposed a new family of perfect codes for the specific case $n=2^s n_1$, where n_1 is odd, and here we describe this family in the following example:

Example 7. *Let K/F be a $n = 2^s$-degree cyclic Galois extension, where $K = \mathbb{Q}(\xi_{2^{s+2}})$, for $s \geq 1$, and $F = \mathbb{Q}(i)$. By* (BOUTROS; VITERBO, 1998)*, for each $s \geq 1$, there is a unitary matrix $U(G)$ isomorphic to the $\mathbb{Z}[i]^{2^s}$-lattices of the form $U(G) = \kappa G$, where G is given by the matrix (15). Let σ be a generator of the Galois group associated to the extension K/F. For each positive integer s, there are $\gamma \in F^*$ such that γ is a non-norm element given by the Example 6 and a perfect code from the cyclic division algebra $\mathscr{A} = (K/F, \sigma, \gamma)$.*

Based on the constructed $\mathbb{Z}^n$-rotated lattices obtained from the n_1-degree cyclic extension field $L/\mathbb{Q}$, (ELIA; SETHURAMAN; KUMAR, 2007) proposed a family of perfect codes given by the following example:

Example 8. *Let K/F be a n_1-degree cyclic Galois extension, where n_1 is odd and $F = \mathbb{Q}(i)$. Thus, there is a unitary matrix $U(G)$ of the form $U(G) = \kappa G$ isomorphic to the $\mathbb{Z}[i]^{n_1}$-lattice, where G is given by the matrix (15). Let σ be a generator of the Galois group associated to the field extension K/F. Then there are $\gamma \in F^*$ such that γ is a non-norm element given by the Example 6 and a perfect code from the cyclic division algebra $\mathscr{A} = (K/F, \sigma, \gamma)$.*

Based on the procedure of the construction of perfect codes in the Examples (7) and (8), Elia et al. obtained a general procedure for the construction of perfect codes from the cyclic field extension K/F of degree $n = 2^s n_1$, where n_1 is odd:

Example 9. *Let K/F be a $n = 2^s n_1$-degree cyclic Galois extension, where n_1 is odd and $F = \mathbb{Q}(i)$. Thus there is a unitary matrix $U(G)$ of the form $U(G) = \kappa G$ isomorphic to the $\mathbb{Z}[i]^{2^s n_1}$-lattice, where G is given by the matrix (15). Let σ be a generator of the Galois group associated to the field extension K/F. For each positive integer s, there are $\gamma \in F^*$ such that γ is a non-norm element given by the Example 6 and a perfect code from the cyclic division algebra $\mathscr{A} = (K/F, \sigma, \gamma)$.*

For the case $F = \mathbb{Q}(\xi_3)$, (ELIA; SETHURAMAN; KUMAR, 2007) constructed families of perfect codes from a $n = 2^s n_1$-degree cyclic field extension K/F, with $s \in \{0, 1\}$. For this case, the unitary matrices $U(G)$ are isomorphic to the $\mathbb{Z}[\xi_3]^{2^s n_1}$-lattice.

Recently, Andrade and Carvalho (ANDRADE; CARVALHO, 2011) proposed an explicit construction of unitary matrices for the case $n = n_2$, where n_2 is an even positive integer. Then since $\mathbb{Q}(w_p)$ and $\mathbb{Q}(\xi_3)$ are linearly disjoint over $\mathbb{Q}$, where $w_p = e^{\frac{2\pi i}{p}}$, the field $L = L_1(\xi_3)$ (see appendix A) will be cyclic over $\mathbb{Q}(\xi_3)$ and the elements $x, \sigma(x), \ldots, \sigma^{n_2-1}(x)$ will be an integral basis for $L/\mathbb{Q}(\xi_3)$. So we have a family of unitary matrices isomorphic to the $\mathscr{A}_2^{n_2}$-lattice when n_2 is an even positive integer.

In the appendix B we have the procedure of the construction of unitary matrices for the case $n = 3^s$ and $F = \mathbb{Q}(\xi_3)$, where $s \geq 1$. However, in this case, these unitary matrices are isomorphic to the $\mathscr{A}_2^n$-lattice.

Therefore when we apply the Kronecker product on the resulting matrices, that is, for the cases $n = 3^s$ and $n = n_2$, it will yield us a unitary matrix $U(G)$ for the general case $n = 3^s n_2$.

Observe that, in this work, we will restrict our attention to the *HEX* case, that is, when $F = \mathbb{Q}(\xi_3)$. Now we will present the following propositions:

Proposition 9. *Let K be a cyclotomic number field given by $K = \mathbb{Q}(\xi_{3^{s+1}})$, with $s \geq 1$ and $F = \mathbb{Q}(\xi_3)$. In this case there are unitary matrices $U(G)$ of the form $U(G) = \kappa G$ isomorphic to the $\mathbb{Z}[\xi_3]^{3^s}$-lattice, where G is given by the matrix (15). Let σ be a generator of the Galois group associated to the extension K/F. Then, for each positive integer s, there are $\gamma \in F^*$ such that γ is a non-norm element in the cyclic field extension K/F and a perfect code from the cyclic division algebra $\mathscr{A} = (K/F, \sigma, \gamma)$.*

Proof. By the Example 2 we have that K/F is a 3^s-degree cyclic field extension. For each s, by Proposition 8, we find $\beta_1 = 3 + \xi_3$ and $\beta_2 = 2 - \xi_3$ being distinct prime ideals in $\mathbb{Z}[\xi_{3^{s+1}}]$ such that β_1^j and $\beta_2^j \neq N_{K/F}(x)$, for all $x \in K - \{0\}$ and $j = 1, 2, \cdots, 3^s - 1$. Thus, for each integer s, we find $\gamma = \frac{\beta_1}{\beta_2}$ such that $|\gamma| = 1$ and $\gamma^j \neq N_{K/F}(x)$, for all $x \in K - \{0\}$ and $j = 1, 2, \cdots, 3^s - 1$. Therefore, for each $s \geq 1$, we find a family of cyclic division algebras $(K/F, \sigma, \gamma)$. Finally, in the Appendix 2, we find unitary matrices $U(G)$ isomorphic to the $\mathscr{A}_2^n$-lattice for the dimension $n = 3^s$. □

Proposition 10. *Let $F = \mathbb{Q}(\xi_3)$ and K be a cyclotomic number field given by $K = \mathbb{Q}(\xi_p)$, where $p \equiv 1 \ (mod\ n_2)$, $gcd(n_2, 3) = 1$ and n_2 is an even positive integer. In this case, there are unitary matrices $U(G_{n_2})$ of the form $U(G_{n_2}) = \kappa G_{n_2}$ isomorphic to the $\mathbb{Z}[\xi_3]^{n_2}$-lattice, where G_{n_2} is given by matrix (15). Let σ be a generator of the Galois group associated to the extension K/F. Then there are $\gamma \in F^*$ such that γ is a non-norm element in the cyclic extension field K/F and a perfect code from the cyclic division algebra $\mathscr{A} = (K/F, \sigma, \gamma)$.*

Proof. The proof of this proposition follows directly from the results of Andrade and Carvalho (ANDRADE; CARVALHO, 2011). So we need the following steps:

1. Pick an odd prime $p \equiv 1 (mod\ n_2)$ (by a theorem of Direchlet);
2. Let $\omega = \xi_p = e^{\frac{2\pi i}{p}}$. Let σ be a generator of the cyclic Galois group $\mathbb{Q}(\omega)/\mathbb{Q}$;
3. Let r be a primitive element of the field $\mathbb{Z}_p^*$;
4. Let $m = \frac{p-1}{2}$ and $\alpha = \prod_{k=0}^{m-1}(1 - \omega^{r_k})$;
5. Take λ such that $\lambda(r-1) \equiv 1 (mod\ p)$ and take $z = \omega^\lambda \alpha(1 - \omega)$;
6. Let σ be an automorphism defined by $\sigma(\omega) = \omega^r$ and set $x = \prod_{k=1}^{\frac{p-1}{n_2}} \sigma^{kn_2}(z)$.

The element x lies in the subfield K_1 of $\mathbb{Q}(\omega)$ fixed by the subgroup $\langle\sigma^{n_2}\rangle$ generated by σ^{n_2}. This subfield K_1 is an extension of $\mathbb{Q}$ of degree n_2. Then the matrix $U(G_{n_2})$ is unitary and given by

$$U(G_{n_2}) = \begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{n_2-2}(x) & \sigma^{n_2-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & \sigma^{n_2-1}(x) & x \\ \sigma^2(x) & \sigma^3(x) & \cdots & x & \sigma(x) \\ & \vdots & & \vdots & \\ \sigma^{n_2-1}(x) & x & \cdots & \sigma^{n_2-3}(x) & \sigma^{n_2-2}(x) \end{pmatrix}. \tag{16}$$

Since $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\xi_3)$ are linearly disjoint over $\mathbb{Q}$, it follows that $K = K_1(\xi_3)$ is a cyclic extension field over $\mathbb{Q}(\xi_3)$ and the elements $x, \sigma(x), \ldots, \sigma^{n_2-1}(x)$ form an integral basis for $K/\mathbb{Q}(\xi_3)$. More specifically, the first row of $U(G_{n_2})$ is given by

$$U(G_{n_2})(0,j) = \frac{1}{p}\omega^{\lambda}\alpha\prod_{k=1}^{\frac{p-1}{n_2}}(-1)^{n_2k+j}(1-\omega^{r^{n_2k+j}}),$$

for $j = 0, \cdots, n_2 - 1$ and the rest of the circulant matrix is given by

$$U(G_{n_2})(i+1,j) = U(G_{n_2})(i, j+1 \ (mod\ n_2),$$

for $i = 0, \cdots, n_2 - 2$.

Now an algorithm to construct an ideal lattice is given by:

1. Choose an even dimension n_2;
2. Compute a prime p such that $p \equiv 1 \ (mod\ n_2)$ and $n_2 | \frac{p-1}{2}$;
3. Compute r and λ such that r is a primitive element modulo p and $\lambda(r-1) \equiv 1 \ (mod\ p)$;
4. Compute α and z in the basis $\{1, \omega, \ldots, \omega^{p-2}\}$ of the cyclotomic field;
5. Compute x and its conjugates in the basis of the cyclotomic field;
6. Compute M the matrix of the lattice, which contains as first column $\sigma^i(x)$, for $i = 0, 1, \ldots, n_2 - 1$, and as other columns a cyclic shift of the first column;
7. Finally, normalize the matrix M to get the determinant equal to 1.

In Appendix 1 we can see that when we can take $\gamma = \frac{\beta_1}{\beta_2}$ in the way given by Proposition 3.4, we find $\gamma \in F$ such that $|\gamma| = 1$ and $\gamma^j \neq N_{K/F}(x)$, for all $x \in K - \{0\}$ and $j = 1, \ldots, n_2 - 1$. □

Now we consider the general case $n = 3^s n_2$. So we will need the following lemma:

Lemma 5. (ELIA; SETHURAMAN; KUMAR, 2007) *Let K be a composition of l Galois extensions L_i over $\mathbb{Q}$ of co-prime degrees n_i. Assuming that there exist unitary matrices $U(G_{n_i})$, for all $i = 1,2,\cdots,l$, it follows that the Kronecker product of these matrices is a unitary matrix of order $n \times n$ given by $U(G_n)$, where $n = \prod_{i=1}^{l} n_i$. In particular, when $n = 3^s n_2$ and $F = \mathbb{Q}(\xi_3)$, we can use the Kronecker product of these matrices constructed separately for the cases $n = n_2$, where n_2 is an even integer, and $n = 3^s$.*

After these conclusions and results we present, in the following proposition, a general result for the construction of perfect codes over HEX constellations:

Proposition 11. *Let K/F be a cyclic Galois extension field of degree $n = 3^s n_2 > 1$, where n_2 is even and $gcd(3,n_2) = 1$. Let σ be a generator of the Galois group associated to extension K/F. Then, for each s, there are $\gamma \in F^*$ such that γ is a non-norm element in the extension K/F and a perfect code $\mathscr{C}$ as a subset of the cyclic division algebra $(K/F, \sigma, \gamma)$.*

3.3 Conclusion

From the arithmetic procedure proposed in (ANDRADE; CARVALHO, 2011) for the construction of $\mathbb{Z}^n$-rotated lattices from cyclic extensions of $\mathbb{Q}$ with even positive degree n, the new class of perfect space-time codes obtained keeps the same properties as the codes proposed by (ELIA; SETHURAMAN; KUMAR, 2007). However, in this case, the good shaping associated to the lattices is given by $\mathscr{A}_2^n$-rotated lattices.

4 CODING FOR THE GAUSSIAN INTERFERENCE CHANNEL

4.1 Introduction

In a wireless network, a transmission from a single node is heard not only by the intended receiver, but also by all other nearby nodes; by analogy, any receiver not only captures the signal from its designated transmitter, but from all other nearby transmitters. The resulting interference is usually viewed as highly undesirable and clever algorithms and protocols have been devised to avoid interference between transmitters.

In a recent work (NAZER; GASTPAR, 2011), Nazer and Gastpar proposed the *compute-and-forward* strategy as a physical-layer network coding scheme. They described a code structure based on nested lattices, whose algebraic structure makes the scheme reliable and efficient. The *compute-and-forward* strategy enables relays to decode linear equations of the transmitted messages using the noisy linear combinations provided by the channel. Each relay, indexed by $m = 1, 2, \ldots, M$, observes a noisy linear combination of the transmitted signals through the channel,

$$y_m = \sum_{l=1}^{L} h_{ml} x_l + z_m, \tag{17}$$

where $h_{ml} \in \mathbb{C}$ are complex-valued channel coefficients, $x_l \in \mathbb{C}^n$ such that $\|x_l\|^2 \leq nP$ (in (NAZER; GASTPAR, 2011), Appendix C, they argue that there exist fixed dithers that meet the power constraint) and z_m is i.i.d. circularly symmetric complex Gaussian noise, $z_m \sim \mathscr{CN}(\mathbf{0}, \mathbf{I}^{M\times M})$. Let $h_m = [h_{m1} \cdots h_{mL}]^T$ denote the vector of channel coefficients to relay m and let $H = \{h_{ml}\}$ denote the entire channel matrix, where T denotes the transpose. Note that by this convention the m^{th} row of H is h_m^T.

The coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself. Specifically, relay m only needs to know h_m. Each transmitter only needs to know the desired message rate, not the realization of the channel.

However, in (NAZER; GASTPAR, 2011) we also have an equivalent channel induced by the modulo-Λ transformation. In this "virtual" channel model each relay observes a $\mathbb{Z}[i]$-combination $\sum a_{ml} t_l$ of the lattice points corrupted by effective noise $z_{eq,m}$, that is,

$$y_m = \sum_{l=1}^{L} a_{ml} t_l + z_{eq,m}. \tag{18}$$

Now, in order to realize interference alignment onto a lattice, we need to quantize the channel coefficients a_{ml}. In this chapter, we are going to explicit two examples of channel quantization, these examples are related to the dimensions 4 and 8 (real) or 2 and 4 (complex) and we will make use of the binary cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{16})$, respectively.

4.2 Lattice Coding

In (NAZER; GASTPAR, 2011), in order to allow relays to decode integer combinations of codewords, Nazer and Gastpar needed codebooks with a linear structure. Specifically, they used nested lattice codes that have both good statistical and good algebraic properties. In (EREZ; ZAMIR, 2004), Erez and Zamir developed a class of nested lattice codes that can approach the capacity of point-to-point AWGN channels. These codes operate under a modulo arithmetic that is well-suited for mapping operations over a finite field to the complex field.

In this work, lattice coding is also done through a nested construction. In order to be able to make private and common data appear at the transmitted signal, all bits are coding some nested lattice partition chain, as explained in (OGGIER; SOLE; BELFIORE, 2011). We can, as an example in dimension $n = 8$, consider the same chain as in (OGGIER; SOLE; BELFIORE, 2011),

$$\mathbb{Z}^8 \supset D_8 \supset D_4^2 \supset L_8 \supset \sqrt{2}E_8 \supset 2L_8^* \supset 2(D_4^2)^* \supset 2D_8^* \supset 2\mathbb{Z}^8, \tag{19}$$

which is periodic up to a scaling factor, or consider a chain of $\mathbb{Z}[i]$-lattice in complex dimension 2,

$$\frac{1}{1+i}\mathbb{Z}[i]^2 \supset \frac{1}{1+i}D_4 \supset \mathbb{Z}[i]^2 \supset D_4 \supset (1+i)\mathbb{Z}[i]^2 \supset (1+i)D_4 \supset 2\mathbb{Z}[i]^2. \tag{20}$$

We remark that in all these inclusions, the considered lattices are always of index 2 as sublattices of the lattice preceeding them. The binary data naturally encode this nested chain, as explained in (OGGIER; SOLE; BELFIORE, 2011).

4.3 Quantization of the Channel Gains

Suppose that our interference channel is complex-valued, specifically $a_{ml} \in \{\mathbb{Z} + i\mathbb{Z}\}$. We suppose that all lattices used by the legitimate user and the interferers are one of a certain lattice partition chain and extended by periodicity. Now the idea we want to develop is that the effect of a channel gain on a given user is to shift the lattice used by the user either to the left, if its channel gain is smaller than 1, or to the right, if it is larger than 1. It is very important that the channel gain does not remove the lattice from the initial chain of nested lattices.

4.3.1 An example in dimension 4 (real) or 2 (complex)

In this section, as we consider 2-dimensional complex valued vectors here, we will use the lattice partition chain defined in (20). So each transmitter is using one of the lattices of this chain (which is extended by periodicity so that it is a doubly infinite chain). Now we write, for a given user, how its codeword can be transformed so that we can perform the channel quantization. We will make use of the binary cyclotomic field $\mathbb{Q}(\xi_8)$.

We will consider the following Galois extensions:

$$\begin{array}{c} L=\mathbb{Q}(\xi_8) \\ \Big| 2 \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{21}$$

As $[\mathbb{Q}(\xi_8):\mathbb{Q}]=\phi(8)=4$, where ϕ is the Euler function, and $[\mathbb{Q}(i):\mathbb{Q}]=2$, then we have $[\mathbb{Q}(\xi_8):\mathbb{Q}(i)]=2$. We have that the Galois groups of $[\mathbb{Q}(\xi_8):\mathbb{Q}(i)]$ and $[\mathbb{Q}(i):\mathbb{Q}]$ are given by

$$Gal(\mathbb{Q}(\xi_8)/\mathbb{Q}(i))=\{\sigma_1=id:\mathbb{Q}(\xi_8)\to\mathbb{Q}(\xi_8) \text{ and } \sigma_2:\mathbb{Q}(\xi_8)\to\mathbb{Q}(\xi_8);\ \sigma_2(\xi_8)=-\xi_8\} \text{ and}$$

$$Gal(\mathbb{Q}(i)/\mathbb{Q})=\{\sigma_1=id:\mathbb{Q}(i)\to\mathbb{Q}(i) \text{ and } \sigma_2:\mathbb{Q}(i)\to\mathbb{Q}(i);\ \sigma_2(i)=-i\},$$

respectively, where *id* is the identity map.

By (OGGIER, 2005), we have $\mathbb{Q}(\xi_8)=\mathbb{Q}(\xi_8+\xi_8^{-1})\mathbb{Q}(i)=\mathbb{Q}(\sqrt{2})\mathbb{Q}(i)$. From proposition 2, it follows that $O_L=\mathbb{Z}[\xi_8]$, the ring of integers of L, is a free $\mathbb{Z}[i]$-module of rank 2 and $\{1,\xi_8\}$ is a $\mathbb{Z}[i]$-basis.

Since $\{1,\xi_8\}$ is a $\mathbb{Z}[i]$-basis of O_L, so the matrix

$$M_0=\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\xi_8) & \sigma_2(\xi_8) \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ \xi_8 & -\xi_8 \end{pmatrix} \tag{22}$$

is the generator matrix of the complex algebraic lattice $\sigma(O_L)$.

Observe that M_0 and $M=M_0^T$ have the same properties. If we take $M_0'=\frac{1}{\sqrt{2}}M_0$, we have $(M_0')(M_0')^H$ equal to the identity matrix, where $(M_0')^H$ denotes the transpose conjugate of M_0'. So $M_0'=\frac{1}{\sqrt{2}}M_0$ is a unitary matrix and using the same argument as before we have that $U=\frac{1}{\sqrt{2}}M_0^T$ is also a unitary matrix.

Therefore, by the proposition 5, $\sigma(O_L)$ is isomorphic to the $\mathbb{Z}[i]^2$-lattice.

At the receiver, we suppose that we apply U to the received vector of (71) to get

$$\bar{y}_m = Uy_m = \sum_{l=1}^{L} a_{ml} U t_l + U z_{eq,m}. \tag{23}$$

As $z_{eq,m}$ is i.i.d. circularly symmetric complex Gaussian noise and U is unitary, then the noise in (66) is also i.i.d. circularly symmetric complex Gaussian. Now let's take a look at the vectors of the form $a_{ml}Ut_l$. For sake of simplicity of notations, we denote it by

$$\bar{x} = h \cdot U \cdot x, \tag{24}$$

where $x = t_l$ is the lattice point transmitted by the considered user and $h = a_{ml}$ is the channel coefficient. We can rewrite it now as

$$\begin{pmatrix} h & 0 \\ 0 & h \end{pmatrix} \cdot U \cdot x = H \cdot U \cdot x. \tag{25}$$

The idea we want to develop is to quantize the diagonal matrix H by the diagonal matrix whose elements are components of the canonical embedding of the power (positive or negative) of an element of O_L with absolute algebraic norm equal to 2.

Observe that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = (1+i)(1-i) = 2$ and $(1+i)^2 = 2i$. As i is a unit in $\mathbb{Q}(i)$, taking as ideals, we have $2\mathbb{Z}[i] = (2) = (2i) = (1+i)^2$ in $\mathbb{Z}[i]$, so 2 is totally ramified in $\mathbb{Q}(i)$ ($2\mathbb{Z}[i] = (2) = (I')^2$, where $I' = (1+i)$).

As $-i$ is also a unit in $\mathbb{Q}(i)$, we have $(1+i) = ((-i)(1+i)) = (1-i)$. Therefore $(2) = I^2$, where $I = (1-i)$.

Also, we have that

$$1 - i = (1+\xi_8)(1-\xi_8) = N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1+\xi_8) = N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1-\xi_8).$$

Then we can conclude that 2 is totally ramified in $\mathbb{Q}(\xi_8)$ and $2\mathbb{Z}[\xi_8] = (2) = \mathfrak{I}^4$, where $\mathfrak{I} = (1+\xi_8)$.

We have that $\mathfrak{I}$ is the ideal in $O_L = \mathbb{Z}[\xi_8]$ generated by $\mu = 1+\xi_8$. By the proposition 4, we have that the ideal $\mathfrak{I}^k$ is generated by μ^k, for all $k \geq 2$. Observe that, for $k = 0$, we have $\mathfrak{I}^0 = O_L = \mathbb{Z}[\xi_8]$.

The *inverse* of the ideal $\mathfrak{I}$ is an ideal of O_L defined as $\mathfrak{I}^{-1} = \{x \in \mathbb{Q}(\xi_8) \mid x\mathfrak{I} \subseteq O_L = \mathbb{Z}[\xi_8]\}$. $\mathfrak{I}^{-1}$ is an O_L-submodule, $\mathfrak{I}^{-1} = (\mu^{-1}) = \mu^{-1}O_L$, since $\mathfrak{I} = (\mu) = \mu O_L$, and $O_L = \mathfrak{I}\mathfrak{I}^{-1}$.

Analogously to the proposition 4, we can prove that $\mathfrak{I}^{-k} = (\mathfrak{I}^{-1})^k = (\mu^{-k}) = ((\mu^{-1})^k) = (\mu^{-1})^k O_L$. So $\mathfrak{I}^k$, $k \in \mathbb{Z}$, is an ideal of O_L generated by μ^k.

Now we will approximate the matrix H with the canonical embedding of the generator μ^k of $\Im^k$, $k \in \mathbb{Z}$, and we are going to make use of the following proposition:

Proposition 12. *We have that $\{u_k, u_k\xi_8\}$ is a $\mathbb{Z}[i]$-basis of $u_k\mathbb{Z}[\xi_8] = u_kO_L$, where $\{1, \xi_8\}$ is a $\mathbb{Z}[i]$-basis of O_L and $u_k = \mu^k$ is the generator of the ideal $\Im^k$, with $k \in \mathbb{Z}$.*

Proof. Let $u_k = \mu^k$ be the generator of the ideal $\Im^k$, where $k \in \mathbb{Z}$ and $\mu = 1 + \xi_8$. Let $x \in u_kO_L$, then $x = u_k\alpha$, with $\alpha \in O_L$. So

$$x = u_k(a + b\xi_8), \text{ where } a, b \in \mathbb{Z}[i], \text{ if, and only if,}$$

$$x = u_ka + u_kb\xi_8 = au_k + b(u_k\xi_8), \text{ with } a, b \in \mathbb{Z}[i],$$

therefore $\{u_k, u_k\xi_8\}$ generates u_kO_L. We will prove now that $\{u_k, u_k\xi_8\}$ is linearly independent. In fact, let $a, b \in \mathbb{Z}[i]$, then

$$au_k + bu_k\xi_8 = 0 \Leftrightarrow au_ku_k^{-1} + bu_ku_k^{-1}\xi_8 = 0 \Leftrightarrow a + b\xi_8 = 0 \Leftrightarrow a = b = 0.$$

So $\{u_k, u_k\xi_8\}$ is a $\mathbb{Z}[i]$-basis of u_kO_L. □

Then, by the proposition 12, we have that the generator matrix of the complex algebraic lattice $\sigma(u_kO_L)$ is given by (note that the transposed matrix has the same properties)

$$M_k = \begin{pmatrix} u_k & u_k\xi_8 \\ \sigma(u_k) & \sigma(u_k)\sigma(\xi_8) \end{pmatrix} = \begin{pmatrix} u_k & 0 \\ 0 & \sigma(u_k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix}, \tag{26}$$

so the matrix H can be approximated by

$$M_k' = \begin{pmatrix} u_k & 0 \\ 0 & \sigma(u_k) \end{pmatrix}. \tag{27}$$

What is really interesting is that the following section will show us that the canonical embeddings of $\Im = \mu O_L$ ($k = 1$), $\Im^2 = \mu^2 O_L$ ($k = 2$), $\Im^3 = \mu^3 O_L$ ($k = 3$) and $\Im^4 = \mu^4 O_L$ ($k = 4$) are simply the lattices D_4, $R\mathbb{Z}^4$, RD_4 and $2\mathbb{Z}^4$, respectively, where R is the rotation transformation.

4.3.1.1 Interference alignment onto a lattice for $k \geq 0$

We will see, in this section, that the quantization of the channel coefficients will give us the lattices D_4, $R\mathbb{Z}^4$, RD_4 and $2\mathbb{Z}^4$, when $k = 1, 2, 3$ and 4, respectively. So we will have a lattice

partition chain and such lattices are related to $k = 1, 2, 3$ and 4. We will also obtain the extension by periodicity of this lattice partition chain.

In fact, for $k = 1$, let

$$\begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_\mu.$$

It is easy to see that M_μ is given by

$$\begin{pmatrix} 1 & i \\ 1 & 1 \end{pmatrix},$$

where M_μ is a generator matrix of the lattice D_4 seen as a $\mathbb{Z}[i]$-lattice; in fact, the matrix M_μ with real entries is given by

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

and we can note that in each column of M_μ the sum of the coefficients is even, therefore the lattice Λ_1 generated by M_μ is a sublattice of D_4. Moreover, we have that $Vol(\Lambda_1) = 2 = Det(M_\mu) = Vol(D_4)$, then the index $|D_4/\Lambda_1|$ is equal to 1 and so $\Lambda_1 = D_4$.

With these properties, we have that M_μ is a generator matrix of D_4 seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_1 = \mu$ generates the ideal μO_L, then the matrix M_μ is a generator matrix of the lattice D_4 in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = 1$. We have that $\mathbb{Z}[i]^2$ has position 0 (note that M_0^T is a generator matrix for the lattice $\mathbb{Z}[i]^2$).

Now, for $k = 2$, let

$$\begin{pmatrix} \mu^2 & 0 \\ 0 & \sigma(\mu)^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^2}.$$

Using the fact that

$$\begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_\mu \text{ and}$$

$$\begin{pmatrix} \mu^2 & 0 \\ 0 & \sigma(\mu)^2 \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix},$$

we have

$$\begin{pmatrix} \mu^2 & 0 \\ 0 & \sigma(\mu)^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_\mu)^2.$$

Observe that

$$(M_\mu)^2 = \begin{pmatrix} 1 & i \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & i \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1+i & 2i \\ 2 & 1+i \end{pmatrix}.$$

The matrix $(M_\mu)^2$ with real entries is given by

$$(M_\mu)^2 = \begin{pmatrix} 1 & -1 & 0 & -2 \\ 1 & 1 & 2 & 0 \\ 2 & 0 & 1 & -1 \\ 0 & 2 & 1 & 1 \end{pmatrix}.$$

Note that in each column of $(M_\mu)^2$ the sum of the coefficients is even. By straightforward computation, it follows that $(M_\mu)^2 = R \cdot M$, where R is the rotation transformation given by

$$R = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \text{ and } M = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & -1 & -1 & -1 \\ 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & -1 \end{pmatrix}.$$

The 4×4 identity matrix $I_{4\times 4}$ is a generator matrix of the lattice $\mathbb{Z}^4$ and we can write $M = M \cdot I_{4\times 4}$; as the determinant of M is equal to 1 and M has integer entries (M is unimodular), then M and $I_{4\times 4}$ generate the same lattice, that is, M also generates the lattice $\mathbb{Z}^4$.

So we have that $(M_\mu)^2 = R \cdot M$ is a generator matrix of the lattice $R\mathbb{Z}^4 \simeq (1+i)\mathbb{Z}[i]^2$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_2 = \mu^2$ generates the ideal $\mu^2 O_L$, then the matrix $M_{\mu^2} = (M_\mu)^2$ is a generator matrix of the lattice $(1+i)\mathbb{Z}[i]^2$ in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = 2$.

For $k = 3$, let

$$\begin{pmatrix} \mu^3 & 0 \\ 0 & \sigma(\mu)^3 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^3}.$$

Using the fact that

$$\begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_\mu \text{ and}$$

$$\begin{pmatrix} \mu^3 & 0 \\ 0 & \sigma(\mu)^3 \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix},$$

we have

$$\begin{pmatrix} \mu^3 & 0 \\ 0 & \sigma(\mu)^3 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_\mu)^3.$$

Observe that

$$(M_\mu)^3 = \begin{pmatrix} 1+i & 2i \\ 2 & 1+i \end{pmatrix} \cdot \begin{pmatrix} 1 & i \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1+3i & -1+3i \\ 3+i & 1+3i \end{pmatrix}.$$

The matrix $(M_\mu)^3$ with real entries is given by

$$(M_\mu)^3 = \begin{pmatrix} 1 & -3 & -1 & -3 \\ 3 & 1 & 3 & -1 \\ 3 & -1 & 1 & -3 \\ 1 & 3 & 3 & 1 \end{pmatrix}.$$

Note that in each column of $(M_\mu)^3$ the sum of the coefficients is even. By straightforward computation, it follows that $(M_\mu)^3 = R \cdot N$, where R is the rotation transformation given by

$$R = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \text{ and } N = \begin{pmatrix} 2 & -1 & 1 & -2 \\ -1 & -2 & -2 & -1 \\ 2 & 1 & 2 & -1 \\ 1 & -2 & -1 & -2 \end{pmatrix}.$$

Note that in each column of N the sum of the coefficients is even, therefore the lattice Λ_2 generated by N is a sublattice of D_4. Moreover, we have that $Vol(\Lambda_2) = 2 = Det(N) = Vol(D_4)$, then the index $|D_4/\Lambda_2|$ is equal to 1 and so $\Lambda_2 = D_4$.

With these properties we have that $(M_\mu)^3 = R \cdot N$ is a generator matrix of $RD_4 \simeq (1+i)D_4$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_3 = \mu^3$ generates the ideal $\mu^3 O_L$, then the matrix $M_{\mu^3} = (M_\mu)^3$ is a generator matrix of the lattice $(1+i)D_4$ in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = 3$.

And for $k = 4$, let

$$\begin{pmatrix} \mu^4 & 0 \\ 0 & \sigma(\mu)^4 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^4}.$$

Using the fact that

$$\begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu} \text{ and}$$

$$\begin{pmatrix} \mu^4 & 0 \\ 0 & \sigma(\mu)^4 \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix},$$

we have

$$\begin{pmatrix} \mu^4 & 0 \\ 0 & \sigma(\mu)^4 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_{\mu})^4.$$

Observe that

$$(M_{\mu})^4 = \begin{pmatrix} 1+3i & -1+3i \\ 3+i & 1+3i \end{pmatrix} \cdot \begin{pmatrix} 1 & i \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 6i & -4+4i \\ 4+4i & 6i \end{pmatrix}.$$

The matrix $(M_{\mu})^4$ with real entries is given by

$$(M_{\mu})^4 = 2 \begin{pmatrix} 0 & -3 & -2 & -2 \\ 3 & 0 & 2 & -2 \\ 2 & -2 & 0 & -3 \\ 2 & 2 & 3 & 0 \end{pmatrix}.$$

Note that in each column of $(M_{\mu})^4$ the sum of the coefficients is even. Let

$$P = \begin{pmatrix} 0 & -3 & -2 & -2 \\ 3 & 0 & 2 & -2 \\ 2 & -2 & 0 & -3 \\ 2 & 2 & 3 & 0 \end{pmatrix}.$$

The 4×4 identity matrix $I_{4\times 4}$ is a generator matrix of the lattice $\mathbb{Z}^4$ and we can write $P = P \cdot I_{4\times 4}$; as the determinant of P is equal to 1 and P has integer entries (P is unimodular), then P and $I_{4\times 4}$ generate the same lattice, that is, P also generates the lattice $\mathbb{Z}^4$.

So we have that $(M_{\mu})^4 = 2 \cdot P$ is a generator matrix of the lattice $2\mathbb{Z}^4 \simeq 2\mathbb{Z}[i]^2$ seen as a

$\mathbb{Z}[i]$-lattice.

This means that, if $u_4 = \mu^4$ generates the ideal $\mu^4 O_L$, then the matrix $M_{\mu^4} = (M_\mu)^4$ is a generator matrix of the lattice $2\mathbb{Z}[i]^2$ in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = 4$.

Now the two following propositions will give us the extension by periodicity of the lattice partition chain in (20) for the positive positions, that is, $k \geq 0$:

Proposition 13. *For $k = 2\alpha$, $\alpha \in \mathbb{N}^*$, we have that $(M_\mu)^{k=2\alpha}$ is a generator matrix of the lattice $R^\alpha \mathbb{Z}^4 \simeq (1+i)^\alpha \mathbb{Z}[i]^2$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. By previously, for $k = 2$ and 4, we have the matrices M_{μ^2} and M_{μ^4} as being generator matrices of the lattices $R\mathbb{Z}^4 \simeq (1+i)\mathbb{Z}[i]^2$ and $2\mathbb{Z}^4 \simeq 2\mathbb{Z}[i]^2$, respectively (for $k = 0$ we know that M_0^T is a generator matrix for the lattice $\mathbb{Z}[i]^2$).

By straightforward computation we can see that the matrix $M_{\mu^2} = (M_\mu)^2$ is equivalent to the rotation matrix R (equivalent matrices generate the same lattice). Now, for $k \geq 1$, we can see by induction that

$$\begin{pmatrix} \mu^k & 0 \\ 0 & \sigma(\mu)^k \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_\mu)^k,$$

where $(M_\mu)^k = M_{\mu^k}$.

Let's suppose, by induction hypothesis, that $(M_\mu)^{2\alpha}$, $\alpha \in \mathbb{N}^*$, is a generator matrix of the lattice $R^\alpha \mathbb{Z}^4$.

We will show, for $k = 2\alpha + 2$, $\alpha \in \mathbb{N}^*$, that the lattice $R^{\alpha+1}\mathbb{Z}^4$ has a generator matrix as being the matrix $(M_\mu)^{2\alpha+2}$. In fact, we have

$$\begin{pmatrix} \mu^{2\alpha+2} & 0 \\ 0 & \sigma(\mu)^{2\alpha+2} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_\mu)^{2\alpha+2},$$

where $(M_\mu)^{2\alpha+2} = M_{\mu^{2\alpha+2}}$.

Then $(M_\mu)^{2\alpha+2} = ((M_\mu)^2)((M_\mu)^{2\alpha})$, using the induction hypothesis and the fact that R is equivalent to $(M_\mu)^2$, we have $(M_\mu)^{2\alpha+2}$ as a generator matrix of the lattice $R^{\alpha+1}\mathbb{Z}^4 \simeq (1+i)^{\alpha+1}\mathbb{Z}[i]^2$.

Therefore we showed that for $k = 2\alpha$, $\alpha \in \mathbb{N}^*$, if $u_{2\alpha} = \mu^{2\alpha}$ generates the ideal $\mu^{2\alpha} O_L$, then the matrix $(M_\mu)^{2\alpha}$ is a generator matrix of the lattice $R^\alpha \mathbb{Z}^4 \simeq (1+i)^\alpha \mathbb{Z}[i]^2$.

But if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}^*$, then $R^\alpha \mathbb{Z}^4 = 2^{\alpha/2}\mathbb{Z}^4 \simeq 2^{\alpha/2}\mathbb{Z}[i]^2$.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$, then $R^\alpha \mathbb{Z}^4 = 2^{(\alpha-1)/2} R\mathbb{Z}^4 \simeq 2^{(\alpha-1)/2}(1+i)\mathbb{Z}[i]^2$. □

Proposition 14. *For $k = 2\alpha + 1$, $\alpha \in \mathbb{N}^*$, we have that $(M_\mu)^{k=2\alpha+1}$ is a generator matrix of the lattice $R^{\frac{k-1}{2}} D_4 = R^\alpha D_4 \simeq (1+i)^\alpha D_4$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. By previously, for $k = 1$ and 3, we have the matrices M_μ and M_{μ^3} as being generator matrices of the lattices D_4 and $RD_4 \simeq (1+i)D_4$, respectively.

By straightforward computation we can see that the matrix $M_{\mu^2} = (M_\mu)^2$ is equivalent to the rotation matrix R (equivalent matrices generate the same lattice). Now, for $k \geq 1$, we can see by induction that

$$\begin{pmatrix} \mu^k & 0 \\ 0 & \sigma(\mu)^k \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_\mu)^k,$$

where $(M_\mu)^k = M_{\mu^k}$.

Let's suppose, by induction hypothesis, that $(M_\mu)^{k=2\alpha+1}$, $\alpha \in \mathbb{N}^*$, is a generator matrix of the lattice $R^{\frac{k-1}{2}} D_4 = R^\alpha D_4$.

We will show, for $k = 2\alpha + 3$, $\alpha \in \mathbb{N}^*$, that the lattice $R^{\alpha+1} D_4$ has a generator matrix as being the matrix $(M_\mu)^{2\alpha+3}$. In fact, we have

$$\begin{pmatrix} \mu^{2\alpha+3} & 0 \\ 0 & \sigma(\mu)^{2\alpha+3} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_\mu)^{2\alpha+3},$$

where $(M_\mu)^{2\alpha+3} = M_{\mu^{2\alpha+3}}$.

Then $(M_\mu)^{2\alpha+3} = ((M_\mu)^2)((M_\mu)^{2\alpha+1})$, using the induction hypothesis and the fact that R is equivalent to $(M_\mu)^2$, we have $(M_\mu)^{2\alpha+3}$ as a generator matrix of the lattice $R^{\alpha+1} D_4 \simeq (1+i)^{\alpha+1} D_4$.

Therefore we showed that for $k = 2\alpha + 1$, $\alpha \in \mathbb{N}^*$, if $u_{2\alpha+1} = \mu^{2\alpha+1}$ generates the ideal $\mu^{2\alpha+1} O_L$, then the matrix $(M_\mu)^{2\alpha+1}$ is a generator matrix of the lattice $R^\alpha D_4 \simeq (1+i)^\alpha D_4$.

But if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}^*$, then $R^\alpha D_4 = 2^{\alpha/2} D_4$.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$, then $R^\alpha D_4 = 2^{(\alpha-1)/2} RD_4 \simeq 2^{(\alpha-1)/2}(1+i)D_4$. □

Thus, in this section, we have the interference alignment onto a lattice for $k \geq 0$. Now, in the following section, we will show that the canonical embeddings of $\Im^{-1} = \mu^{-1} O_L$ ($k = -1$), $\Im^{-2} = \mu^{-2} O_L$ ($k = -2$), $\Im^{-3} = \mu^{-3} O_L$ ($k = -3$) and $\Im^{-4} = \mu^{-4} O_L$ ($k = -4$) are simply the lattices $R^{-1} D_4$, $R^{-1}\mathbb{Z}^4$, $\frac{1}{2} D_4$ and $\frac{1}{2}\mathbb{Z}^4$, respectively, where R is the rotation transformation and R^{-1} is its inverse.

4.3.1.2 Interference alignment onto a lattice for $k < 0$

We will see, in this section, that the quantization of the channel coefficients will give us the lattices $R^{-1}D_4$, $R^{-1}\mathbb{Z}^4$, $\frac{1}{2}D_4$ and $\frac{1}{2}\mathbb{Z}^4$, when $k = -1, -2, -3$ and -4, respectively. Thus, we will have a lattice partition chain and such lattices are related to $k = -1, -2, -3$ and -4. We will also obtain the extension by periodicity of this lattice partition chain.

In fact, for $k = -1$, let

$$\begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-1}}, \tag{28}$$

where $M_{\mu^{-1}}$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then, by (28), we have

$$\begin{pmatrix} \mu^{-1} & \mu^{-1}\xi_8 \\ \sigma(\mu)^{-1} & -\sigma(\mu)^{-1}\xi_8 \end{pmatrix} = \begin{pmatrix} a+\xi_8 c & b+\xi_8 d \\ a-\xi_8 c & b-\xi_8 d \end{pmatrix}.$$

By straightforward computation, we have

$$M_{\mu^{-1}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ -1-i & 1+i \end{pmatrix} = \frac{1}{2}\left(\frac{1}{1+i}\right)\begin{pmatrix} 2i & 2 \\ -2i & 2i \end{pmatrix} = \left(\frac{1}{1+i}\right)\begin{pmatrix} i & 1 \\ -i & i \end{pmatrix}.$$

Let M be the matrix such that $M_{\mu^{-1}} = \frac{1}{(1+i)}M$, that is,

$$M = \begin{pmatrix} i & 1 \\ -i & i \end{pmatrix}.$$

We have that M is a generator matrix of the lattice D_4 seen as a $\mathbb{Z}[i]$-lattice; in fact, the matrix M with real entries is given by

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

and we note that in each column of M the sum of the coefficients is even, therefore the lattice Λ_{-1} generated by M is a sublattice of D_4. Moreover, we have that $Vol(\Lambda_{-1}) = 2 = Det(M) =$

$Vol(D_4)$, then the index $|D_4/\Lambda_{-1}|$ is equal to 1 and so $\Lambda_{-1} = D_4$.

With these properties we have that M is a generator matrix of D_4 seen as a $\mathbb{Z}[i]$-lattice. So $M_{\mu^{-1}}$ is a generator matrix of the lattice $\frac{1}{(1+i)}D_4$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_{-1} = \mu^{-1}$ generates the ideal $\mu^{-1}O_L$, then the matrix $M_{\mu^{-1}}$ is a generator matrix of the lattice $\frac{1}{(1+i)}D_4$ in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = -1$ (left side). We have that $\mathbb{Z}[i]^2$ has position 0 (note that M_0^T is a generator matrix for $\mathbb{Z}[i]^2$).

Now, for $k = -2$, let

$$\begin{pmatrix} \mu^{-2} & 0 \\ 0 & \sigma(\mu)^{-2} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-2}}.$$

Using the fact that

$$\begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-1}} \text{ and}$$

$$\begin{pmatrix} \mu^{-2} & 0 \\ 0 & \sigma(\mu)^{-2} \end{pmatrix} = \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix},$$

we have

$$\begin{pmatrix} \mu^{-2} & 0 \\ 0 & \sigma(\mu)^{-2} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_{\mu^{-1}})^2.$$

Observe that

$$(M_{\mu^{-1}})^2 = M_{\mu^{-2}} = \frac{1}{(1+i)} \begin{pmatrix} -1 & 1+i \\ 1-i & -1 \end{pmatrix}.$$

So $(M_{\mu^{-1}})^2 = \frac{1}{(1+i)}M$, where M is given by

$$M = \begin{pmatrix} -1 & 1+i \\ 1-i & -1 \end{pmatrix}.$$

The matrix M with real entries is given by

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

The 4×4 identity matrix $I_{4\times 4}$ is a generator matrix of the lattice $\mathbb{Z}^4$ and we can write $M = M \cdot I_{4\times 4}$; as the determinant of M is equal to 1 and M has integer entries (M is unimodular), then M and $I_{4\times 4}$ generate the same lattice, that is, M also generates the lattice $\mathbb{Z}^4$.

So we have that $(M_{\mu^{-1}})^2 = \frac{1}{(1+i)}M$ is a generator matrix of the lattice $R^{-1}\mathbb{Z}^4 \simeq \frac{1}{(1+i)}\mathbb{Z}[i]^2$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_{-2} = \mu^{-2}$ generates the ideal $\mu^{-2}O_L$, then the matrix $M_{\mu^{-2}} = (M_{\mu^{-1}})^2$ is a generator matrix of the lattice $\frac{1}{(1+i)}\mathbb{Z}[i]^2$ in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = -2$.

For $k = -3$, let

$$\begin{pmatrix} \mu^{-3} & 0 \\ 0 & \sigma(\mu)^{-3} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-3}}.$$

Using the fact that

$$\begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-1}} \text{ and}$$

$$\begin{pmatrix} \mu^{-3} & 0 \\ 0 & \sigma(\mu)^{-3} \end{pmatrix} = \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix},$$

we have

$$\begin{pmatrix} \mu^{-3} & 0 \\ 0 & \sigma(\mu)^{-3} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_{\mu^{-1}})^3.$$

Observe that $(M_{\mu^{-1}})^3 = \frac{1}{2}M$, where M is given by

$$M = \begin{pmatrix} -2-i & 1+2i \\ 2-i & -2-i \end{pmatrix}.$$

The matrix M with real entries is given by

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

Note that in each column of M the sum of the coefficients is even, therefore the lattice Λ_{-3} generated by M is a sublattice of D_4. Moreover, we have that $Vol(\Lambda_{-3}) = 2 = Det(M) =$

$Vol(D_4)$, then the index $|D_4/\Lambda_{-3}|$ is equal to 1 and so $\Lambda_{-3} = D_4$.

With these properties we have that $(M_{\mu^{-1}})^3 = \frac{1}{2}M$ is a generator matrix of $\frac{1}{2}D_4$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_{-3} = \mu^{-3}$ generates the ideal $\mu^{-3}O_L$, then the matrix $M_{\mu^{-3}} = (M_{\mu^{-1}})^3$ is a generator matrix of the lattice $\frac{1}{2}D_4$ in (20), whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = -3$.

And, for $k = -4$, let

$$\begin{pmatrix} \mu^{-4} & 0 \\ 0 & \sigma(\mu)^{-4} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-4}}.$$

Using the fact that

$$\begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_{\mu^{-1}} \text{ and}$$

$$\begin{pmatrix} \mu^{-4} & 0 \\ 0 & \sigma(\mu)^{-4} \end{pmatrix} = \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} \cdots \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \sigma(\mu)^{-1} \end{pmatrix} (4\text{times}),$$

we have

$$\begin{pmatrix} \mu^{-4} & 0 \\ 0 & \sigma(\mu)^{-4} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_{\mu^{-1}})^4.$$

Observe that $(M_{\mu^{-1}})^4 = \frac{1}{2}M$, where M is given by

$$M = \begin{pmatrix} -3i & -2+2i \\ 2+2i & -3i \end{pmatrix}.$$

The matrix M with real entries is given by

$$M = \begin{pmatrix} 0 & 3 & -2 & -2 \\ -3 & 0 & 2 & -2 \\ 2 & -2 & 0 & 3 \\ 2 & 2 & -3 & 0 \end{pmatrix}.$$

The 4×4 identity matrix $I_{4\times 4}$ is a generator matrix of the lattice $\mathbb{Z}^4$ and we can write $M = M \cdot I_{4\times 4}$; as the determinant of M is equal to 1 and M has integer entries (M is unimodular), then M and $I_{4\times 4}$ generate the same lattice, that is, M also generates the lattice $\mathbb{Z}^4$.

So we have that $(M_{\mu^{-1}})^4 = \frac{1}{2}M$ is a generator matrix of the lattice $\frac{1}{2}\mathbb{Z}^4 \simeq \frac{1}{2}\mathbb{Z}[i]^2$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_{-4} = \mu^{-4}$ generates the ideal $\mu^{-4}O_L$, then the matrix $M_{\mu^{-4}} = (M_{\mu^{-1}})^4$ is a generator matrix of the lattice $\frac{1}{2}\mathbb{Z}[i]^2$ in 20, whose position compared to $\mathbb{Z}[i]^2$ is equal to $k = -4$.

Now the two following propositions will give us the extension by periodicity of the lattice partition chain in (20) for the negative positions, that is, $k \leq -1$:

Proposition 15. *For $k = -2\alpha$, $\alpha \in \mathbb{N}^*$, we have that $(M_{\mu^{-1}})^{k=2\alpha}$ is a generator matrix of the lattice $R^{-\alpha}\mathbb{Z}^4 \simeq \left(\frac{1}{(1+i)}\right)^{\alpha}\mathbb{Z}[i]^2$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. By previously, for $k = -2$ and -4, we have the matrices $M_{\mu^{-2}}$ and $M_{\mu^{-4}}$ as being generator matrices of the lattices $R^{-1}\mathbb{Z}^4 \simeq \frac{1}{(1+i)}\mathbb{Z}[i]^2$ and $\frac{1}{2}\mathbb{Z}^4 \simeq \frac{1}{2}\mathbb{Z}[i]^2$, respectively.

By straightforward computation we can see that the matrix $M_{\mu^{-2}} = (M_{\mu^{-1}})^2 = \frac{1}{2}M$, where

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

is equivalent (equivalent matrices generate the same lattice) to the matrix $R^{-1} = \frac{1}{2}R$ (inverse of the matrix R), where

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

Now, for $k \leq -1$, we can see by induction that

$$\begin{pmatrix} \mu^k & 0 \\ 0 & \sigma(\mu)^k \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_{\mu^{-1}})^{-k},$$

where $(M_{\mu^{-1}})^{-k} = M_{\mu^k}$.

Let's suppose, by induction hypothesis, that $(M_{\mu^{-1}})^{2\alpha}$, $\alpha \in \mathbb{N}^*$, is a generator matrix of the lattice $R^{-\alpha}\mathbb{Z}^4$.

We will show, for $k = -2\alpha - 2$, $\alpha \in \mathbb{N}^*$, that the lattice $R^{-\alpha-1}\mathbb{Z}^4$ has a generator matrix as

being the matrix $(M_{\mu^{-1}})^{2\alpha+2}$. In fact, we have

$$\begin{pmatrix} \mu^{-2\alpha-2} & 0 \\ 0 & \sigma(\mu)^{-2\alpha-2} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} = \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot (M_{\mu^{-1}})^{2\alpha+2},$$

where $(M_{\mu^{-1}})^{2\alpha+2} = M_{\mu^{-2\alpha-2}}$.

Then $(M_{\mu^{-1}})^{2\alpha+2} = ((M_{\mu^{-1}})^2)((M_{\mu^{-1}})^{2\alpha})$, using the induction hypothesis and the fact that R^{-1} is equivalent to $(M_{\mu^{-1}})^2$, we have $(M_{\mu^{-1}})^{2\alpha+2}$ as a generator matrix of the lattice $R^{-\alpha-1}\mathbb{Z}^4 \simeq \left(\frac{1}{(1+i)}\right)^{\alpha+1}\mathbb{Z}[i]^2$.

Therefore we showed that for $k = -2\alpha$, $\alpha \in \mathbb{N}^*$, if $u_{-2\alpha} = \mu^{-2\alpha}$ generates the ideal $\mu^{-2\alpha}O_L$, then the matrix $(M_{\mu^{-1}})^{2\alpha}$ is a generator matrix of the lattice $R^{-\alpha}\mathbb{Z}^4 \simeq \left(\frac{1}{(1+i)}\right)^{\alpha}\mathbb{Z}[i]^2$.

But if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}^*$, then $R^{-\alpha}\mathbb{Z}^4 = \left(\frac{1}{2}\right)^{\alpha/2}\mathbb{Z}^4 \simeq \left(\frac{1}{2}\right)^{\alpha/2}\mathbb{Z}[i]^2$.

Now, if α is odd, we have $\alpha = 2\beta+1$, where $\beta \in \mathbb{N}$, then $R^{-\alpha}\mathbb{Z}^4 = \left(\frac{1}{2}\right)^{(\alpha-1)/2}R^{-1}\mathbb{Z}^4 \simeq \left(\frac{1}{2}\right)^{(\alpha-1)/2}\left(\frac{1}{1+i}\right)\mathbb{Z}[i]^2$. □

Proposition 16. *For $k = -2\alpha+1$, $\alpha \in \mathbb{N}^*$, we have that $(M_{\mu^{-1}})^{-k=2\alpha-1}$ is a generator matrix of the lattice $R^{-\alpha=(k-1)/2}D_4 \simeq \left(\frac{1}{1+i}\right)^{\alpha}D_4$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. The proof is analogous to the previous proposition. So if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}^*$, then $R^{-\alpha}D_4 = \left(\frac{1}{2}\right)^{\alpha/2}D_4$.

Now, if α is odd, we have $\alpha = 2\beta+1$, where $\beta \in \mathbb{N}$, then $R^{-\alpha}D_4 = \left(\frac{1}{2}\right)^{(\alpha-1)/2}R^{-1}D_4 \simeq \left(\frac{1}{2}\right)^{(\alpha-1)/2}\left(\frac{1}{1+i}\right)D_4$. □

Thus, in this section, we have the interference alignment onto a lattice for $k < 0$. So we can conclude that, by using the binary cyclotomic field $\mathbb{Q}(\xi_8)$, we obtained the construction of an infinite nested lattice partition chain in dimension 4 (real) or 2 (complex). In the following section, we will present another example of channel quantization, this example is related to the dimension 8 (real) or 4 (complex):

4.3.2 An example in dimension 8 (real) or 4 (complex)

In this section, as we consider 4-dimensional complex valued vectors here, we will make use of the lattice partition chain defined as

$$(\phi\mathbb{Z}[i]^4)^* \supset (\Lambda')^* \supset \Lambda^* \supset D_8^* \supset \mathbb{Z}[i]^4 \supset D_8 \supset \Lambda \supset \Lambda' \supset \phi\mathbb{Z}[i]^4, \tag{29}$$

where the lattices Λ and Λ' are given by their construction A.

So each transmitter is using one of the lattices of this lattice partition chain (which is extended by periodicity so that it is a doubly infinite chain). Now we write, for a given user, how its codeword can be transformed so that we can perform the channel quantization. We will make use of the binary cyclotomic field $\mathbb{Q}(\xi_{16})$.

Then let's consider the following Galois extensions:

$$\begin{array}{c} L=\mathbb{Q}(\xi_{16}) \\ \Big| 4 \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{30}$$

As $[\mathbb{Q}(\xi_{16}):\mathbb{Q}]=\phi(16)=8$, where ϕ is the Euler function, and $[\mathbb{Q}(i):\mathbb{Q}]=2$, then we have $[\mathbb{Q}(\xi_{16}):\mathbb{Q}(i)]=4$. We have that the Galois groups of $[\mathbb{Q}(\xi_{16}):\mathbb{Q}(i)]$ and $[\mathbb{Q}(i):\mathbb{Q}]$ are given by

$$Gal(\mathbb{Q}(\xi_{16})/\mathbb{Q}(i))=\{\sigma_1=id:\mathbb{Q}(\xi_{16})\to\mathbb{Q}(\xi_{16});\ \sigma_2=\sigma:\mathbb{Q}(\xi_{16})\to\mathbb{Q}(\xi_{16}),\ \text{where}$$

$$\sigma_2(1)=1,\ \sigma_2(\xi_{16})=i\xi_{16},\ \sigma_2(\xi_{16}^2)=-\xi_{16}^2 \text{ and } \sigma_2(\xi_{16}^3)=-i\xi_{16}^3;$$

$$\sigma_3:\mathbb{Q}(\xi_{16})\to\mathbb{Q}(\xi_{16}),\ \text{where } \sigma_3(1)=1,\ \sigma_3(\xi_{16})=-\xi_{16},$$

$$\sigma_3(\xi_{16}^2)=\xi_{16}^2 \text{ and } \sigma_3(\xi_{16}^3)=-\xi_{16}^3;$$

$$\sigma_4:\mathbb{Q}(\xi_{16})\to\mathbb{Q}(\xi_{16}),\ \text{where } \sigma_4(1)=1,\ \sigma_4(\xi_{16})=-i\xi_{16},$$

$$\sigma_4(\xi_{16}^2)=-\xi_{16}^2 \text{ and } \sigma_4(\xi_{16}^3)=i\xi_{16}^3\} \text{ and}$$

$$Gal(\mathbb{Q}(i)/\mathbb{Q})=\{\sigma_1=id:\mathbb{Q}(i)\to\mathbb{Q}(i) \text{ and } \sigma_2:\mathbb{Q}(i)\to\mathbb{Q}(i),\ \text{where } \sigma_2(i)=-i\},$$

respectively, where *id* is the identity map.

By (OGGIER, 2005), we have $\mathbb{Q}(\xi_{16})=\mathbb{Q}(\xi_{16}+\xi_{16}^{-1})\mathbb{Q}(i)=\mathbb{Q}(\sqrt{2+\sqrt{2}})\mathbb{Q}(i)$. From proposition 2, it follows that $O_L=\mathbb{Z}[\xi_{16}]$, the ring of integers of L, is a free $\mathbb{Z}[i]$-module of rank 4 and $\{1,\xi_{16},\xi_{16}^2,\xi_{16}^3\}$ is a $\mathbb{Z}[i]$-basis.

Since $\{1,\xi_{16},\xi_{16}^2,\xi_{16}^3\}$ is a $\mathbb{Z}[i]$-basis of O_L, so the matrix

$$M_1=\begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) & \sigma_4(1) \\ \sigma_1(\xi_{16}) & \sigma_2(\xi_{16}) & \sigma_3(\xi_{16}) & \sigma_4(\xi_{16}) \\ \sigma_1(\xi_{16}^2) & \sigma_2(\xi_{16}^2) & \sigma_3(\xi_{16}^2) & \sigma_4(\xi_{16}^2) \\ \sigma_1(\xi_{16}^3) & \sigma_2(\xi_{16}^3) & \sigma_3(\xi_{16}^3) & \sigma_4(\xi_{16}^3) \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & 1 \\ \xi_{16} & i\xi_{16} & -\xi_{16} & -i\xi_{16} \\ \xi_{16}^2 & -\xi_{16}^2 & \xi_{16}^2 & -\xi_{16}^2 \\ \xi_{16}^3 & -i\xi_{16}^3 & -\xi_{16}^3 & i\xi_{16}^3 \end{pmatrix} \tag{31}$$

is the generator matrix of the complex algebraic lattice $\sigma(O_L)$.

Observe that M_0 and $M=M_0^T$ have the same properties. If we take $M_0'=\frac{1}{2}M_0$, we have

$(M_0')(M_0')^H$ equal to the identity matrix, where $(M_0')^H$ denotes the transpose conjugate of M_0'. So $M_0' = \frac{1}{2}M_0$ is a unitary matrix and using the same argument as before we have that $U = \frac{1}{2}M_0^T$ is also a unitary matrix.

Therefore, by proposition 5, $\sigma(O_L)$ is isomorphic to the $\mathbb{Z}[i]^4$-lattice.

At the receiver, we suppose that we apply U to the received vector of (71) to get

$$\bar{y}_m = Uy_m = \sum_{l=1}^{L} a_{ml}Ut_l + Uz_{eq,m}. \tag{32}$$

As $z_{eq,m}$ is i.i.d. circularly symmetric complex Gaussian noise and U is unitary, then the noise in (66) is also i.i.d. circularly symmetric complex Gaussian. Now let's take a look at the vectors of the form $a_{ml}Ut_l$. For sake of simplicity of notations, we denote it by

$$\bar{x} = h \cdot U \cdot x, \tag{33}$$

where $x = t_l$ is the lattice point transmitted by the considered user and $h = a_{ml}$ is the channel coefficient. We can rewrite it now as

$$\begin{pmatrix} h & 0 & 0 & 0 \\ 0 & h & 0 & 0 \\ 0 & 0 & h & 0 \\ 0 & 0 & 0 & h \end{pmatrix} \cdot U \cdot x = H \cdot U \cdot x. \tag{34}$$

The idea we want to develop is to quantize the diagonal matrix H by the diagonal matrix whose elements are components of the canonical embedding of the power (positive or negative) of an element of O_L with absolute algebraic norm equal to 2.

Observe that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = (1+i)(1-i) = 2$ and $(1+i)^2 = 2i$. As i is a unit in $\mathbb{Q}(i)$, taking as ideals, we have $2\mathbb{Z}[i] = (2) = (2i) = (1+i)^2$ in $\mathbb{Z}[i]$, so 2 is totally ramified in $\mathbb{Q}(i)$ ($2\mathbb{Z}[i] = (2) = (I')^2$, where $I' = (1+i)$).

As $-i$ is also a unit in $\mathbb{Q}(i)$, we have $(1+i) = ((-i)(1+i)) = (1-i)$. Therefore $(2) = I^2$, where $I = (1-i)$.

Observe that

$$1 - i = (1+\xi_{16})(1-\xi_{16})(1+i\xi_{16})(1-i\xi_{16}) =$$
$$= N_{\mathbb{Q}(\xi_{16})/\mathbb{Q}(i)}(1+\xi_{16}) = N_{\mathbb{Q}(\xi_{16})/\mathbb{Q}(i)}(1-\xi_{16}).$$

Therefore 2 is totally ramified in $\mathbb{Q}(\xi_{16})$ and $2\mathbb{Z}[\xi_{16}] = (2) = \mathfrak{I}^8$, where $\mathfrak{I} = (1+\xi_{16})$.

We have that $\mathfrak{I}$ is the ideal in $O_L = \mathbb{Z}[\xi_{16}]$ generated by $\mu = 1+\xi_{16}$. By the proposition 4, we have that the ideal $\mathfrak{I}^k$ is generated by μ^k, for all $k \geq 2$. Observe that, for $k = 0$, we have

$\Im^0 = O_L = \mathbb{Z}[\xi_{16}]$.

The *inverse* of the ideal $\Im$ is an ideal of O_L defined as $\Im^{-1} = \{x \in \mathbb{Q}(\xi_{16}) \mid x\Im \subseteq O_L = \mathbb{Z}[\xi_{16}]\}$. $\Im^{-1}$ is an O_L-submodule, $\Im^{-1} = (\mu^{-1}) = \mu^{-1}O_L$, since $\Im = (\mu) = \mu O_L$, and $O_L = \Im\Im^{-1}$.

Analogously to the proposition 4, we can prove that $\Im^{-k} = (\Im^{-1})^k = (\mu^{-k}) = ((\mu^{-1})^k) = (\mu^{-1})^k O_L$. So $\Im^k$, $k \in \mathbb{Z}$, is an ideal of O_L generated by μ^k.

Now we will approximate the matrix H with the canonical embedding of the generator μ^k of $\Im^k$, $k \in \mathbb{Z}$, and we are going to make use of the following proposition:

Proposition 17. *We have that $\{u_k, u_k\xi_{16}, u_k\xi_{16}^2, u_k\xi_{16}^3\}$ is a $\mathbb{Z}[i]$-basis of $u_k\mathbb{Z}[\xi_{16}] = u_k O_L$, where $\{1, \xi_{16}, \xi_{16}^2, \xi_{16}^3\}$ is a $\mathbb{Z}[i]$-basis of O_L and $u_k = \mu^k$ is the generator of the ideal $\Im^k$, with $k \in \mathbb{Z}$ and $\mu = 1 + \xi_{16}$.*

Proof. Let $u_k = \mu^k$ be the generator of the ideal $\Im^k$, where $k \in \mathbb{Z}$ and $\mu = 1 + \xi_{16}$. Let $x \in u_k O_L$, then $x = u_k\alpha$, with $\alpha \in O_L$. So

$$x = u_k(a + b\xi_{16} + c\xi_{16}^2 + d\xi_{16}^3), \text{ where } a,b,c,d \in \mathbb{Z}[i], \text{ if, and only if,}$$

$$x = u_k a + u_k b\xi_{16} + u_k c\xi_{16}^2 + u_k d\xi_{16}^3 = au_k + b(u_k\xi_{16}) + c(u_k\xi_{16}^2) + d(u_k\xi_{16}^3),$$

with $a,b,c,d \in \mathbb{Z}[i]$. Therefore $\{u_k, u_k\xi_{16}, u_k\xi_{16}^2, u_k\xi_{16}^3\}$ generates $u_k O_L$. We will prove now that $\{u_k, u_k\xi_{16}, u_k\xi_{16}^2, u_k\xi_{16}^3\}$ is linearly independent. In fact, let $a,b,c,d \in \mathbb{Z}[i]$, then

$$au_k + bu_k\xi_{16} + cu_k\xi_{16}^2 + du_k\xi_{16}^3 = 0 \Leftrightarrow$$

$$\Leftrightarrow au_k u_k^{-1} + bu_k u_k^{-1}\xi_{16} + cu_k u_k^{-1}\xi_{16}^2 + du_k u_k^{-1}\xi_{16}^3 = 0 \Leftrightarrow$$

$$\Leftrightarrow a + b\xi_{16} + c\xi_{16}^2 + d\xi_{16}^3 = 0 \Leftrightarrow a = b = c = d = 0,$$

so $\{u_k, u_k\xi_{16}, u_k\xi_{16}^2, u_k\xi_{16}^3\}$ is a $\mathbb{Z}[i]$-basis of $u_k O_L$. □

Then, by the proposition 17, we have that the generator matrix of the complex algebraic lattice $\sigma(u_k O_L)$ is given by (note that the transposed matrix has the same properties)

$$M_k = \begin{pmatrix} u_k & u_k\xi_{16} & u_k\xi_{16}^2 & u_k\xi_{16}^3 \\ \sigma(u_k) & \sigma(u_k)\sigma(\xi_{16}) & \sigma(u_k)\sigma(\xi_{16}^2) & \sigma(u_k)\sigma(\xi_{16}^3) \\ \sigma_3(u_k) & \sigma_3(u_k)\sigma_3(\xi_{16}) & \sigma_3(u_k)\sigma_3(\xi_{16}^2) & \sigma_3(u_k)\sigma_3(\xi_{16}^3) \\ \sigma_4(u_k) & \sigma_4(u_k)\sigma_4(\xi_{16}) & \sigma_4(u_k)\sigma_4(\xi_{16}^2) & \sigma_4(u_k)\sigma_4(\xi_{16}^3) \end{pmatrix} =$$

$$= \begin{pmatrix} u_k & 0 & 0 & 0 \\ 0 & \sigma(u_k) & 0 & 0 \\ 0 & 0 & \sigma_3(u_k) & 0 \\ 0 & 0 & 0 & \sigma_4(u_k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix}, \tag{35}$$

so the matrix H can be approximated by

$$M'_k = \begin{pmatrix} u_k & 0 & 0 & 0 \\ 0 & \sigma(u_k) & 0 & 0 \\ 0 & 0 & \sigma_3(u_k) & 0 \\ 0 & 0 & 0 & \sigma_4(u_k) \end{pmatrix}. \tag{36}$$

What is really interesting is that the following section will show us that the canonical embeddings of $\Im = \mu O_L$ ($k=1$), $\Im^2 = \mu^2 O_L$ ($k=2$), $\Im^3 = \mu^3 O_L$ ($k=3$) and $\Im^4 = \mu^4 O_L$ ($k=4$) are simply the lattices D_8, Λ, Λ' and $R\mathbb{Z}^8$, respectively, where R is the rotation transformation.

4.3.2.1 *Interference alignment onto a lattice for* $k \in \mathbb{Z}$

We will see, in this section, that the quantization of the channel coefficients will give us the lattices D_8, Λ, Λ' and $R\mathbb{Z}^8$, when $k = 1,2,3$ and 4, respectively. So we will have a lattice partition chain and such lattices are related to $k = 1,2,3$ and 4. We will also obtain, for k positive and k negative, the extension by periodicity of this lattice partition chain.

In fact, for $k = 1$, let

$$\begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_\mu,$$

by straightforward computation we have that M_μ is given by

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

where M_μ is a generator matrix of D_8 seen as a $\mathbb{Z}[i]$-lattice; in fact, the matrix M_μ with real entries is given by

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

and we note that in each column of M_μ the sum of the coefficients is even, therefore the lattice Λ_1 generated by M_μ is a sublattice of D_8. Moreover, we have that $Vol(\Lambda_1) = 2 = Det(M_\mu) = Vol(D_8)$, then the index $|D_8/\Lambda_1|$ is equal to 1 and so $\Lambda_1 = D_8$.

With these properties we have that M_μ is a generator matrix of D_8 seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_1 = \mu$ generates the ideal μO_L, then the matrix M_μ is a generator matrix of the lattice D_8 in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 1$. We have that $\mathbb{Z}[i]^4$ has position 0 (note that M_0^T is a generator matrix for the lattice $\mathbb{Z}[i]^4$).

Now, for $k = 2$, let

$$\begin{pmatrix} \mu^2 & 0 & 0 & 0 \\ 0 & \sigma(\mu^2) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^2) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^2) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_{\mu^2}.$$

Using the fact that

$$\begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_\mu \text{ and}$$

$$\begin{pmatrix} \mu^2 & 0 & 0 & 0 \\ 0 & \sigma(\mu^2) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^2) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^2) \end{pmatrix} =$$

$$= \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdot \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix},$$

we have

$$\begin{pmatrix} \mu^2 & 0 & 0 & 0 \\ 0 & \sigma(\mu^2) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^2) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^2) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot (M_\mu)^2.$$

Observe that

$$(M_\mu)^2 = \begin{pmatrix} 1 & 0 & i & 2i \\ 2 & 1 & 0 & i \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

The matrix $(M_\mu)^2$ with real entries is given by

$$(M_\mu)^2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & -2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 2 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \end{pmatrix}.$$

Note that in each column of $(M_\mu)^2$ the sum of the coefficients is even, therefore the lattice Λ generated by $(M_\mu)^2$ is a sublattice of D_8. Observe also that $v_1 = (1,0,2,0,1,0,0,0)$, $v_2 = (0,1,0,2,0,1,0,0)$, $v_3 = (0,0,1,0,2,0,1,0)$, $v_4 = (0,0,0,1,0,2,0,1)$, $v_5 = (0,1,0,0,1,0,2,0)$, $v_6 = (-1,0,0,0,0,1,0,2)$, $v_7 = (0,2,0,1,0,0,1,0)$ and $v_8 = (-2,0,-1,0,0,0,0,1)$ generate the lattice Λ.

Taking the vectors v_1, v_2, v_3, v_4, v_5, v_6, v_7 and v_8 modulo 2, we have the respective vectors: $c_1 = (1,0,0,0,1,0,0,0)$, $c_2 = (0,1,0,0,0,1,0,0)$, $c_3 = (0,0,1,0,0,0,1,0)$, $c_4 = (0,0,0,1,0,0,0,1)$, $c_5 = (0,1,0,0,1,0,0,0)$, $c_6 = (1,0,0,0,0,1,0,0)$, $c_7 = (0,0,0,1,0,0,1,0)$ and $c_8 = (0,0,1,0,0,0,0,1)$.

Placing the vectors c_1, c_2, c_3, c_4, c_5, c_6, c_7 and c_8 as the rows of a matrix (say M_Λ), we have

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

So this means that among the vectors c_i's, $i = 1,2,\ldots,8$, six of them are linearly independent. By straightforward computation we can see that c_1, c_2, c_3, c_4, c_5 and c_7 are such vectors.

Then the set $\{c_1,c_2,c_3,c_4,c_5,c_7\}$ is a basis for a linear binary block code C_Λ $(n = 8, k = 6)$

and M_{C_Λ} is a generator matrix of the code C_Λ, where M_{C_Λ} is given by

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

So by lemma 3 in (FORNEY, 1988), we have $\Lambda = 2\mathbb{Z}^8 + (8,6)$ is a binary lattice and $d^2_{min}(\Lambda) = min\{4, d_H(C_\Lambda)\}$, where $d_H(C_\Lambda)$ is the minimum Hamming distance of the code C_Λ. Let's calculate such a minimum Hamming distance: the matrix M_{C_Λ} by permutation of the columns and elementary row operations becomes

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

We have $M_{C_\Lambda} = [I : P]$ and $H_\Lambda = [P^T : I]$, where H_Λ is the parity check matrix. So

$$H^T_\Lambda = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector is necessary to make the sum of, at least, 2 lines of the matrix H^T_Λ, so the minimum Hamming distance is given by 2. However, $d^2_{min}(\Lambda) = min\{4, d_H(C_\Lambda)\} = min\{4,2\} = 2$.

Therefore if $u_2 = \mu^2$ generates the ideal $\mu^2 O_L$, then the matrix $M_{\mu^2} = (M_\mu)^2$ is a generator matrix of the lattice $\Lambda = 2\mathbb{Z}^8 + (8,6,2)$ in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 2$.

For $k = 3$, let

$$\begin{pmatrix} \mu^3 & 0 & 0 & 0 \\ 0 & \sigma(\mu^3) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^3) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^3) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_{\mu^3}.$$

Using the fact that

$$\begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_{\mu} \text{ and}$$

$$\begin{pmatrix} \mu^3 & 0 & 0 & 0 \\ 0 & \sigma(\mu^3) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^3) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^3) \end{pmatrix} =$$

$$= \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdots \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \text{ (3 times)},$$

we have

$$\begin{pmatrix} \mu^3 & 0 & 0 & 0 \\ 0 & \sigma(\mu^3) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^3) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^3) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot (M_\mu)^3.$$

Observe that

$$(M_\mu)^3 = \begin{pmatrix} 1 & i & 3i & 3i \\ 3 & 1 & i & 3i \\ 3 & 3 & 1 & i \\ 1 & 3 & 3 & 1 \end{pmatrix}.$$

The matrix $(M_\mu)^3$ with real entries is given by

$$(M_\mu)^3 = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & -3 & 0 & -3 \\ 0 & 1 & 1 & 0 & 3 & 0 & 3 & 0 \\ 3 & 0 & 1 & 0 & 0 & -1 & 0 & -3 \\ 0 & 3 & 0 & 1 & 1 & 0 & 3 & 0 \\ 3 & 0 & 3 & 0 & 1 & 0 & 0 & -1 \\ 0 & 3 & 0 & 3 & 0 & 1 & 1 & 0 \\ 1 & 0 & 3 & 0 & 3 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 0 & 3 & 0 & 1 \end{pmatrix}.$$

Note that in each column of $(M_\mu)^3$ the sum of the coefficients is even, therefore the lattice Λ' generated by $(M_\mu)^3$ is a sublattice of D_8. Observe also that $v_1 = (1,0,3,0,3,0,1,0)$, $v_2 = (0,1,0,3,0,3,0,1)$, $v_3 = (0,1,1,0,3,0,3,0)$, $v_4 = (-1,0,0,1,0,3,0,3)$, $v_5 = (0,3,0,1,1,0,3,0)$, $v_6 = (-3,0,-1,0,0,1,0,3)$, $v_7 = (0,3,0,3,0,1,1,0)$ and $v_8 = (-3,0,-3,0,-1,0,0,1)$ generate the lattice Λ'.

Taking the vectors v_1, v_2, v_3, v_4, v_5, v_6, v_7 and v_8 modulo 2, we have the respective vectors: $c_1 = (1,0,1,0,1,0,1,0)$, $c_2 = (0,1,0,1,0,1,0,1)$, $c_3 = (0,1,1,0,1,0,1,0)$, $c_4 = (1,0,0,1,0,1,0,1)$, $c_5 = (0,1,0,1,1,0,1,0)$, $c_6 = (1,0,1,0,0,1,0,1)$, $c_7 = (0,1,0,1,0,1,1,0)$ and $c_8 = (1,0,1,0,1,0,0,1)$.

Placing the vectors c_1, c_2, c_3, c_4, c_5, c_6, c_7 and c_8 as the rows of a matrix (say $M_{\Lambda'}$), we

have

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

So this means that among the vectors c_i's, $i = 1,2,\ldots,8$, five of them are linearly independent. By straightforward computation we can see that c_2, c_4, c_6, c_7 and c_8 are such vectors.

Then the set $\{c_2, c_4, c_6, c_7, c_8\}$ is a basis for a linear binary block code $C_{\Lambda'}$ $(n = 8, k = 5)$ and $M_{C_{\Lambda'}}$ is a generator matrix of the code $C_{\Lambda'}$, where $M_{C_{\Lambda'}}$ is given by

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

So by lemma 3 in (FORNEY, 1988), we have that $\Lambda' = 2\mathbb{Z}^8 + (8,5)$ is a binary lattice and $d^2_{min}(\Lambda') = min\{4, d_H(C_{\Lambda'})\}$, where $d_H(C_{\Lambda'})$ is the minimum Hamming distance of the code $C_{\Lambda'}$. Let's calculate such a minimum Hamming distance: the matrix $M_{C_{\Lambda'}}$ by permutation of the columns and elementary row operations becomes

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

We have $M_{C_{\Lambda'}} = [I : P]$ and $H_{\Lambda'} = [P^T : I]$, where $H_{\Lambda'}$ is the parity check matrix. So

$$H_{\Lambda'}^T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector is necessary to make the sum of, at least, 2 lines of the matrix $H_{\Lambda'}^T$, so the minimum Hamming distance is given by 2. However, $d_{min}^2(\Lambda') = min\{4, d_H(C_{\Lambda'})\} = min\{4,2\} = 2$.

Therefore if $u_3 = \mu^3$ generates the ideal $\mu^3 O_L$, then the matrix $M_{\mu^3} = (M_\mu)^3$ is a generator matrix of the lattice $\Lambda' = 2\mathbb{Z}^8 + (8,5,2)$ in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 3$.

And, for $k = 4$, let

$$\begin{pmatrix} \mu^4 & 0 & 0 & 0 \\ 0 & \sigma(\mu^4) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^4) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^4) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_{\mu^4}.$$

Using the fact that

$$\begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_\mu \text{ and}$$

$$\begin{pmatrix} \mu^4 & 0 & 0 & 0 \\ 0 & \sigma(\mu^4) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^4) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^4) \end{pmatrix} =$$

$$= \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \cdots \begin{pmatrix} \mu & 0 & 0 & 0 \\ 0 & \sigma(\mu) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu) \end{pmatrix} \text{ (4 times)},$$

we have

$$\begin{pmatrix} \mu^4 & 0 & 0 & 0 \\ 0 & \sigma(\mu^4) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^4) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^4) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot (M_\mu)^4.$$

Observe that

$$(M_\mu)^4 = \begin{pmatrix} 1+i & 4i & 6i & 4i \\ 4 & 1+i & 4i & 6i \\ 6 & 4 & 1+i & 4i \\ 4 & 6 & 4 & 1+i \end{pmatrix}.$$

The matrix $(M_\mu)^4$ with real entries is given by

$$(M_\mu)^4 = \begin{pmatrix} 1 & -1 & 0 & -4 & 0 & -6 & 0 & -4 \\ 1 & 1 & 4 & 0 & 6 & 0 & 4 & 0 \\ 4 & 0 & 1 & -1 & 0 & -4 & 0 & -6 \\ 0 & 4 & 1 & 1 & 4 & 0 & 6 & 0 \\ 6 & 0 & 4 & 0 & 1 & -1 & 0 & -4 \\ 0 & 6 & 0 & 4 & 1 & 1 & 4 & 0 \\ 4 & 0 & 6 & 0 & 4 & 0 & 1 & -1 \\ 0 & 4 & 0 & 6 & 0 & 4 & 1 & 1 \end{pmatrix}.$$

Note that in each column of $(M_\mu)^4$ the sum of the coefficients is even, therefore the lattice

generated by $(M_\mu)^4$ is a sublattice of D_8.

By straightforward computation, it follows that $(M_\mu)^4 = R \cdot U$, where R is the rotation transformation given by

$$R = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix} \text{ and}$$

$$U = \begin{pmatrix} 1 & 0 & 2 & -2 & 3 & -3 & 2 & -2 \\ 0 & -1 & -2 & -2 & -3 & -3 & -2 & -2 \\ 2 & 2 & 1 & 0 & 2 & -2 & 3 & -3 \\ 2 & -2 & 0 & -1 & -2 & -2 & -3 & -3 \\ 3 & 3 & 2 & 2 & 1 & 0 & 2 & -2 \\ 3 & -3 & 2 & -2 & 0 & -1 & -2 & -2 \\ 2 & 2 & 3 & 3 & 2 & 2 & 1 & 0 \\ 2 & -2 & 3 & -3 & 2 & -2 & 0 & -1 \end{pmatrix}.$$

As the determinant of U is equal to 1 and U has integer entries (U is unimodular), then $(M_\mu)^4$ and R generate the same lattice ($(M_\mu)^4$ and R are equivalent matrices).

Observe that $R = R \cdot I_{8\times 8}$, where $I_{8\times 8}$ is the 8×8 identity matrix. Therefore R is a generator matrix of the lattice $R\mathbb{Z}^8$, since $I_{8\times 8}$ is a generator matrix of the lattice $\mathbb{Z}^8$.

So we have that $(M_\mu)^4$ and R are generator matrices of the lattice $R\mathbb{Z}^8 \simeq (1+i)\mathbb{Z}[i]^4$ seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_4 = \mu^4$ generates the ideal $\mu^4 O_L$, then the matrix $M_{\mu^4} = (M_\mu)^4$ is a generator matrix of the lattice $(1+i)\mathbb{Z}[i]^4$ in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 4$.

Now the four following propositions give the extension by periodicity of the chain in (29) for the positive positions, that is, $k \geq 0$:

Proposition 18. *For $k = 4\alpha$, $\alpha \in \mathbb{N}^*$, we have that $M_{\mu^{4\alpha}} = (M_\mu)^{k=4\alpha}$ is a generator matrix of the lattice $R^\alpha\mathbb{Z}^8 \simeq (1+i)^\alpha\mathbb{Z}[i]^4$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. By previously, for $k = 4$, we have the matrix M_{μ^4} as being a generator matrix of the lattice $R\mathbb{Z}^8 \simeq (1+i)\mathbb{Z}[i]^4$ (for $k = 0$ we know that M_1^T is a generator matrix for the lattice $\mathbb{Z}[i]^4$).

For $k = 8 = 4 \cdot 2$, using the same argument as before, we have the matrix $M_{\mu^8} = (M_\mu)^8 = ((M_\mu)^4)^2$. As $(M_\mu)^4$ and R are equivalent matrices, we have that $M_{\mu^8} = ((M_\mu)^4)^2$ is a generator matrix of the lattice $2\mathbb{Z}^8 \simeq 2\mathbb{Z}[i]^4$.

Now, for $k \geq 1$, we can see by induction that

$$\begin{pmatrix} \mu^k & 0 & 0 & 0 \\ 0 & \sigma(\mu^k) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^k) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot (M_\mu)^k$$

where $(M_\mu)^k = M_{\mu^k}$.

Let's suppose, by induction hypothesis, that $(M_\mu)^{4\alpha}$, $\alpha \in \mathbb{N}^*$, is a generator matrix of the lattice $R^\alpha \mathbb{Z}^8$.

We will show, for $k = 4\alpha + 4$, $\alpha \in \mathbb{N}^*$, that the lattice $R^{\alpha+1}\mathbb{Z}^8$ has a generator matrix as being the matrix $(M_\mu)^{4\alpha+4}$. In fact, we have

$$\begin{pmatrix} \mu^{4\alpha+4} & 0 & 0 & 0 \\ 0 & \sigma(\mu^{4\alpha+4}) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^{4\alpha+4}) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^{4\alpha+4}) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot (M_\mu)^{4\alpha+4},$$

where $(M_\mu)^{4\alpha+4} = M_{\mu^{4\alpha+4}}$.

Then $(M_\mu)^{4\alpha+4} = ((M_\mu)^4)((M_\mu)^{4\alpha})$, using the induction hypothesis and the fact that R and $(M_\mu)^4$ are equivalent matrices, we have $(M_\mu)^{4\alpha+4}$ as a generator matrix of the lattice $R^{\alpha+1}\mathbb{Z}^8 \simeq (1+i)^{\alpha+1}\mathbb{Z}[i]^4$.

Therefore we showed that for $k = 4\alpha$, $\alpha \in \mathbb{N}^*$, the matrix $(M_\mu)^{4\alpha}$ is a generator matrix of the lattice $R^\alpha \mathbb{Z}^8 \simeq (1+i)^\alpha \mathbb{Z}[i]^4$.

But if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}^*$. Then $R^\alpha \mathbb{Z}^8 = 2^{\alpha/2}\mathbb{Z}^8 \simeq 2^{\alpha/2}\mathbb{Z}[i]^4$.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$. Then $R^\alpha \mathbb{Z}^8 = 2^{(\alpha-1)/2} R\mathbb{Z}^8 \simeq 2^{(\alpha-1)/2}(1+i)\mathbb{Z}[i]^4$. □

Proposition 19. *For $k = 4\alpha + 1$, $\alpha \in \mathbb{N}$, we have that $M_{\mu^{4\alpha+1}} = (M_\mu)^{k=4\alpha+1}$ is a generator matrix of the lattice $R^{\frac{(k-1)}{4}} D_8 = R^\alpha D_8 \simeq (1+i)^\alpha D_8$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. The proof is analogous to the proposition 18. So if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}$. Then $R^\alpha D_8 = 2^{(\alpha/2)} D_8$.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$. Then $R^\alpha D_8 = 2^{(\alpha-1)/2} R D_8 \simeq 2^{(\alpha-1)/2}(1+i)D_8$. □

Proposition 20. *For $k = 4\alpha + 2$, $\alpha \in \mathbb{N}$, we have that $M_{\mu^{4\alpha+2}} = (M_\mu)^{k=4\alpha+2}$ is a generator matrix of the lattice $R^{\frac{(k-2)}{4}} \Lambda = R^\alpha \Lambda \simeq (1+i)^\alpha \Lambda$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. The proof is analogous to the proposition 18. So if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}$. Then $R^\alpha \Lambda = 2^{(\alpha/2)} \Lambda$.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$. Then $R^\alpha \Lambda = 2^{(\alpha-1)/2} R\Lambda \simeq 2^{(\alpha-1)/2}(1+i)\Lambda$. □

Proposition 21. *For $k = 4\alpha + 3$, $\alpha \in \mathbb{N}$, we have that $M_{\mu^{4\alpha+3}} = (M_\mu)^{k=4\alpha+3}$ is a generator matrix of the lattice $R^{\frac{(k-3)}{4}} \Lambda' = R^\alpha \Lambda' \simeq (1+i)^\alpha \Lambda'$ seen as a $\mathbb{Z}[i]$-lattice.*

Proof. The proof is analogous to the proposition 18. So if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}$. Then $R^\alpha \Lambda' = 2^{(\alpha/2)} \Lambda'$.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$. Then $R^\alpha \Lambda' = 2^{(\alpha-1)/2} R\Lambda' \simeq 2^{(\alpha-1)/2}(1+i)\Lambda'$. □

Now the following proposition directly gives the extension by periodicity of the chain in (29) for the negative positions, that is, $k \leq -1$:

Proposition 22. *For all $k \in \mathbb{N}^*$, we have $\sigma(\Im^{-k}) = \sigma(\Im^k)^*$, where $\sigma(\Im^k)^*$ indicates the dual lattice of $\sigma(\Im^k)$.*

Proof. Let $\overrightarrow{x}$ and $\overrightarrow{y}$ be arbitrary elements of $\sigma(\Im^k)$ and $\sigma(\Im^{-k})$, respectively, where $k \in \mathbb{N}^*$. Therefore we have

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{L/\mathbb{Q}(i)}(x \cdot y),$$

where $x \in \Im^k$ and $y \in \Im^{-k}$, then $x = (1+\xi_{16})^k x_0$, with $x_0 \in O_L$, and $y = (1+\xi_{16})^{-k} y_0$, with $y_0 \in O_L$.

It is easy to see that

$$Tr_{L/\mathbb{Q}(i)}(x \cdot y) = \sum_{i=1}^{4} \sigma_i(x \cdot y) = \sum_{i=1}^{4} \sigma_i(x)\sigma_i(y) = \sum_{i=1}^{4} \sigma_i(x_0)\sigma_i(y_0) = Tr_{L/\mathbb{Q}(i)}(x_0 \cdot y_0).$$

By straightforward computation we have that $Tr_{L/\mathbb{Q}(i)}(x_0 \cdot y_0) \in \mathbb{Z}[i]$, so

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{L/\mathbb{Q}(i)}(x \cdot y) \in \mathbb{Z}[i].$$

Then $\sigma(\Im^{-k}) \subset \sigma(\Im^k)^*$, for all $k \in \mathbb{N}^*$. We also have that

$$Vol[\sigma(\Im^k)^*] = \frac{1}{Vol[\sigma(\Im^k)]} = Vol[\sigma(\Im^{-k})].$$

However the index $|\sigma(\Im^k)^*/\sigma(\Im^{-k})|$ is equal to 1 and so $\sigma(\Im^{-k}) = \sigma(\Im^k)^*$. □

Thus, by using the proposition 5.3.2, we have the following result, where we show that if $u_3 = \mu^3$ generates the ideal $\mu^3 O_L$, then the matrix $M_{\mu^3} = (M_\mu)^3$ is a generator matrix of the lattice $RD_8^* \simeq (1+i)D_8^*$ in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 3$:

Proposition 23. *If $u_3 = \mu^3$ generates the ideal $\mu^3 O_L$, then the matrix M_{μ^3} is a generator matrix of the lattice $RD_8^* \simeq (1+i)D_8^*$ in* (29)*, whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 3$.*

Proof. For using the proposition 5.3.2, we will observe the case $k = -3$. In fact, let

$$\begin{pmatrix} \mu^{-3} & 0 & 0 & 0 \\ 0 & \sigma(\mu^{-3}) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^{-3}) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^{-3}) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_{\mu^{-3}}.$$

Using the fact that

$$\begin{pmatrix} \mu^{-1} & 0 & 0 & 0 \\ 0 & \sigma(\mu)^{-1} & 0 & 0 \\ 0 & 0 & \sigma_3(\mu)^{-1} & 0 \\ 0 & 0 & 0 & \sigma_4(\mu)^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot M_{\mu^{-1}} \text{ and}$$

$$\begin{pmatrix} \mu^{-3} & 0 & 0 & 0 \\ 0 & \sigma(\mu^{-3}) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^{-3}) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^{-3}) \end{pmatrix} =$$

$$= \begin{pmatrix} \mu^{-1} & 0 & 0 & 0 \\ 0 & \sigma(\mu)^{-1} & 0 & 0 \\ 0 & 0 & \sigma_3(\mu)^{-1} & 0 \\ 0 & 0 & 0 & \sigma_4(\mu)^{-1} \end{pmatrix} \cdots \begin{pmatrix} \mu^{-1} & 0 & 0 & 0 \\ 0 & \sigma(\mu)^{-1} & 0 & 0 \\ 0 & 0 & \sigma_3(\mu)^{-1} & 0 \\ 0 & 0 & 0 & \sigma_4(\mu)^{-1} \end{pmatrix} \text{ (3 times),}$$

we have

$$\begin{pmatrix} \mu^{-3} & 0 & 0 & 0 \\ 0 & \sigma(\mu^{-3}) & 0 & 0 \\ 0 & 0 & \sigma_3(\mu^{-3}) & 0 \\ 0 & 0 & 0 & \sigma_4(\mu^{-3}) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_{16} & \xi_{16}^2 & \xi_{16}^3 \\ 1 & i\xi_{16} & -\xi_{16}^2 & -i\xi_{16}^3 \\ 1 & -\xi_{16} & \xi_{16}^2 & -\xi_{16}^3 \\ 1 & -i\xi_{16} & -\xi_{16}^2 & i\xi_{16}^3 \end{pmatrix} \cdot (M_{\mu^{-1}})^3.$$

Observe that $(M_{\mu^{-1}})^3 = \frac{1}{(1+i)}M$, where

$$M = \begin{pmatrix} 1-6i & -3+5i & 5-3i & -6+i \\ 1+6i & 1-6i & -3+5i & 5-3i \\ -3-5i & 1+6i & 1-6i & -3+5i \\ 5+3i & -3-5i & 1+6i & 1-6i \end{pmatrix}.$$

The matrix M with real entries is given by

$$M = \begin{pmatrix} 1 & 6 & -3 & -5 & 5 & 3 & -6 & -1 \\ -6 & 1 & 5 & -3 & -3 & 5 & 1 & -6 \\ 1 & -6 & 1 & 6 & -3 & -5 & 5 & 3 \\ 6 & 1 & -6 & 1 & 5 & -3 & -3 & 5 \\ -3 & 5 & 1 & -6 & 1 & 6 & -3 & -5 \\ -5 & -3 & 6 & 1 & -6 & 1 & 5 & -3 \\ 5 & -3 & -3 & 5 & 1 & -6 & 1 & 6 \\ 3 & 5 & -5 & -3 & 6 & 1 & -6 & 1 \end{pmatrix}.$$

Note that in each column of M the sum of the coefficients is even, therefore the lattice generated by M is a sublattice of D_8. Moreover, we have that $Vol(M) = 2 = Det(M) = Vol(D_8)$, then the index $|D_8/M|$ is equal to 1 and so $M = D_8$.

With these properties we have that M is a generator matrix of D_8 seen as a $\mathbb{Z}[i]$-lattice.

This means that, if $u_{-3} = \mu^{-3}$ generates the ideal $\mu^{-3}O_L$, then the matrix $M_{\mu^{-3}} = (M_{\mu^{-1}})^3$ is a generator matrix of the lattice $\frac{1}{(1+i)}D_8 \simeq R^{-1}D_8$ in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = -3$.

Then, by using the proposition 5.3.2, we have that if $u_3 = \mu^3$ generates the ideal $\mu^3 O_L$, then the matrix $M_{\mu^3} = (M_\mu)^3$ is a generator matrix of the lattice $RD_8^* \simeq (1+i)D_8^*$ in (29), whose position compared to $\mathbb{Z}[i]^4$ is equal to $k = 3$. □

Thus, in this section, we have the interference alignment onto a lattice for $k \in \mathbb{Z}$. We can also conclude that, by using the binary cyclotomic field $\mathbb{Q}(\xi_{16})$, we obtained the construction of an infinite nested lattice partition chain in dimension 8 (real) or 4 (complex).

5 CONSTRUCTION OF NESTED LATTICES FROM IDEALS FOR CHANNEL APPROXIMATION

5.1 Introduction

In chapter 4, we have explicited two examples of channel quantization, these examples were related to the dimensions 4 and 8 (real) or 2 and 4 (complex) and we made use of the binary cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{16})$, respectively.

As we discussed in chapter 4, we know that the *compute-and-forward* strategy enables relays to decode linear equations of the transmitted messages using the noisy linear combinations provided by the channel. Each relay, indexed by $m = 1,2,\ldots,M$, observes a noisy linear combination of the transmitted signals through the channel,

$$y_m = \sum_{l=1}^{L} h_{ml} x_l + z_m, \tag{37}$$

where $h_{ml} \in \mathbb{C}$ are complex-valued channel coefficients, $x_l \in \mathbb{C}^n$ such that $\|x_l\|^2 \leq nP$ (in (NAZER; GASTPAR, 2011), Appendix C, they argue that there exist fixed dithers that meet the power constraint) and z_m is i.i.d. circularly symmetric complex Gaussian noise, $z_m \sim \mathscr{CN}(\mathbf{0}, \mathbf{I}^{M\times M})$.

But, in (NAZER; GASTPAR, 2011), we also have an equivalent channel induced by the modulo-Λ transformation. In this "virtual" channel model each relay observes a $\mathbb{Z}[i]$-combination $\sum a_{ml} t_l$ of the lattice points corrupted by effective noise $z_{eq,m}$, that is,

$$y_m = \sum_{l=1}^{L} a_{ml} t_l + z_{eq,m}. \tag{38}$$

In this chapter, also in order to realize interference alignment onto a lattice, we need to quantize the channel coefficients a_{ml}. We are going to describe a way to find a lattice partition chain, for any dimension $n = 2^{(r-2)}$, with $r \geq 3$, in order to quantize the channel coefficients. For that, we will make use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, with $r \geq 3$, $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{(r-1)}$, where ϕ is the Euler function, and $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$.

For the generalization of the lattice partition chain in order to quantize the channel coefficients, we also have that the coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself. Specifically, relay m only needs to know h_m. Each transmitter only needs to know the desired message rate, not the realization of the channel.

5.2 Quantization of the Channel Gains

As described in chapter 4, suppose that our interference channel is complex-valued, specifically $a_{ml} \in \{\mathbb{Z}+i\mathbb{Z}\}$. We suppose that all lattices used by the legitimate user and the interferers are one of a certain lattice partition chain and extended by periodicity. Now the idea we want to develop is that the effect of a channel gain on a given user is to shift the lattice used by the user either to the left, if its channel gain is smaller than 1, or to the right, if it is larger than 1. It is very important that the channel gain does not remove the lattice from the initial chain of nested lattices.

In this section we will consider n-dimensional complex valued vectors, where $n = 2^{r-2}$ and $r \geq 3$. Now we write, for a given user, how its codeword can be transformed so that we can perform the channel quantization. We will make use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, where $r \geq 3$.

We will consider the following Galois extensions, where $r \geq 3$:

$$\begin{array}{c} L = \mathbb{Q}(\xi_{2^r}) \\ \Big| \, 2^{(r-2)} \\ \mathbb{Q}(i) \\ \Big| \, 2 \\ \mathbb{Q} \end{array} \tag{39}$$

As $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{(r-1)}$, where ϕ is the Euler function, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, then we have $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$. We have that the Galois groups of $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)]$ and $[\mathbb{Q}(i) : \mathbb{Q}]$ are given by

$$Gal(\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)) = \{\sigma_1 = id : \mathbb{Q}(\xi_{2^r}) \to \mathbb{Q}(\xi_{2^r}), \sigma_2, \sigma_3, \ldots, \sigma_{2^{(r-2)}}\} \text{ and}$$

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma_1 = id : \mathbb{Q}(i) \to \mathbb{Q}(i) \text{ and } \sigma_2 : \mathbb{Q}(i) \to \mathbb{Q}(i), \text{ where } \sigma_2(i) = -i\}.$$

By (OGGIER, 2005), we have $\mathbb{Q}(\xi_{2^r}) = \mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})\mathbb{Q}(i)$. From proposition 2, it follows that $O_L = \mathbb{Z}[\xi_{2^r}]$, the ring of integers of L, is a free $\mathbb{Z}[i]$-module of rank $2^{(r-2)}$ and

$$\{1, \xi_{2^r}, \xi_{2^r}^2, \ldots, \xi_{2^r}^{(2^{(r-2)}-1)}\}$$

is a $\mathbb{Z}[i]$-basis.

Since $\{1, \xi_{2^r}, \xi_{2^r}^2, \ldots, \xi_{2^r}^{(2^{(r-2)}-1)}\}$ is a $\mathbb{Z}[i]$-basis of O_L, so the matrix

$$M_0 = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \ldots & \sigma_{2^{(r-2)}}(1) \\ \sigma_1(\xi_{2^r}) & \sigma_2(\xi_{2^r}) & \ldots & \sigma_{2^{(r-2)}}(\xi_{2^r}) \\ \sigma_1(\xi_{2^r}^2) & \sigma_2(\xi_{2^r}^2) & \ldots & \sigma_{2^{(r-2)}}(\xi_{2^r}^2) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\xi_{2^r}^{(2^{(r-2)}-1)}) & \sigma_2(\xi_{2^r}^{(2^{(r-2)}-1)}) & \ldots & \sigma_{2^{(r-2)}}(\xi_{2^r}^{(2^{(r-2)}-1)}) \end{pmatrix} \tag{40}$$

is the generator matrix of the complex algebraic lattice $\sigma(O_L)$.

Observe that M_0 and $M = M_0^T$ have the same properties. If we take $M_0' = \frac{1}{2^{((r-2)/2)}} M_0$, we have $(M_0')(M_0')^H$ equal to the identity matrix, where $(M_0')^H$ denotes the transpose conjugate of M_0'. So $M_0' = \frac{1}{2^{((r-2)/2)}} M_0$ is a unitary matrix and using basic properties it is easy to see that $U = \frac{1}{2^{((r-2)/2)}} M_0^T$ is also a unitary matrix.

Therefore, by the proposition 5, $\sigma(O_L)$ is isomorphic to the $\mathbb{Z}[i]^{2^{(r-2)}}$-lattice.

At the receiver, we suppose that we apply U to the received vector of (71) to get

$$\bar{y}_m = U y_m = \sum_{l=1}^{L} a_{ml} U t_l + U z_{eq,m}. \tag{41}$$

As $z_{eq,m}$ is i.i.d. circularly symmetric complex Gaussian noise and U is unitary, then the noise in (66) is also i.i.d. circularly symmetric complex Gaussian. Now let's take a look at the vectors of the form $a_{ml} U t_l$. For sake of simplicity of notations, we denote it by

$$\bar{x} = h \cdot U \cdot x, \tag{42}$$

where $x = t_l$ is the lattice point transmitted by the considered user and $h = a_{ml}$ is the channel coefficient. We can rewrite it now as

$$\begin{pmatrix} h & 0 & \cdots & 0 \\ 0 & h & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h \end{pmatrix} \cdot U \cdot x = H \cdot U \cdot x. \tag{43}$$

The idea we want to develop is to quantize the diagonal matrix H by the diagonal matrix whose elements are components of the canonical embedding of the power (positive or negative) of an element of O_L with absolute algebraic norm equal to 2.

Observe that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = (1+i)(1-i) = 2$ and $(1+i)^2 = 2i$. As i is a unit in $\mathbb{Q}(i)$, taking as ideals, we have $2\mathbb{Z}[i] = (2) = (2i) = (1+i)^2$ in $\mathbb{Z}[i]$, so 2 is totally ramified in $\mathbb{Q}(i)$ ($2\mathbb{Z}[i] = (2) = (I')^2$, where $I' = (1+i)$).

As $-i$ is also a unit in $\mathbb{Q}(i)$, we have $(1+i) = ((-i)(1+i)) = (1-i)$. Therefore $(2) = I^2$, where $I = (1-i)$.

By previously we have

$$N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1+\xi_8) = N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1-\xi_8) =$$

$$= N_{\mathbb{Q}(\xi_{16})/\mathbb{Q}(i)}(1+\xi_{16}) = N_{\mathbb{Q}(\xi_{16})/\mathbb{Q}(i)}(1-\xi_{16}) = 1-i.$$

Now we can show, by induction over r, that $N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1+\xi_{2^r}) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^r}) = 1-i$. In fact, consider the following Galois extensions:

$$\begin{array}{c} \mathbb{Q}(\xi_{2^{r+1}}) \\ \Big| 2 \\ \mathbb{Q}(\xi_{2^r}) \\ \Big| 2^{(r-2)} \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{44}$$

Note that it is easy to verify that $\xi_{2^{r+1}}^2 = \xi_{2^r}$, for all $r \geq 3$. Suppose by induction that $N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1+\xi_{2^r}) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^r}) = 1-i$ and let's prove it for $r+1$. So

$$N_{\mathbb{Q}(\xi_{2^{r+1}})/\mathbb{Q}(i)}(1+\xi_{2^{r+1}}) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(N_{\mathbb{Q}(\xi_{2^{r+1}})/\mathbb{Q}(\xi_{2^r})}(1+\xi_{2^{r+1}})) =$$

$$= N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1+\xi_{2^{r+1}})(1-\xi_{2^{r+1}})) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^{r+1}}^2) =$$

$$= N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^r}) = 1-i \text{ and}$$

$$N_{\mathbb{Q}(\xi_{2^{r+1}})/\mathbb{Q}(i)}(1-\xi_{2^{r+1}}) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(N_{\mathbb{Q}(\xi_{2^{r+1}})/\mathbb{Q}(\xi_{2^r})}(1-\xi_{2^{r+1}})) =$$

$$= N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}((1-\xi_{2^{r+1}})(1+\xi_{2^{r+1}})) =$$

$$= N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^{r+1}}^2) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^r}) = 1-i.$$

Therefore 2 is totally ramified in $\mathbb{Q}(\xi_{2^r})$ and $2\mathbb{Z}[\xi_{2^r}] = (2) = \mathfrak{I}^{2^{(r-1)}}$, where $\mathfrak{I} = (1+\xi_{2^r})$.

We have that $\Im$ is the ideal in $O_L = \mathbb{Z}[\xi_{2^r}]$ generated by $\mu = 1 + \xi_{2^r}$. By the proposition 4, we have that the ideal $\Im^k$ is generated by μ^k, for all $k \geq 2$. Observe that, for $k = 0$, we have $\Im^0 = O_L = \mathbb{Z}[\xi_{2^r}]$.

The *inverse* of the ideal $\Im$ is an ideal of O_L defined as $\Im^{-1} = \{x \in \mathbb{Q}(\xi_{2^r}) \mid x\Im \subseteq O_L = \mathbb{Z}[\xi_{2^r}]\}$. $\Im^{-1}$ is an O_L-submodule, $\Im^{-1} = (\mu^{-1}) = \mu^{-1}O_L$, since $\Im = (\mu) = \mu O_L$, and $O_L = \Im\Im^{-1}$.

Analogously to the proposition 4, we can prove that $\Im^{-k} = (\Im^{-1})^k = (\mu^{-k}) = ((\mu^{-1})^k) = (\mu^{-1})^k O_L$. So $\Im^k$, $k \in \mathbb{Z}$, is an ideal of O_L generated by μ^k.

Now we will approximate the matrix H with the canonical embedding of the generator μ^k of $\Im^k$, where $k \in \mathbb{Z}$, and we are going to make use of the following proposition:

Proposition 24. *We have that $\{u_k, u_k\xi, u_k\xi^2, \ldots, u_k\xi^{(n-1)}\}$ is a $\mathbb{Z}[i]$-basis of $u_k\mathbb{Z}[\xi] = u_k O_L$, where $n = 2^{(r-2)}$, $\{1, \xi, \xi^2, \ldots, \xi^{(n-1)}\}$ is a $\mathbb{Z}[i]$-basis of O_L and $u_k = \mu^k$ is the generator of the ideal $\Im^k$, with $k \in \mathbb{Z}$ and $\mu = 1 + \xi_{2^r}$.*

Proof. Let $\xi_{2^r} = \xi$ and $u_k = \mu^k$ be the generator of the ideal $\Im^k$, where $k \in \mathbb{Z}$ and $\mu = 1 + \xi$. Let $x \in u_k O_L$, then $x = u_k\alpha$, with $\alpha \in O_L$. So

$$x = u_k(a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{n-1}\xi^{n-1}), \text{ where}$$

$$a_i \in \mathbb{Z}[i],\ i = 0, 1, \ldots, n-1, \text{ if, and only if,}$$

$$x = a_0u_k + a_1u_k\xi + a_2u_k\xi^2 + \ldots + a_{n-1}u_k\xi^{n-1}, \text{ with } a_i \in \mathbb{Z}[i],\ i = 0, 1, \ldots, n-1.$$

Therefore $\{u_k, u_k\xi, \ldots, u_k\xi^{n-1}\}$ generates $u_k O_L$. We will prove now that

$$\{u_k, u_k\xi, \ldots, u_k\xi^{n-1}\}$$

is linearly independent. In fact, let $a_i \in \mathbb{Z}[i]$, with $i = 0, 1, \ldots, n-1$, then

$$a_0u_k + a_1u_k\xi + \ldots + a_{n-1}u_k\xi^{n-1} = 0 \Leftrightarrow$$

$$\Leftrightarrow a_0u_ku_k^{-1} + a_1u_ku_k^{-1}\xi + \ldots + a_{n-1}u_ku_k^{-1}\xi^{n-1} = 0 \Leftrightarrow$$

$$\Leftrightarrow a_0 + a_1\xi + \ldots + a_{n-1}\xi^{n-1} = 0 \Leftrightarrow a_i = 0,\ \forall\, i = 0, 1, \ldots, n-1,$$

so $\{u_k, u_k\xi, \ldots, u_k\xi^{n-1}\}$ is a $\mathbb{Z}[i]$-basis of $u_k O_L$. □

Then, by the proposition 24, we have that the generator matrix of the complex algebraic lattice $\sigma(u_k O_L)$ is given by (note that the transposed matrix has the same properties)

$$M_k = \begin{pmatrix} u_k & u_k\xi & \cdots & u_k\xi^{n-1} \\ \sigma_2(u_k) & \sigma_2(u_k\xi) & \cdots & \sigma_2(u_k\xi^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(u_k) & \sigma_n(u_k\xi) & \cdots & \sigma_n(u_k\xi^{n-1}) \end{pmatrix} =$$

$$= \begin{pmatrix} u_k & 0 & \cdots & 0 \\ 0 & \sigma_2(u_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n(u_k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi & \cdots & \xi^{n-1} \\ 1 & \sigma_2(\xi) & \cdots & \sigma_2(\xi^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi) & \cdots & \sigma_n(\xi^{n-1}) \end{pmatrix}, \tag{45}$$

so the matrix H can be approximated by

$$M'_k = \begin{pmatrix} u_k & 0 & \cdots & 0 \\ 0 & \sigma_2(u_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n(u_k) \end{pmatrix}. \tag{46}$$

Observe that

$$M'_k M_0^T = \begin{pmatrix} u_k & 0 & \cdots & 0 \\ 0 & \sigma_2(u_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n(u_k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi & \cdots & \xi^{n-1} \\ 1 & \sigma_2(\xi) & \cdots & \sigma_2(\xi^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi) & \cdots & \sigma_n(\xi^{n-1}) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi & \cdots & \xi^{n-1} \\ 1 & \sigma_2(\xi) & \cdots & \sigma_2(\xi^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi) & \cdots & \sigma_n(\xi^{n-1}) \end{pmatrix} \cdot M_{\mu^k} = M_0^T M_{\mu^k}, \tag{47}$$

where M_{μ^k} is an $n \times n$ matrix whose entries belong to the ring $\mathbb{Z}[i]$.

This means that if $u_k = \mu^k$ generates the ideal $\mu^k O_L$, then the matrix M_{μ^k} is a generator matrix of the lattice that is the canonical embedding of the ideal $\Im^k$, whose position compared to the $\mathbb{Z}[i]^n$-lattice is equal to k.

Since for $k = 1$ we have

$$\begin{pmatrix} \mu & 0 & \cdots & 0 \\ 0 & \sigma_2(\mu) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_n(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi & \cdots & \xi^{n-1} \\ 1 & \sigma_2(\xi) & \cdots & \sigma_2(\xi^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi) & \cdots & \sigma_n(\xi^{n-1}) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi & \cdots & \xi^{n-1} \\ 1 & \sigma_2(\xi) & \cdots & \sigma_2(\xi^{n-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_n(\xi) & \cdots & \sigma_n(\xi^{n-1}) \end{pmatrix} \cdot M_\mu = M_0^T M_\mu, \tag{48}$$

then we can see, by induction, that $M_1' M_0^T = M_0^T (M_\mu)^k$, for $k \geq 1$; that is, $M_{\mu^k} = (M_\mu)^k$, for $k \geq 1$.

In the following section, we will present a method of generalization of the lattice partition chain in order to quantize the channel coefficients for any dimension $n = 2^{r-2}$, with $r \geq 3$, and we will make use of the Pascal's triangle:

5.3 Method of Generalization by Using the Pascal's Triangle

We have seen in chapter 4 that the lattice partition chains related to $r = 3$ and $r = 4$ are given by

$$\cdots \supset \phi^{-1}\mathbb{Z}[i]^2 \supset \phi^{-1} D_4 \supset \mathbb{Z}[i]^2 \supset D_4 \supset \phi\mathbb{Z}[i]^2 \supset \phi D_4 \supset 2\mathbb{Z}[i]^2 \supset \cdots \tag{49}$$

and

$$\cdots \supset (\phi\mathbb{Z}[i]^4)^* \supset (\Lambda')^* \supset \Lambda^* \supset D_8^* \supset \mathbb{Z}[i]^4 \supset D_8 \supset \Lambda \supset \Lambda' \supset \phi\mathbb{Z}[i]^4 \supset \cdots, \tag{50}$$

respectively, where $*$ denotes the dual of a lattice.

Here we are going to describe a way to find the lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$. Consider the following Galois extensions:

$$\begin{array}{c} \mathbb{L} = \mathbb{Q}(\xi_{2^r}) \\ \Big| 2 \\ \mathbb{K} = \mathbb{Q}(\xi_{2^{r-1}}) \\ \Big| 2^{(r-3)} \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{51}$$

Let $\theta = \xi_{2^{r-1}}$, $\beta = \xi_{2^r}$, $\mu = 1+\theta$, $\mu' = 1+\beta$, $\Im = (1+\theta) = \mu O_{\mathbb{K}}$ and $\mathscr{J} = (1+\beta) = \mu' O_{\mathbb{L}}$, where $O_{\mathbb{K}} = \mathbb{Z}[\theta]$ and $O_{\mathbb{L}} = \mathbb{Z}[\beta]$.

We have $\beta^2 = \theta$, $\Im^k = (\mu^k) = \mu^k O_{\mathbb{K}}$, $\mathscr{J}^k = ((\mu')^k) = (\mu')^k O_{\mathbb{L}}$, where $k \in \mathbb{Z}$, and, due to the ideal ramification, $\mathscr{J}^2 = \Im$.

The following proposition will give us the lattices related to the canonical embeddings of the ideals $\mathscr{J}^k$, for k even:

Proposition 25. *Let σ and τ be the canonical embeddings of the ideals in $\mathbb{K}$ and $\mathbb{L}$, respectively. Let $\{id, \delta\}$ be the Galois group of the field extension $\mathbb{L}/\mathbb{K}$, where $\delta : \mathbb{L} \to \mathbb{L}$, with $\delta(\beta) = -\beta$, and $id : \mathbb{L} \to \mathbb{L}$ is the identity map. Let Λ_k be the lattice related to the canonical embedding of the ideal $\Im^k$, $k \geq 1$. Then $\tau(\mathscr{J}^{2k}) = \Lambda_k^2 = \Lambda \times \Lambda$.*

Proof. By hypothesis we have $\sigma(\Im^k) = \Lambda_k$, where $k \geq 1$. Then

$$\tau(\mathscr{J}^{2k}) = \tau((\mathscr{J}^2)^k) = \tau(\Im^k) = (\{id, \delta\} \circ \sigma)(\Im^k) = \{\sigma, (\delta \circ \sigma)\}(\Im^k),$$

where $\{id, \delta\} \circ \sigma$ denotes the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$. So

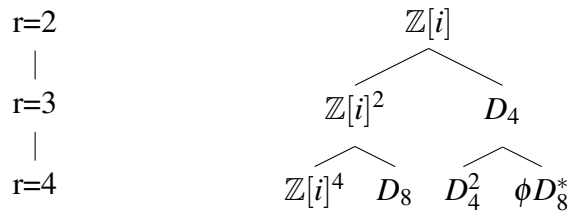
$$\{\sigma, (\delta \circ \sigma)\}(\Im^k) = \begin{pmatrix} \sigma(\Im^k) \\ \sigma(\Im^k) \end{pmatrix} = \begin{pmatrix} \Lambda_k \\ \Lambda_k \end{pmatrix} = \Lambda_k \times \Lambda_k = \Lambda_k^2,$$

since δ fixes the elements of $\mathbb{K}$. Therefore $\tau(\mathscr{J}^{2k}) = \Lambda_k^2$. □

So using the proposition 25, we can conclude that if $\sigma(\Im^k) = \phi(D_n^*)^\alpha$, where $\alpha \geq 1$ and $k \geq 1$, then $\tau(\mathscr{J}^{2k}) = \phi(D_n^*)^{2\alpha}$, and if $\sigma(\Im^k) = \phi\mathbb{Z}[i]^n$, where $n = 2^{r-3}$, then $\tau(\mathscr{J}^{2k}) = \phi\mathbb{Z}[i]^{2n}$.

We can observe by (49) and (50) that $\sigma(\Im^k) = \phi\mathbb{Z}[i]^n$, when $k = n$. However $\tau(\mathscr{J}^{2n}) = \phi\mathbb{Z}[i]^{2n}$. We also have, for any $r \geq 3$, that the lattice related to the canonical embedding of the ideal when $k = 0$ is isomorphic to the $\mathbb{Z}[i]^n$-lattice, where $n = 2^{r-2}$.

Therefore, for $r = 2, 3$ and 4, we can observe the lattice partition chains related to each r as the following trees:



Now, before generalizing the lattice partition chain for any $r \geq 3$, the following section shows us the construction of the lattice partition chain related to $r = 5$.

5.3.1 The construction of the lattice partition chain related to r=5

This section will give us the lattice partition chain related to $r = 5$ and we will obtain the construction A of the lattices of this chain.

Thus, for $r = 5$, we have the following Galois extensions:

$$\begin{array}{c} \mathbb{L} = \mathbb{Q}(\xi_{32}) \\ \Big| 2 \\ \mathbb{K} = \mathbb{Q}(\xi_{16}) \\ \Big| 4 \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{52}$$

Let $\theta = \xi_{16}$, $\beta = \xi_{32}$, $\mu = 1+\theta$, $\mu' = 1+\beta$, $\mathfrak{I} = (1+\theta) = \mu O_{\mathbb{K}}$ and $\mathscr{J} = (1+\beta) = \mu' O_{\mathbb{L}}$, where $O_{\mathbb{K}} = \mathbb{Z}[\theta]$ and $O_{\mathbb{L}} = \mathbb{Z}[\beta]$.

We have $\beta^2 = \theta$, $\mathfrak{I}^k = (\mu^k) = \mu^k O_{\mathbb{K}}$, $\mathscr{J}^k = ((\mu')^k) = (\mu')^k O_{\mathbb{L}}$, where $k \in \mathbb{Z}$, and, due to the ideal ramification, $\mathscr{J}^2 = \mathfrak{I}$.

Let σ and τ be the canonical embeddings of the ideals in $\mathbb{K}$ and $\mathbb{L}$, respectively. For $r = 4$ observe that $\sigma(\mathfrak{I}) = D_8$ and $\sigma(\mathfrak{I}^2) = D_4^2$. Therefore, by the proposition 25, we can conclude that $\tau(\mathscr{J}^2) = \tau(\mathfrak{I}) = D_8^2$.

Therefore, for $r = 5$ and $k = 2$, we have the lattice D_8^2, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 2$. We also know that $\tau(\mathscr{J}^8) = \phi\mathbb{Z}[i]^8$ and the lattice related to the canonical embedding of the ideal when $k = 0$ is isomorphic to the $\mathbb{Z}[i]^8$-lattice.

Now the following proposition will show us, for $k = 1$, that $\tau(\mathscr{J}) = D_{16}$:

Proposition 26. *We have, for $k = 1$, that $\tau(\mathscr{J}) = D_{16}$.*

Proof. We have $\mathbb{Z}[i]^8/\tau(\mathscr{J})/D_8^2$ and

$$\mathbb{Z}[i]^8 = D_8^2 \cup (D_8 \oplus (D_8 + (1,0,0,0))) \cup$$

$$\cup((D_8 + (1,0,0,0)) \oplus D_8) \cup ((D_8 + (1,0,0,0)) \oplus (D_8 + (1,0,0,0))) =$$

$$= D_8^2 \cup (D_8^2 + (0,1,0,0,0,0,0,0)) \cup$$

$$\cup(D_8^2 + (1,0,0,0,0,0,0,0)) \cup (D_8^2 + (1,1,0,0,0,0,0,0)).$$

So $\tau(\mathscr{J})$ is the union of D_8^2 with either $(D_8 \oplus (D_8 + (1,0,0,0)))$, or $((D_8 + (1,0,0,0)) \oplus D_8)$, or $((D_8 + (1,0,0,0)) \oplus (D_8 + (1,0,0,0)))$.

Observe that $\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta))$, then $\tau(\mathscr{J}) = \tau(\mathscr{J}^2) \cup \tau(\mathscr{J}^2 + (1+\beta)) = D_8^2 \cup \tau(\mathscr{J}^2 + (1+\beta))$ and we can conclude that $\tau(\mathscr{J}^2 + (1+\beta))$ is equal to either $(D_8 \oplus (D_8 + (1,0,0,0)))$, or $((D_8 + (1,0,0,0)) \oplus D_8)$, or $((D_8 + (1,0,0,0)) \oplus (D_8 + (1,0,0,0)))$.

We have $\tau(\mathscr{J}^2 + (1+\beta)) = \tau(\mathscr{J}^2) + \tau(1+\beta) = D_8^2 + \tau(1+\beta)$, where

$$\tau(1+\beta) = (1+\beta, \tau_2(1+\beta), \ldots, \tau_8(1+\beta)) = (1+\beta, 1+\tau_2(\beta), \ldots, 1+\tau_8(\beta)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

A $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ is given by

$$\{1, \beta, \beta^2, \beta^3, \ldots, \beta^7\} = \{1, \beta, \theta, \theta\beta, \theta^2, \theta^2\beta, \theta^3, \theta^3\beta\}. \tag{53}$$

So the matrix

$$M = \begin{pmatrix} 1 & \beta & \theta & \theta\beta & \theta^2 & \theta^2\beta & \theta^3 & \theta^3\beta \\ 1 & \tau_2(\beta) & \tau_2(\theta) & \tau_2(\theta\beta) & \tau_2(\theta^2) & \tau_2(\theta^2\beta) & \tau_2(\theta^3) & \tau_2(\theta^3\beta) \\ 1 & \tau_3(\beta) & \tau_3(\theta) & \tau_3(\theta\beta) & \tau_3(\theta^2) & \tau_3(\theta^2\beta) & \tau_3(\theta^3) & \tau_3(\theta^3\beta) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \tau_8(\beta) & \tau_8(\theta) & \tau_8(\theta\beta) & \tau_8(\theta^2) & \tau_8(\theta^2\beta) & \tau_8(\theta^3) & \tau_8(\theta^3\beta) \end{pmatrix} \tag{54}$$

generates the complex algebraic lattice $\tau(O_{\mathbb{L}})$.

However it follows that

$$\tau(1+\beta) = M \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\beta \\ 1+\tau_2(\beta) \\ 1+\tau_3(\beta) \\ 1+\tau_4(\beta) \\ 1+\tau_5(\beta) \\ 1+\tau_6(\beta) \\ 1+\tau_7(\beta) \\ 1+\tau_8(\beta) \end{pmatrix}.$$

Therefore we have that

$$\tau(\mathscr{J}^2 + (1+\beta)) = D_8^2 + (1,1,0,0,0,0,0,0) = (D_8 + (1,0,0,0)) \oplus (D_8 + (1,0,0,0))$$

and

$$\tau(\mathscr{J}) = D_8^2 \cup ((D_8 + (1,0,0,0)) \oplus (D_8 + (1,0,0,0))) = D_{16}.$$

So, for $r = 5$ and $k = 1$, we have the lattice D_{16}, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 1$. □

Now, in the following section, we will obtain the construction A of the lattices related to the canonical embedding of the ideals $\mathscr{J}^k$, $k = 0,1,2,3,\ldots,7$:

5.3.1.1 The construction A of the lattice partition chain related to r=5

In this section we are going to find the construction A of the lattices related to the canonical embedding of the ideals $\mathscr{J}^k$ and we will start the calculations from the last position to the first, that is, from $k = 7$ to $k = 0$. In fact: for $r = 4$ observe that $\sigma(\Im^3) = \phi D_8^*$ and we know, by the proposition 25, that $\tau(\mathscr{J}^6) = \tau(\Im^3) = \phi(D_8^*)^2$.

Then for $r = 5$ and $k = 6$ we have the lattice $\phi(D_8^*)^2$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 6$. We also have that $\tau(\mathscr{J}^8) = \phi\mathbb{Z}[i]^8$.

Now we will show, for $k = 7$, that $\tau(\mathscr{J}^7) = \phi\mathbb{Z}[i]^8 + C_7$, where

$$M_{C_7} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is the generator matrix of the linear binary block code C_7. In fact:

Since $\tau(\mathscr{J}^6) = \phi(D_8^*)^2$ and $\tau(\mathscr{J}^8) = \phi\mathbb{Z}[i]^8$, then we have $\phi(D_8^*)^2/\tau(\mathscr{J}^7)/\phi\mathbb{Z}[i]^8$. Ob-

serve that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta)),$$

then $\mathscr{J}^7 = \mathscr{J}^8 \cup (\mathscr{J}^8 + (1+\beta)(1+\theta)^3)$. So we have

$$\tau(\mathscr{J}^7) = \tau(\mathscr{J}^8) \cup \tau(\mathscr{J}^8 + (1+\beta)(1+\theta)^3) = \phi\mathbb{Z}[i]^8 \cup \tau(\mathscr{J}^8 + (1+\beta)(1+\theta)^3).$$

Also observe that

$$\tau(\mathscr{J}^8 + (1+\beta)(1+\theta)^3) = \tau(\mathscr{J}^8) + \tau((1+\beta)(1+\theta)^3) =$$

$$= \phi\mathbb{Z}[i]^8 + \tau(1+\beta+\theta+\beta\theta+\theta^2+\beta\theta^2+\theta^3+\beta\theta^3),$$

since $2 \equiv 0$ (modulo ϕ), and we have

$$\tau(1+\beta+\theta+\beta\theta+\theta^2+\beta\theta^2+\theta^3+\beta\theta^3) = (1+\beta+\theta+\beta\theta+\theta^2+\beta\theta^2+\theta^3+\beta\theta^3,$$

$$1+\tau_2(\beta)+\tau_2(\theta)+\tau_2(\beta\theta)+\tau_2(\theta^2)+\tau_2(\beta\theta^2)+\tau_2(\theta^3)+\tau_2(\beta\theta^3),\ldots,$$

$$1+\tau_8(\beta)+\tau_8(\theta)+\tau_8(\beta\theta)+\tau_8(\theta^2)+\tau_8(\beta\theta^2)+\tau_8(\theta^3)+\tau_8(\beta\theta^3)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau((1+\beta)(1+\theta)^3) = M \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1+\beta+\theta+\beta\theta+\theta^2+\beta\theta^2+\theta^3+\beta\theta^3 \\ 1+\tau_2(\beta)+\tau_2(\theta)+\tau_2(\beta\theta)+\tau_2(\theta^2)+\tau_2(\beta\theta^2)+\tau_2(\theta^3)+\tau_2(\beta\theta^3) \\ 1+\tau_3(\beta)+\tau_3(\theta)+\tau_3(\beta\theta)+\tau_3(\theta^2)+\tau_3(\beta\theta^2)+\tau_3(\theta^3)+\tau_3(\beta\theta^3) \\ 1+\tau_4(\beta)+\tau_4(\theta)+\tau_4(\beta\theta)+\tau_4(\theta^2)+\tau_4(\beta\theta^2)+\tau_4(\theta^3)+\tau_4(\beta\theta^3) \\ \vdots \\ 1+\tau_8(\beta)+\tau_8(\theta)+\tau_8(\beta\theta)+\tau_8(\theta^2)+\tau_8(\beta\theta^2)+\tau_8(\theta^3)+\tau_8(\beta\theta^3) \end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^8+(1+\beta)(1+\theta)^3) = \phi\mathbb{Z}[i]^8+(1,1,1,1,1,1,1,1)$$

and

$$\tau(\mathscr{J}^7) = \phi\mathbb{Z}[i]^8 \cup (\phi\mathbb{Z}[i]^8+(1,1,1,1,1,1,1,1)) = \phi\mathbb{Z}[i]^8+C_7 = \phi D_{16}^*,$$

where $C_7=(8,1,8)$ is the linear binary block code generated by the matrix

$$M_{C_7} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^7$.

Then, for $r=5$ and $k=7$, we have the lattice $\phi\mathbb{Z}[i]^8+C_7=\phi D_{16}^*$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k=7$ and C_7 is a linear binary block code with parameters $(8,1,8)$.

So now let's find the construction A of the lattice for $k=6$. In fact, we have $\tau(\mathscr{J}^6) = \phi(D_8^*)^2$, $\tau(\mathscr{J}^7)=\phi D_{16}^*=\phi\mathbb{Z}[i]^8+C_7$ and $\tau(\mathscr{J}^6)=\phi(D_8^*)^2/\tau(\mathscr{J}^7)=\phi\mathbb{Z}[i]^8+C_7$. Observe that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2+(1+\beta)),$$

then $\mathscr{J}^6=\mathscr{J}^7\cup(\mathscr{J}^7+(1+\beta)^2(1+\theta)^2)$. So we have

$$\tau(\mathscr{J}^6) = \tau(\mathscr{J}^7)\cup\tau(\mathscr{J}^7+(1+\theta)^3) = (\phi\mathbb{Z}[i]^8+C_7)\cup\tau(\mathscr{J}^7+(1+\theta)^3),$$

since $2\equiv 0$ (modulo ϕ).

Also observe that

$$\tau(\mathscr{J}^7+(1+\theta)^3) = \tau(\mathscr{J}^7)+\tau((1+\theta)^3) =$$

$$= (\phi\mathbb{Z}[i]^8 + C_7) + \tau(1+\theta+\theta^2+\theta^3),$$

since $2 \equiv 0$ (modulo ϕ), and we have

$$\tau(1+\theta+\theta^2+\theta^3) = (1+\theta+\theta^2+\theta^3,$$

$$1+\tau_2(\theta)+\tau_2(\theta^2)+\tau_2(\theta^3),\ldots,1+\tau_8(\theta)+\tau_8(\theta^2)+\tau_8(\theta^3)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau((1+\theta)^3) = M\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\theta+\theta^2+\theta^3 \\ 1+\tau_2(\theta)+\tau_2(\theta^2)+\tau_2(\theta^3) \\ 1+\tau_3(\theta)+\tau_3(\theta^2)+\tau_3(\theta^3) \\ 1+\tau_4(\theta)+\tau_4(\theta^2)+\tau_4(\theta^3) \\ \vdots \\ 1+\tau_8(\theta)+\tau_8(\theta^2)+\tau_8(\theta^3) \end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^7 + (1+\theta)^3) = (\phi\mathbb{Z}[i]^8 + C_7) + (1,0,1,0,1,0,1,0)$$

and

$$\tau(\mathscr{J}^6) = (\phi\mathbb{Z}[i]^8 + C_7) \cup ((\phi\mathbb{Z}[i]^8 + C_7) + (1,0,1,0,1,0,1,0)).$$

But since $\tau(\mathscr{J}^6) = (\phi\mathbb{Z}[i]^8 + C_7) \cup ((\phi\mathbb{Z}[i]^8 + C_7) + (1,0,1,0,1,0,1,0))$, the following proposition gives us the complex code formula of $\tau(\mathscr{J}^6)$:

Proposition 27. *Let $\Lambda = (\phi\mathbb{Z}[i]^n + C) \cup ((\phi\mathbb{Z}[i]^n + C) + c)$, where Λ is an n-dimensional lattice, C is a linear binary block code and c is an n-dimensional binary vector. Then $\Lambda = \phi\mathbb{Z}[i]^n + C'$, where C' is a linear binary block code, M_C is a generator matrix of the code C and $M_{C'}$ is a generator matrix of the code C', whose rows are formed by the rows of M_C by adding the binary vector c.*

Proof. Suppose that $c_1, c_2, \ldots, c_k$ and $c_1, c_2, \ldots, c_k, c$ are the rows of the matrices M_C and $M_{C'}$,

respectively, that is, the sets $\{c_1, c_2, \ldots, c_k\}$ and $\{c_1, c_2, \ldots, c_k, c\}$ are the basis of the linear binary block codes C and C', respectively.

We have to prove that $\Lambda = (\phi\mathbb{Z}[i]^n + C) \cup ((\phi\mathbb{Z}[i]^n + C) + c) = \phi\mathbb{Z}[i]^n + C'$; in fact: if $x \in \phi\mathbb{Z}[i]^n + C'$, then

$$x = \lambda + (a_1c_1 + a_2c_2 + \cdots + a_kc_k + a_{k+1}c),$$

where $\lambda \in \phi\mathbb{Z}[i]^n$ and $a_i \in \{0,1\}$, for $i = 1,2,\ldots,k+1$. So if $a_{k+1} = 0$, then $x \in \phi\mathbb{Z}[i]^n + C$, and if $a_{k+1} = 1$, then $x \in (\phi\mathbb{Z}[i]^n + C) + c$. Therefore $x \in \phi\mathbb{Z}[i]^n + C$ or $x \in (\phi\mathbb{Z}[i]^n + C) + c$, that is, $x \in (\phi\mathbb{Z}[i]^n + C) \cup ((\phi\mathbb{Z}[i]^n + C) + c)$. Then we can conclude that

$$(\phi\mathbb{Z}[i]^n + C') \subset ((\phi\mathbb{Z}[i]^n + C) \cup ((\phi\mathbb{Z}[i]^n + C) + c).$$

It is trivial that $(\phi\mathbb{Z}[i]^n + C) \cup ((\phi\mathbb{Z}[i]^n + C) + c) \subset (\phi\mathbb{Z}[i]^n + C')$, so $\Lambda = (\phi\mathbb{Z}[i]^n + C) \cup ((\phi\mathbb{Z}[i]^n + C) + c) = \phi\mathbb{Z}[i]^n + C'$. □

By the proposition 27 we can conclude that $\tau(\mathscr{J}^6) = \phi\mathbb{Z}[i]^8 + C_6$, where $C_6 = (8,2)$ is the linear binary block code generated by the matrix

$$M_{C_6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^6$.

So, for $r = 5$ and $k = 6$, we have the lattice $\phi\mathbb{Z}[i]^8 + C_6$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 6$ and C_6 is a linear binary block code with parameters $(8,2)$.

Now let's calculate the minimum Hamming distance of the code C_6: by permutation of the columns and elementary row operations, the matrix M_{C_6} becomes

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

We have $M_{C_6} = [I : P]$ and $H = [P^T : I]$, where H is the parity-check matrix of the code C_6

related to the generator matrix M_{C_6} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector it is necessary to make the sum of, at least, four lines of the matrix H^T, so the minimum Hamming distance of the code C_6 is given by 4 ($d_H(C_6) = 4$) and the parameters of the code C_6 are given by $(8,2,4)$.

Continuing the calculations, let's find the construction A of the lattice for $k = 5$. In fact, we have $\tau(\mathscr{J}^4) = D_4^4$ (by proposition 25), $\tau(\mathscr{J}^6) = \phi(D_8^*)^2 = \phi\mathbb{Z}[i]^8 + C_6$ and

$$\tau(\mathscr{J}^4) = D_4^4/\tau(\mathscr{J}^5)/\tau(\mathscr{J}^6) = \phi\mathbb{Z}[i]^8 + C_6 = \phi(D_8^*)^2.$$

Observe that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta)),$$

then $\mathscr{J}^5 = \mathscr{J}^6 \cup (\mathscr{J}^6 + (1+\beta)(1+\theta)^2)$. So we have

$$\tau(\mathscr{J}^5) = \tau(\mathscr{J}^6) \cup \tau(\mathscr{J}^6 + (1+\beta)(1+\theta)^2) = (\phi\mathbb{Z}[i]^8 + C_6) \cup \tau(\mathscr{J}^6 + (1+\beta)(1+\theta)^2).$$

Also observe that

$$\tau(\mathscr{J}^6 + (1+\beta)(1+\theta)^2) = \tau(\mathscr{J}^6) + \tau((1+\beta)(1+\theta)^2) =$$

$$= (\phi\mathbb{Z}[i]^8 + C_6) + \tau(1+\beta+\theta^2+\beta\theta^2),$$

since $2 \equiv 0$ (modulo ϕ), and we have

$$\tau(1+\beta+\theta^2+\beta\theta^2) = (1+\beta+\theta^2+\beta\theta^2,$$

$$1+\tau_2(\beta)+\tau_2(\theta^2)+\tau_2(\beta\theta^2),\ldots,1+\tau_8(\beta)+\tau_8(\theta^2)+\tau_8(\beta\theta^2)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the

identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau((1+\beta)(1+\theta)^2) = M\begin{pmatrix}1\\1\\0\\0\\1\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1+\beta+\theta^2+\beta\theta^2\\1+\tau_2(\beta)+\tau_2(\theta^2)+\tau_2(\beta\theta^2)\\1+\tau_3(\beta)+\tau_3(\theta^2)+\tau_3(\beta\theta^2)\\1+\tau_4(\beta)+\tau_4(\theta^2)+\tau_4(\beta\theta^2)\\\vdots\\1+\tau_8(\beta)+\tau_8(\theta^2)+\tau_8(\beta\theta^2)\end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^6+(1+\beta)(1+\theta)^2) = (\phi\mathbb{Z}[i]^8+C_6)+(1,1,0,0,1,1,0,0)$$

and

$$\tau(\mathscr{J}^5) = (\phi\mathbb{Z}[i]^8+C_6)\cup((\phi\mathbb{Z}[i]^8+C_6)+(1,1,0,0,1,1,0,0)).$$

But since $\tau(\mathscr{J}^5) = (\phi\mathbb{Z}[i]^8+C_6)\cup((\phi\mathbb{Z}[i]^8+C_6)+(1,1,0,0,1,1,0,0))$, by the proposition 27 we can conclude that $\tau(\mathscr{J}^5) = \phi\mathbb{Z}[i]^8+C_5$, where $C_5=(8,3)$ is the linear binary block code generated by the matrix

$$M_{C_5} = \begin{pmatrix}1&1&1&1&1&1&1&1\\1&0&1&0&1&0&1&0\\1&1&0&0&1&1&0&0\end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^5$.

So, for $r=5$ and $k=5$, we have the lattice $\phi\mathbb{Z}[i]^8+C_5$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k=5$ and C_5 is a linear binary block code with parameters $(8,3)$.

Now let's calculate the minimum Hamming distance of the code C_5: by elementary row operations, the matrix M_{C_5} becomes

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

We have $M_{C_5} = [I : P]$ and $H = [P^T : I]$, where H is the parity-check matrix of the code C_5 related to the generator matrix M_{C_5} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector it is necessary to make the sum of, at least, four lines of the matrix H^T, so the minimum Hamming distance of the code C_5 is given by 4 ($d_H(C_5) = 4$) and the parameters of the code C_5 are given by $(8,3,4)$.

So now let's find the construction A of the lattice for $k = 4$. In fact, we have $\tau(\mathscr{J}^4) = D_4^4$, $\tau(\mathscr{J}^5) = \phi\mathbb{Z}[i]^8 + C_5$ and

$$\tau(\mathscr{J}^4) = D_4^4/\tau(\mathscr{J}^5) = \phi\mathbb{Z}[i]^8 + C_5.$$

Observe that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta)),$$

then $\mathscr{J}^4 = \mathscr{J}^5 \cup (\mathscr{J}^5 + (1+\beta)(1+\beta)(1+\theta))$. So we have

$$\tau(\mathscr{J}^4) = \tau(\mathscr{J}^5) \cup \tau(\mathscr{J}^5 + (1+\beta)^2(1+\theta)) = (\phi\mathbb{Z}[i]^8 + C_5) \cup \tau(\mathscr{J}^5 + (1+\beta)^2(1+\theta)).$$

Also observe that

$$\tau(\mathscr{J}^5 + (1+\beta)^2(1+\theta)) = \tau(\mathscr{J}^5) + \tau((1+\beta)^2(1+\theta)) =$$

$$= (\phi\mathbb{Z}[i]^8 + C_5) + \tau(1+\theta^2),$$

since $2 \equiv 0$ (modulo ϕ), and we have

$$\tau(1+\theta^2) = (1+\theta^2, 1+\tau_2(\theta^2), \ldots, 1+\tau_8(\theta^2)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau((1+\beta)^2(1+\theta)) = M\begin{pmatrix}1\\0\\0\\0\\1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1+\theta^2\\1+\tau_2(\theta^2)\\1+\tau_3(\theta^2)\\1+\tau_4(\theta^2)\\\vdots\\1+\tau_8(\theta^2)\end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^5 + (1+\beta)^2(1+\theta)) = (\phi\mathbb{Z}[i]^8 + C_5) + (1,0,0,0,1,0,0,0)$$

and

$$\tau(\mathscr{J}^4) = (\phi\mathbb{Z}[i]^8 + C_5) \cup ((\phi\mathbb{Z}[i]^8 + C_5) + (1,0,0,0,1,0,0,0)).$$

But since $\tau(\mathscr{J}^4) = (\phi\mathbb{Z}[i]^8 + C_5) \cup ((\phi\mathbb{Z}[i]^8 + C_5) + (1,0,0,0,1,0,0,0))$, by the proposition 27 we can conclude that $\tau(\mathscr{J}^4) = \phi\mathbb{Z}[i]^8 + C_4$, where $C_4 = (8,4)$ is the linear binary block code generated by the matrix

$$M_{C_4} = \begin{pmatrix}1&1&1&1&1&1&1&1\\1&0&1&0&1&0&1&0\\1&1&0&0&1&1&0&0\\1&0&0&0&1&0&0&0\end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^4$.

So, for $r = 5$ and $k = 4$, we have the lattice $\phi\mathbb{Z}[i]^8 + C_4$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 4$ and C_4 is a linear binary block code with parameters $(8,4)$.

Now let's calculate the minimum Hamming distance of the code C_4: by elementary row operations, the matrix M_{C_4} becomes

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

We have $M_{C_4} = [I : P]$ and $H = [P^T : I]$, where H is the parity-check matrix of the code C_4 related to the generator matrix M_{C_4} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector it is necessary to make the sum of, at least, two lines of the matrix H^T, so the minimum Hamming distance of the code C_4 is given by 2 ($d_H(C_4) = 2$) and the parameters of the code C_4 are given by $(8,4,2)$.

Now we will show, for $k = 3$, that $\tau(\mathscr{J}^3) = \phi\mathbb{Z}[i]^8 + C_3$, where

$$M_{C_3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is the generator matrix of the linear binary block code C_3.

In fact, we have $\tau(\mathscr{J}^2) = D_8^2$ (by proposition 25), $\tau(\mathscr{J}^4) = D_4^4 = \phi\mathbb{Z}[i]^8 + C_4$ and

$$\tau(\mathscr{J}^2) = D_8^2/\tau(\mathscr{J}^3)/\tau(\mathscr{J}^4) = \phi\mathbb{Z}[i]^8 + C_4 = D_4^4.$$

Observe that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta)),$$

then $\mathscr{J}^3 = \mathscr{J}^4 \cup (\mathscr{J}^4 + (1+\beta)(1+\theta))$. So we have

$$\tau(\mathscr{J}^3) = \tau(\mathscr{J}^4) \cup \tau(\mathscr{J}^4 + (1+\beta)(1+\theta)) = (\phi\mathbb{Z}[i]^8 + C_4) \cup \tau(\mathscr{J}^4 + (1+\beta)(1+\theta)).$$

Also observe that

$$\tau(\mathscr{J}^4 + (1+\beta)(1+\theta)) = \tau(\mathscr{J}^4) + \tau((1+\beta)(1+\theta)) =$$

$$= (\phi\mathbb{Z}[i]^8 + C_4) + \tau(1+\beta+\theta+\beta\theta)$$

and we have

$$\tau(1+\beta+\theta+\beta\theta) =$$

$$= (1+\beta+\theta+\beta\theta, 1+\tau_2(\beta)+\tau_2(\theta)+\tau_2(\beta\theta), \ldots, 1+\tau_8(\beta)+\tau_8(\theta)+\tau_8(\beta\theta)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau((1+\beta)(1+\theta)) = M \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\beta+\theta+\beta\theta \\ 1+\tau_2(\beta)+\tau_2(\theta)+\tau_2(\beta\theta) \\ 1+\tau_3(\beta)+\tau_3(\theta)+\tau_3(\beta\theta) \\ 1+\tau_4(\beta)+\tau_4(\theta)+\tau_4(\beta\theta) \\ \vdots \\ 1+\tau_8(\beta)+\tau_8(\theta)+\tau_8(\beta\theta) \end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^4 + (1+\beta)(1+\theta)) = (\phi\mathbb{Z}[i]^8 + C_4) + (1,1,1,1,0,0,0,0)$$

and

$$\tau(\mathscr{J}^3) = (\phi\mathbb{Z}[i]^8 + C_4) \cup ((\phi\mathbb{Z}[i]^8 + C_4) + (1,1,1,1,0,0,0,0)).$$

But since $\tau(\mathscr{J}^3) = (\phi\mathbb{Z}[i]^8 + C_4) \cup ((\phi\mathbb{Z}[i]^8 + C_4) + (1,1,1,1,0,0,0,0))$, by the proposition 27 we can conclude that $\tau(\mathscr{J}^3) = \phi\mathbb{Z}[i]^8 + C_3$, where $C_3 = (8,5)$ is the linear binary block code generated by the matrix

$$M_{C_3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^3$.

So, for $r = 5$ and $k = 3$, we have the lattice $\phi\mathbb{Z}[i]^8 + C_3$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 3$ and C_3 is a linear binary block code with parameters $(8,5)$.

Now let's calculate the minimum Hamming distance of the code C_3: by elementary row operations, the matrix M_{C_3} becomes

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

We have $M_{C_3} = [I : P]$ and $H = [P^T : I]$, where H is the parity-check matrix of the code C_3 related to the generator matrix M_{C_3} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector it is necessary to make the sum of, at least, two lines of the matrix H^T, so the minimum Hamming distance of the code C_3 is given by 2 ($d_H(C_3) = 2$) and the parameters of the code C_3 are given by $(8,5,2)$.

By continuing the calculations, we will find the construction A of the lattice for $k = 2$, that is, we will show that $\tau(\mathscr{J}^2) = D_8^2 = \phi\mathbb{Z}[i]^8 + C_2$, where

$$M_{C_2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is the generator matrix of the linear binary block code C_2.

In fact, we have $\tau(\mathscr{J}) = D_{16}$, $\tau(\mathscr{J}^2) = D_8^2$, $\tau(\mathscr{J}^3) = \phi\mathbb{Z}[i]^8 + C_3$ and

$$\tau(\mathscr{J}) = D_{16}/\tau(\mathscr{J}^2) = D_8^2/\tau(\mathscr{J}^3) = \phi\mathbb{Z}[i]^8 + C_3.$$

Observe that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta)),$$

then $\mathscr{J}^2 = \mathscr{J}^3 \cup (\mathscr{J}^3 + (1+\beta)^2)$. So we have

$$\tau(\mathscr{J}^2) = \tau(\mathscr{J}^3) \cup \tau(\mathscr{J}^3 + (1+\beta)^2) = (\phi\mathbb{Z}[i]^8 + C_3) \cup \tau(\mathscr{J}^3 + (1+\beta)^2).$$

Also observe that

$$\tau(\mathscr{J}^3 + (1+\beta)^2) = \tau(\mathscr{J}^3) + \tau((1+\beta)^2) =$$

$$= (\phi\mathbb{Z}[i]^8 + C_3) + \tau(1+\theta),$$

since $2 \equiv 0$ (modulo ϕ), and we have

$$\tau(1+\theta) = (1+\theta, 1+\tau_2(\theta), \ldots, 1+\tau_8(\theta)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau((1+\beta)^2) = M \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\theta \\ 1+\tau_2(\theta) \\ 1+\tau_3(\theta) \\ 1+\tau_4(\theta) \\ \vdots \\ 1+\tau_8(\theta) \end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^3 + (1+\beta)^2) = (\phi\mathbb{Z}[i]^8 + C_3) + (1,0,1,0,0,0,0,0)$$

and

$$\tau(\mathscr{J}^2) = (\phi\mathbb{Z}[i]^8 + C_3) \cup ((\phi\mathbb{Z}[i]^8 + C_3) + (1,0,1,0,0,0,0,0)).$$

But since $\tau(\mathscr{J}^2) = (\phi\mathbb{Z}[i]^8 + C_3) \cup ((\phi\mathbb{Z}[i]^8 + C_3) + (1,0,1,0,0,0,0,0))$, by the proposition 27 we can conclude that $\tau(\mathscr{J}^2) = \phi\mathbb{Z}[i]^8 + C_2$, where $C_2 = (8,6)$ is the linear binary block code generated by the matrix

$$M_{C_2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^2$.

So, for $r = 5$ and $k = 2$, we have the lattice $\phi\mathbb{Z}[i]^8 + C_2$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 2$ and C_2 is a linear binary block code with parameters $(8,6)$.

Now let's calculate the minimum Hamming distance of the code C_2: by elementary row operations, the matrix M_{C_2} becomes

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

We have $M_{C_2} = [I : P]$ and $H = [P^T : I]$, where H is the parity-check matrix of the code C_2 related to the generator matrix M_{C_2} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Observe that for obtaining the null vector it is necessary to make the sum of, at least, two lines of the matrix H^T, so the minimum Hamming distance of the code C_2 is given by 2 ($d_H(C_2) = 2$) and the parameters of the code C_2 are given by $(8,6,2)$.

Finally we are going to find the construction B of the lattice for $k = 1$. In fact, we have $\tau(\mathscr{J}) = D_{16}$, $\tau(\mathscr{J}^2) = D_8^2 = \phi\mathbb{Z}[i]^8 + C_2$ and

$$\mathbb{Z}[i]^8/\tau(\mathscr{J}) = D_{16}/\tau(\mathscr{J}^2) = D_8^2 = \phi\mathbb{Z}[i]^8 + C_2.$$

Observe that

$$\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta)),$$

then $\tau(\mathscr{J}) = \tau(\mathscr{J}^2) \cup \tau(\mathscr{J}^2 + (1+\beta)) = (\phi\mathbb{Z}[i]^8 + C_2) \cup \tau(\mathscr{J}^2 + (1+\beta))$.

Also observe that

$$\tau(\mathscr{J}^2 + (1+\beta)) = \tau(\mathscr{J}^2) + \tau(1+\beta) =$$

$$= (\phi\mathbb{Z}[i]^8 + C_2) + \tau(1+\beta)$$

and we have

$$\tau(1+\beta) = (1+\beta, 1+\tau_2(\beta), \ldots, 1+\tau_8(\beta)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_8\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

We know that (53) is a $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ and (54) is a generator matrix of the complex algebraic lattice $\tau(O_{\mathbb{L}})$, so it follows that

$$\tau(1+\beta) = M \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\beta \\ 1+\tau_2(\beta) \\ 1+\tau_3(\beta) \\ 1+\tau_4(\beta) \\ \vdots \\ 1+\tau_8(\beta) \end{pmatrix}.$$

Therefore we have

$$\tau(\mathscr{J}^2+(1+\beta))=(\phi\mathbb{Z}[i]^8+C_2)+(1,1,0,0,0,0,0,0)$$

and

$$\tau(\mathscr{J})=(\phi\mathbb{Z}[i]^8+C_2)\cup((\phi\mathbb{Z}[i]^8+C_2)+(1,1,0,0,0,0,0,0)).$$

But since $\tau(\mathscr{J})=(\phi\mathbb{Z}[i]^8+C_2)\cup((\phi\mathbb{Z}[i]^8+C_2)+(1,1,0,0,0,0,0,0))$, by the proposition 27 we can conclude that $\tau(\mathscr{J})=\phi\mathbb{Z}[i]^8+C_1$, where $C_1=(8,7)$ is the linear binary block code generated by the matrix

$$M_{C_1}=\begin{pmatrix}1&1&1&1&1&1&1&1\\1&0&1&0&1&0&1&0\\1&1&0&0&1&1&0&0\\1&0&0&0&1&0&0&0\\1&1&1&1&0&0&0&0\\1&0&1&0&0&0&0&0\\1&1&0&0&0&0&0&0\end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}$.

So, for $r=5$ and $k=1$, we have the lattice $\phi\mathbb{Z}[i]^8+C_1$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k=1$ and C_1 is a linear binary block code with parameters $(8,7)$.

Now let's calculate the minimum Hamming distance of the code C_1: by elementary row operations, the matrix M_{C_1} becomes

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

We have $M_{C_1}=[I:P]$ and $H=[P^T:I]$, where H is the parity-check matrix of the code C_1

related to the generator matrix M_{C_1} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Observe that for obtaining the null vector it is necessary to make the sum of, at least, two lines of the matrix H^T, so the minimum Hamming distance of the code C_1 is given by 2 ($d_H(C_1) = 2$) and the parameters of the code C_1 are given by $(8,7,2)$. Then $\tau(\mathscr{J}) = \phi\mathbb{Z}[i]^8 + C_1 = \phi\mathbb{Z}[i]^8 + (8,7,2) = D_{16}$.

Therefore we have obtained the construction A of the lattices related to the canonical embedding of the ideals $\mathscr{J}^k$, $k = 1,2,3,\ldots,7$.

We know that the lattice related to the canonical embedding of the ideal when $k = 0$ is isomorphic to the $\mathbb{Z}[i]^8$-lattice and we have $\mathbb{Z}[i]^8 = D_{16} \cup (D_{16} + (1,0,0,0,0,0,0,0))$.

Since $\tau(\mathscr{J}) = \phi\mathbb{Z}[i]^8 + C_1 = \phi\mathbb{Z}[i]^8 + (8,7,2) = D_{16}$, we can conclude that

$$\mathbb{Z}[i]^8 = (\phi\mathbb{Z}[i]^8 + C_1) \cup ((\phi\mathbb{Z}[i]^8 + C_1) + (1,0,0,0,0,0,0,0))$$

and by the proposition 27 we have $\mathbb{Z}[i]^8 = \phi\mathbb{Z}[i]^8 + C_0$, where $C_0 = (8,8)$ is the linear binary block code generated by the matrix

$$M_{C_0} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal when $k = 0$, that is, we obtained the construction A of the $\mathbb{Z}[i]^8$-lattice.

So, for $r = 5$ and $k = 0$, we have the lattice $\mathbb{Z}[i]^8 = \phi\mathbb{Z}[i]^8 + C_0$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 0$ and C_0 is a linear binary block code with parameters $(8,8)$.

Now let's calculate the minimum Hamming distance of the code C_0: by elementary row operations, the matrix M_{C_0} becomes

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

We have $M_{C_0} = I$ and $H = (0,0,0,0,0,0,0,0)$, where H is the parity-check matrix of the code C_0 related to the generator matrix M_{C_0} and T denotes the transpose of a matrix. Then

$$H^T = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

As all the lines of the matrix H^T are equal to the null vector, so the minimum Hamming distance of the code C_0 is given by 1 ($d_H(C_0) = 1$) and the parameters of the code C_0 are given by $(8,8,1)$. Then $\mathbb{Z}[i]^8 = \phi\mathbb{Z}[i]^8 + C_0 = \phi\mathbb{Z}[i]^8 + (8,8,1) = \phi\mathbb{Z}[i]^8 + \mathbb{F}_2^8$, where $\mathbb{F}_2 = \{0,1\}$.

Thus, we have found the construction A of the lattices related to the canonical embedding of the ideals $\mathscr{J}^k$, where $k = 0,1,2,\ldots,7$.

5.3.1.2 *The Pascal's triangle and the extension by periodicity of the lattice partition chain related to r=5*

In section 5.3.1.1, for $r = 5$ and $k = 0$, we have the lattice $\mathbb{Z}[i]^8 = \phi\mathbb{Z}[i]^8 + C_0$, whose position compared to the $\mathbb{Z}[i]^8$-lattice is equal to $k = 0$ and C_0 is a linear binary block code with parameters $(8,8,1)$. We can note a relation between the generators of the codes C_k, where $k = 0,1,\ldots,7$, and the Pascal's triangle.

Observe that the code C_0 is the universal code $\mathbb{F}_2^8$ and its generator matrix is given by the matrix M_{C_0}. By (HODGSON, 1992), page 36, we note that the lines of the matrix M_{C_0} are the rows $0,1,2,\ldots,7$ of the Pascal's triangle modulo 2. Also, observe that if we remove the row 0

of the Pascal's triangle modulo 2, we will obtain the lines of the matrix M_{C_1}, which generates the code C_1, and the lattice $\tau(\mathscr{J}) = \phi\mathbb{Z}[i]^8 + C_1 = D_{16}$, which is related to $k = 1$.

Then we can conclude that if we remove the rows $0, 1, \ldots, j$ of the Pascal's triangle modulo 2, where $0 \leq j \leq 6$, we will obtain the lines of the matrix $M_{C_{j+1}}$, which generates the code C_{j+1}, and the lattice $\tau(\mathscr{J}^{j+1}) = \phi\mathbb{Z}[i]^8 + C_{j+1}$, which is related to $k = j+1$.

Since $\tau(\mathscr{J}^8) = \phi\mathbb{Z}[i]^8$, we have that the matrix $(M_{\mu'})^8$ generates the lattice $\phi\mathbb{Z}[i]^8$. But we know that the matrix $\phi I_{8\times 8}$ also generates the lattice $\phi\mathbb{Z}[i]^8$, where $I_{8\times 8}$ is the 8×8 identity matrix.

Therefore, we can conclude that the matrices $(M_{\mu'})^8$ and $\phi I_{8\times 8}$ are equivalent. Hence, using this fact, the following proposition gives us the extension by periodicity of the lattice partition chain for the positive positions, that is, $k \geq 0$:

Proposition 28. *For $k = 8\alpha + j$, where $\alpha \in \mathbb{N}$ and $0 \leq j \leq 7$, we have that $M_{\mu'^{(8\alpha+j)}} = (M_{\mu'})^{k=(8\alpha+j)}$ is a generator matrix of the lattice $\phi^\alpha\Lambda_j$ seen as a $\mathbb{Z}[i]$-lattice, where Λ_j is the lattice found previously in the section 5.3.1.1 related to the position k compared to the $\mathbb{Z}[i]^8$-lattice.*

Proof. By previously, we have found the lattices Λ_j, where $0 \leq j \leq 7$ and Λ_j is the lattice related to the position k, and we have that $M_{\mu'^j} = (M_{\mu'})^j$ is a generator matrix of the lattice Λ_j. We know that the matrices $(M_{\mu'})^8$ and $\phi I_{8\times 8}$ are equivalent.

For $k = 8$, the matrix $(M_{\mu'})^8$ generates the lattice $\phi\mathbb{Z}[i]^8$; for $k = 8 + j$, we have $M_{\mu'^{(8+j)}} = (M_{\mu'})^{(8+j)} = ((M_{\mu'})^8)(M_{\mu'})^j = \phi(M_{\mu'})^j$ as being a generator matrix of the lattice $\phi\Lambda_j$ and for $k = 16 + j$, we have $M_{\mu'^{(16+j)}} = (M_{\mu'})^{(16+j)} = ((M_{\mu'})^{16})(M_{\mu'})^j = \phi^2(M_{\mu'})^j = 2(M_{\mu'})^j$ as being a generator matrix of the lattice $2\Lambda_j$, since the matrices $(M_{\mu'})^8$ and $\phi I_{8\times 8}$ are equivalent.

So let's suppose, by induction hypothesis, that $(M_{\mu'})^{8\alpha+j}$, $\alpha \in \mathbb{N}$ and $0 \leq j \leq 7$, is a generator matrix of the lattice $\phi^\alpha\Lambda_j$.

We will show, for $k = 8(\alpha+1) + j$, that the lattice $\phi^{\alpha+1}\Lambda_j$ has a generator matrix as being the matrix $(M_{\mu'})^{(8(\alpha+1)+j)}$. In fact, $(M_{\mu'})^{8(\alpha+1)+j} = ((M_{\mu'})^8)((M_{\mu'})^{(8\alpha+j)})$, using the induction hypothesis and the fact that $\phi I_{8\times 8}$ and $(M_{\mu'})^8$ are equivalent matrices, we have $(M_{\mu'})^{8(\alpha+1)+j}$ as a generator matrix of the lattice $\phi^{\alpha+1}\Lambda_j$.

Therefore we showed that for $k = 8\alpha + j$, $\alpha \in \mathbb{N}$ and $0 \leq j \leq 7$, the matrix $(M_{\mu'})^{8\alpha+j}$ is a generator matrix of the lattice $\phi^\alpha\Lambda_j$.

But if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}$. Then $\phi^\alpha\Lambda_j = 2^{\alpha/2}\Lambda_j$, for $\alpha \neq 0$, and when $\alpha = 0$ we have the lattice Λ_j.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$, then $\phi^\alpha\Lambda_j = 2^{(\alpha-1)/2}\phi\Lambda_j$. □

And now the following proposition gives us the extension by periodicity of the lattice partition chain for the negative positions, that is, $k \leq -1$:

Proposition 29. *For all $k \in \mathbb{N}^*$, we have $\tau(\mathscr{J}^{-k}) = \tau(\mathscr{J}^{k})^*$, where $\tau(\mathscr{J}^{k})^*$ indicates the dual lattice of $\tau(\mathscr{J}^{k})$.*

Proof. Let $\overrightarrow{x}$ and $\overrightarrow{y}$ be arbitrary elements of $\tau(\mathscr{J}^{k})$ and $\tau(\mathscr{J}^{-k})$, respectively, where $k \in \mathbb{N}^*$. Therefore we have

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{\mathbb{L}/\mathbb{Q}(i)}(x \cdot y),$$

where $x \in \mathscr{J}^{k}$ and $y \in \mathscr{J}^{-k}$, then $x = (1+\xi_{32})^k x_0$, with $x_0 \in O_{\mathbb{L}}$, and $y = (1+\xi_{32})^{-k} y_0$, with $y_0 \in O_{\mathbb{L}}$.

It is easy to see that

$$Tr_{\mathbb{L}/\mathbb{Q}(i)}(x \cdot y) = \sum_{i=1}^{8} \tau_i(x \cdot y) = \sum_{i=1}^{8} \tau_i(x)\tau_i(y) = \sum_{i=1}^{8} \tau_i(x_0)\tau_i(y_0) = Tr_{\mathbb{L}/\mathbb{Q}(i)}(x_0 \cdot y_0).$$

Since the Galois group of the field extension $[\mathbb{L}/\mathbb{Q}(i)]$ is given by $\{\tau_1, \tau_2, \ldots, \tau_8\} = \langle \tau_2 \rangle$, where $\tau_i : \mathbb{L} \to \mathbb{L}$, for $i = 1, 2, \ldots, 8$, $\tau_1 = id$ (id is the identity map), $\tau_2(\xi_{32}) = \xi_{32}^5$, $\tau_3(\xi_{32}) = -i\xi_{32}$, $\tau_4(\xi_{32}) = -i\xi_{32}^5$, $\tau_5(\xi_{32}) = -\xi_{32}$, $\tau_6(\xi_{32}) = -\xi_{32}^5$, $\tau_7(\xi_{32}) = i\xi_{32}$ and $\tau_8(\xi_{32}) = i\xi_{32}^5$, by straightforward computation we have that $Tr_{\mathbb{L}/\mathbb{Q}(i)}(x_0 \cdot y_0) \in \mathbb{Z} \subset \mathbb{Z}[i]$, so

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{\mathbb{L}/\mathbb{Q}(i)}(x \cdot y) \in \mathbb{Z}[i].$$

Then $\tau(\mathscr{J}^{-k}) \subset \tau(\mathscr{J}^{k})^*$, for all $k \in \mathbb{N}^*$. We also have that

$$Vol[\tau(\mathscr{J}^{k})^*] = \frac{1}{Vol[\tau(\mathscr{J}^{k})]} = Vol[\tau(\mathscr{J}^{-k})].$$

However the index $|\tau(\mathscr{J}^{k})^* / \tau(\mathscr{J}^{-k})|$ is equal to 1 and so $\tau(\mathscr{J}^{-k}) = \tau(\mathscr{J}^{k})^*$. □

So we obtained the lattice partition chain related to $r = 5$, the relation between the construction A of the lattices of such a lattice partition chain and the Pascal's triangle and the extension by periodicity of this lattice partition chain. Now the following section is going to give us the generalization of the lattice partition chain for any $r \geq 3$ (for any dimension $n = 2^{r-2}$, where $r \geq 3$).

5.3.2 The generalization of the lattice partition chain for any $r \geq 3$

We are going to start this section showing that, for any $r \geq 3$ (for any dimension $n = 2^{r-2}$, where $r \geq 3$), the lattice related to $k = 1$ is given by the lattice D_{2n}, where $n = 2^{(r-2)}$.

For $r \geq 3$, suppose that $\sigma(\Im) = D_n$ and we know, by the proposition 25, that $\tau(\mathscr{J}^2) = \tau(\Im) = D_n^2$.

Therefore, for $r \geq 3$ and $k = 2$, we have the lattice D_n^2, whose position compared to the $\mathbb{Z}[i]^n$-lattice is equal to $k = 2$. We also know that $\tau(\mathscr{J}^n) = \phi\mathbb{Z}[i]^n$ and the lattice related to the canonical embedding of the ideal when $k = 0$ is isomorphic to the $\mathbb{Z}[i]^n$-lattice.

The following proposition will show us, for any $r \geq 3$, that the lattice related to $k = 1$ is given by the lattice D_{2n}, where $n = 2^{(r-2)}$:

Proposition 30. *We have, for $k = 1$, that $\tau(\mathscr{J}) = D_{2n}$, where $n = 2^{(r-2)}$.*

Proof. We have $\mathbb{Z}[i]^n/\tau(\mathscr{J})/D_n^2$ and

$$\mathbb{Z}[i]^n = D_n^2 \cup (D_n \oplus (D_n + (1,0,0,\ldots,0))) \cup$$

$$\cup((D_n + (1,0,0,\ldots,0)) \oplus D_n) \cup ((D_n + (1,0,0,\ldots,0)) \oplus (D_n + (1,0,0,\ldots,0))) =$$

$$= D_n^2 \cup (D_n^2 + (0,1,0,0,\ldots,0)) \cup$$

$$\cup(D_n^2 + (1,0,0,\ldots,0)) \cup (D_n^2 + (1,1,0,0,\ldots,0)).$$

So $\tau(\mathscr{J})$ is the union of D_n^2 with either $(D_n \oplus (D_n + (1,0,0,\ldots,0)))$, or $((D_n + (1,0,0,\ldots,0)) \oplus D_n)$ or $((D_n + (1,0,0,\ldots,0)) \oplus (D_n + (1,0,0,\ldots,0)))$.

Observe that $\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta))$, then $\tau(\mathscr{J}) = \tau(\mathscr{J}^2) \cup \tau(\mathscr{J}^2 + (1+\beta)) = D_n^2 \cup \tau(\mathscr{J}^2 + (1+\beta))$ and we can conclude that $\tau(\mathscr{J}^2 + (1+\beta))$ is equal to either $(D_n \oplus (D_n + (1,0,0,\ldots,0)))$, or $((D_n + (1,0,0,\ldots,0)) \oplus D_n)$ or $((D_n + (1,0,0,\ldots,0)) \oplus (D_n + (1,0,0,\ldots,0)))$.

We have $\tau(\mathscr{J}^2 + (1+\beta)) = \tau(\mathscr{J}^2) + \tau(1+\beta) = D_n^2 + \tau(1+\beta)$, where

$$\tau(1+\beta) = (1+\beta, \tau_2(1+\beta), \ldots, \tau_n(1+\beta)) = (1+\beta, 1+\tau_2(\beta), \ldots, 1+\tau_n(\beta)),$$

where $\{id = \tau_1, \tau_2, \tau_3, \ldots, \tau_n\}$ is the Galois group of the field extension $\mathbb{L}/\mathbb{Q}(i)$ and id is the identity map.

A $\mathbb{Z}[i]$-basis of $O_{\mathbb{L}}$ is given by

$$\{1,\beta,\beta^2,\beta^3,\ldots,\beta^{n-1}\} = \{1,\beta,\theta,\theta\beta,\theta^2,\theta^2\beta,\theta^3,\theta^3\beta,\ldots,\theta^{2^{r-3}-1},\theta^{2^{r-3}-1}\beta\}. \tag{55}$$

So the matrix

$$M = \begin{pmatrix} 1 & \beta & \theta & \theta\beta & \theta^2 & \theta^2\beta & \cdots & \theta^{2^{r-3}-1}\beta \\ 1 & \tau_2(\beta) & \tau_2(\theta) & \tau_2(\theta\beta) & \tau_2(\theta^2) & \tau_2(\theta^2\beta) & \cdots & \tau_2(\theta^{2^{r-3}-1}\beta) \\ 1 & \tau_3(\beta) & \tau_3(\theta) & \tau_3(\theta\beta) & \tau_3(\theta^2) & \tau_3(\theta^2\beta) & \cdots & \tau_3(\theta^{2^{r-3}-1}\beta) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \tau_n(\beta) & \tau_n(\theta) & \tau_n(\theta\beta) & \tau_n(\theta^2) & \tau_n(\theta^2\beta) & \cdots & \tau_n(\theta^{2^{r-3}-1}\beta) \end{pmatrix} \tag{56}$$

generates the complex algebraic lattice $\tau(O_{\mathbb{L}})$.

However it follows that

$$\tau(1+\beta) = M\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1+\beta \\ 1+\tau_2(\beta) \\ 1+\tau_3(\beta) \\ 1+\tau_4(\beta) \\ 1+\tau_5(\beta) \\ \vdots \\ 1+\tau_n(\beta) \end{pmatrix}.$$

Therefore we have that

$$\tau(\mathscr{J}^2+(1+\beta)) = D_n^2+(1,1,0,0,\ldots,0) = (D_n+(1,0,0,\ldots,0))\oplus(D_n+(1,0,0,\ldots,0))$$

and

$$\tau(\mathscr{J}) = D_n^2 \cup ((D_n+(1,0,0,\ldots,0))\oplus(D_n+(1,0,0,\ldots,0))) = D_{2n}.$$

So, for $r \geq 3$ and $k = 1$, we have the lattice D_{2n}, whose position compared to the $\mathbb{Z}[i]^n$-lattice is equal to $k = 1$. □

From now on we are going to explain how to obtain, for any $r \geq 3$, the construction A of the lattices related to the canonical embedding of the ideals $\mathscr{J}^k$, $k = 1,2,3,\ldots,n-1$. We will use the same construction from the previous section to obtain the generalization, so first, for each $k = 1,2,3,\ldots,n-1$, we will find the binary vector related to each k such that this binary vector is added to the code related to the construction A of the posterior lattice (we will again make use of the proposition 27), that is, the lattice related to the position $k+1$. Then, after that, we

will have the construction A of these lattices.

Let $r \geq 3$ and $n = 2^{r-2}$, we have that $\Im = \mathscr{J}^2$, $\beta^2 = \theta$ and

$$\{1, \beta, \theta, \beta\theta, \theta^2, \beta\theta^2, \ldots, \theta^{2^{r-3}-1}, \beta\theta^{2^{r-3}-1}\}$$

is a $\mathbb{Z}[i]$-basis of $\mathbb{L}$. Then

$$M = \begin{pmatrix} 1 & \beta & \theta & \theta\beta & \theta^2 & \theta^2\beta & \cdots & \theta^{2^{r-3}-1}\beta \\ 1 & \tau_2(\beta) & \tau_2(\theta) & \tau_2(\theta\beta) & \tau_2(\theta^2) & \tau_2(\theta^2\beta) & \cdots & \tau_2(\theta^{2^{r-3}-1}\beta) \\ 1 & \tau_3(\beta) & \tau_3(\theta) & \tau_3(\theta\beta) & \tau_3(\theta^2) & \tau_3(\theta^2\beta) & \cdots & \tau_3(\theta^{2^{r-3}-1}\beta) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \tau_n(\beta) & \tau_n(\theta) & \tau_n(\theta\beta) & \tau_n(\theta^2) & \tau_n(\theta^2\beta) & \cdots & \tau_n(\theta^{2^{r-3}-1}\beta) \end{pmatrix}$$

generates the complex algebraic lattice $\tau(O_{\mathbb{L}})$.

Let's find the binary vectors related to the positions k, where k is odd. In fact, let $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3} - 1) = w$. Since $\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta))$, we have

$$\mathscr{J}^k = \mathscr{J}^{k-1}\mathscr{J} = \mathscr{J}^{k+1} \cup (\mathscr{J}^{k+1} + (1+\theta)^{\alpha}(1+\beta)).$$

Observe in (HODGSON, 1992) that the row α from the Pascal's triangle modulo 2 indicates the coefficients of $(1+\theta)^{\alpha}$ modulo 2 (coefficients equal to 0 or 1).

For each $r \geq 3$ and $n = 2^{r-2}$ we have $1, \theta, \theta^2, \ldots, \theta^{2^{r-3}-1}$ and a $\mathbb{Z}[i]$-basis given by

$$\mathscr{B} = \{1, \beta, \theta, \beta\theta, \theta^2, \beta\theta^2, \ldots, \theta^{2^{r-3}-1}, \beta\theta^{2^{r-3}-1}\}.$$

We can see that the elements $1, \theta, \theta^2, \ldots, \theta^w$ are located at the odd positions of the basis $\mathscr{B}$ and the elements $\beta, \beta\theta, \ldots, \beta\theta^w$ are located at the even positions of the basis $\mathscr{B}$ and are posterior to the elements $1, \theta, \theta^2, \ldots, \theta^w$, respectively.

Therefore, for $k = 2\alpha + 1$, let the row α from the Pascal's triangle modulo 2 be filled by zeros to obtain $\frac{n}{2}$ coefficients. Thus, by observing the position of the elements of the basis $\mathscr{B}$ and the fact that for all $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3} - 1) = w$, we have $(1+\theta)^{\alpha}(1+\beta)$, we can conclude that each coefficient of the row α filled by zeros will be repeated twice and, after that, this new vector will have n coefficients.

However, with this construction we can find, for any $r \geq 3$, all the binary vectors with n coordinates related to the positions $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3} - 1) = w$.

For example, let $k = 9 = 2 \cdot 4 + 1 = 2 \cdot \alpha + 1$ and, in this case, we have $r = 6$ and $n = 16$. The row 4 from the Pascal's triangle modulo 2 is given by 10001 and filling it by zeros we have 10001000. So repeating each coefficient twice we have 1100000011000000. Then the binary

vector related to the position $k = 9$ is given by 1100000011000000.

But through the above construction we can also see, for any $r \geq 3$ ($n = 2^{r-2}$) and $k = 2\alpha + 1$, where $0 \leq \alpha \leq (2^{r-3} - 1) = w$, that the binary vector related to the position k is simply the row $2\alpha + 1$ from the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients modulo 2.

This can be verified through the basic properties given in (HODGSON, 1992):

1) Row $2^h - 1$ consists of 2^h ones: 111...111 (2^h 1's).

2) Row 2^h consists of two ones separated by $2^h - 1$ zeros: 100...001 (($2^h - 1$) 0's).

3) More generally, row $2^h + u$, where $0 \leq u < 2^h$, consists of two copies of the row u separated by $(2^h - 1 - u)$ zeros.

Now we are going to find the binary vectors related to the positions k, where k is even. In fact, let $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1) = w$. Since $\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1 + \beta))$, we have

$$\mathscr{J}^k = \mathscr{J}^{k-1}\mathscr{J} = \mathscr{J}^{k+1} \cup (\mathscr{J}^{k+1} + (1 + \theta)^\alpha).$$

Observe in (HODGSON, 1992) that the row α from the Pascal's triangle modulo 2 indicates the coefficients of $(1 + \theta)^\alpha$ modulo 2 (coefficients equal to 0 or 1).

For each $r \geq 3$ and $n = 2^{r-2}$ we have $1, \theta, \theta^2, \ldots, \theta^{2^{r-3}-1}$ and a $\mathbb{Z}[i]$-basis given by

$$\mathscr{B} = \{1, \beta, \theta, \beta\theta, \theta^2, \beta\theta^2, \ldots, \theta^{2^{r-3}-1}, \beta\theta^{2^{r-3}-1}\}.$$

We can see that the elements $1, \theta, \theta^2, \ldots, \theta^w$ are located at the odd positions of the basis $\mathscr{B}$ and the elements $\beta, \beta\theta, \ldots, \beta\theta^w$ are located at the even positions of the basis $\mathscr{B}$ and are posterior to the elements $1, \theta, \theta^2, \ldots, \theta^w$, respectively.

Therefore, for $k = 2\alpha$, let the row α from the Pascal's triangle modulo 2 be filled by zeros to obtain $\frac{n}{2}$ coefficients. Thus, by observing the position of the elements of the basis $\mathscr{B}$ and the fact that for all $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1) = w$, we have $(1 + \theta)^\alpha$, we can conclude that the coefficients of the row α filled by zeros will be put at the odd positions, with the same order, and the even positions will be equal to zero. After that, this new vector will have n coefficients (coordinates).

However, with this construction we can find, for any $r \geq 3$, all the binary vectors with n coordinates related to the positions $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1) = w$.

For example, let $k = 10 = 2 \cdot 5 = 2 \cdot \alpha$ and, in this case, we have $r = 6$ and $n = 16$. The row 5 from the Pascal's triangle modulo 2 is given by 110011 and filling it by zeros we have 11001100. So putting these coefficients at the odd positions, with the same order, and filling the even positions with zeros, we have 1010000010100000. Then the binary vector related to

the position $k = 10$ is given by 1010000010100000.

But through the above construction we can also see, for any $r \geq 3$ ($n = 2^{r-2}$) and $k = 2\alpha$, where $1 \leq \alpha \leq (2^{r-3} - 1) = w$, that the binary vector related to the position k is simply the row 2α from the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients modulo 2.

And analogously to the case where k is odd, this can be verified through the basic properties given in (HODGSON, 1992).

Since $\mathscr{J} = \mathscr{J}^2 \cup (\mathscr{J}^2 + (1+\beta))$, we have

$$\mathscr{J}^k = \mathscr{J}^{k-1}\mathscr{J} = \mathscr{J}^{k+1} \cup (\mathscr{J}^{k+1} + (1+\beta)(1+\theta)^\alpha),$$

when $k = 2\alpha + 1$, $0 \leq \alpha \leq 2^{r-3} - 1 = w$, and

$$\mathscr{J}^k = \mathscr{J}^{k-1}\mathscr{J} = \mathscr{J}^{k+1} \cup (\mathscr{J}^{k+1} + (1+\theta)^\alpha), \text{ when } k = 2\alpha,\ 1 \leq \alpha \leq 2^{r-3} - 1 = w.$$

Let's denote by c_k the binary vector with n coordinates related to the position k, $1 \leq k \leq n-1$. As we have seen, this vector c_k is found through the constructions above for the cases where k is either odd or even.

Then for obtaining the construction A of the lattice related to the canonical embedding of the ideal $\mathscr{J}^k$, $k = 1, 2, \ldots, n-1$, we have

$$\tau(\mathscr{J}^k) = \tau(\mathscr{J}^{k-1}\mathscr{J}) = \tau(\mathscr{J}^{k+1}) \cup (\tau(\mathscr{J}^{k+1}) + c_k) =$$

$$= (\phi\mathbb{Z}[i]^n + C_{k+1}) \cup ((\phi\mathbb{Z}[i]^n + C_{k+1}) + c_k),$$

where $\tau(\mathscr{J}^{k+1}) = \phi\mathbb{Z}[i]^n + C_{k+1}$ is the complex code formula for the lattice related to the canonical embedding of the ideal $\mathscr{J}^{k+1}$.

By using the proposition 27 we can conclude that $\tau(\mathscr{J}^k) = \phi\mathbb{Z}[i]^n + C_k$, where C_k is a linear binary block code and M_{C_k} is a generator matrix of the code C_k, whose rows are formed by the rows of $M_{C_{k+1}}$ by adding the binary vector c_k, where $M_{C_{k+1}}$ is a generator matrix of the code C_{k+1}.

So as we have $\tau(\mathscr{J}^n) = \phi\mathbb{Z}[i]^n$, we will obtain the construction A of the lattices related to the canonical embedding of the ideals $\mathscr{J}^k$, $k = 1, 2, \ldots, n-1$. As in the previous section (for $r = 5$), we are going to find the construction A of these lattices starting the calculations from the last position ($k = n-1$) to the first ($k = 1$).

We know that the lattice related to the canonical embedding of the ideal when $k = 0$ is isomorphic to the $\mathbb{Z}[i]^n$-lattice and we have $\mathbb{Z}[i]^n = D_n \cup (D_n + (1,0,0,\ldots,0))$.

Since $\tau(\mathscr{J}) = \phi\mathbb{Z}[i]^n + C_1$, we can conclude that

$$\mathbb{Z}[i]^n = (\phi\mathbb{Z}[i]^n + C_1) \cup ((\phi\mathbb{Z}[i]^n + C_1) + (1,0,0,\ldots,0))$$

and by the proposition 27 we have $\mathbb{Z}[i]^n = \phi\mathbb{Z}[i]^n + C_0$, where $C_0 = (n,n)$ is the linear binary block code generated by the matrix M_{C_0}, whose rows are formed by the rows of M_{C_1} by adding the vector $(1,0,0,\ldots,0)$, where M_{C_1} is a generator matrix of the code C_1.

However, we obtained the construction A of the lattice related to the canonical embedding of the ideal when $k = 0$, that is, we obtained the construction A of the $\mathbb{Z}[i]^n$-lattice.

So, for $r \geq 3$ and $k = 0$, we have the lattice $\mathbb{Z}[i]^n = \phi\mathbb{Z}[i]^n + C_0$, whose position compared to the $\mathbb{Z}[i]^n$-lattice is equal to $k = 0$ and C_0 is a linear binary block code with parameters (n,n).

Observe that the code C_0 is the universal code $\mathbb{F}_2^n$ and its generator matrix is given by the matrix M_{C_0}. By (HODGSON, 1992), page 36, we note that the lines of the matrix M_{C_0} are the rows $0,1,2,\ldots,n-1$ of the Pascal's triangle modulo 2 filled by zeros to obtain n coefficients (due to the construction to find the construction A of the lattices). Also observe that if we remove the row 0 of the Pascal's triangle modulo 2, that is, the first row of the matrix M_{C_0}, we will obtain the lines of the matrix M_{C_1}, which generates the code C_1, and the lattice $\tau(\mathscr{J}) = \phi\mathbb{Z}[i]^n + C_1 = D_{2n}$, which is related to $k = 1$.

Then we can conclude that if we remove the rows $0,1,\ldots,j$ of the Pascal's triangle modulo 2, where $0 \leq j \leq n-2$, we will obtain the lines of the matrix $M_{C_{j+1}}$, which generates the code C_{j+1}, and the lattice $\tau(\mathscr{J}^{j+1}) = \phi\mathbb{Z}[i]^n + C_{j+1}$, which is related to $k = j+1$. Also we can see that the dimension of the codes $C_{j+1} = C_k$, where $0 \leq j \leq n-2$, is given by $n-(j+1) = n-k$ and $d_k \leq d_{k+1}$, where d_k and d_{k+1} are the minimum Hamming distances of the codes C_k and C_{k+1}, respectively, since C_k is the augmented code.

The following proposition shows us that the minimum Hamming distance d_k of the code C_k, where $k = 1,2,\ldots,n-1 = 2^{r-2}-1$, is even and $d_k \geq 2$.

Proposition 31. *Let C_k be the linear binary block code related to the construction A at the position k, where $k = 1,2,\ldots,n-1 = 2^{r-2}-1$. Then d_k is even and $d_k \geq 2$, where d_k is the minimum Hamming distance of the code C_k.*

Proof. We have that C_0 is the universal code $\mathbb{F}_2^n$ and its generator matrix is given by the matrix M_{C_0}, whose rows are the rows $0,1,2,\ldots,n-1$ of the Pascal's triangle modulo 2 ((HODGSON, 1992)) filled by zeros to obtain n coefficients. We also know that the matrix M_{C_1} generates the code C_1, whose rows are the rows $1,2,\ldots,n-1$ of the Pascal's triangle modulo 2 filled by zeros (n coefficients), that is, are the rows of M_{C_0} by removing the first row of M_{C_0} (row 0 of the Pascal's triangle).

We are going to show, for any $r \geq 3$ ($n = 2^{r-2}$ and $k = 1,2,\ldots,n-1$), that the rows of the matrix M_{C_1} have an even number of 1's and, at least, two 1's. In fact, for $r = 3$ ($n = 2$ and $k = 1$) the matrix M_{C_1} is given by (11), so $d_1 = 2$ and is even.

For $r = 4$ ($n = 4$ and $k = 1,2,3$) the rows of the matrix M_{C_1} are given by the rows 1,2,3 of the Pascal's triangle modulo 2 filled by zeros to obtain 4 coefficients. And we can see that these rows have an even number of 1's and, at least, two 1's. So $d_k \geq 2$ and is even.

For $r = 5$ ($n = 8$ and $k = 1,2,3,4,5,6,7$) the rows of the matrix M_{C_1} are given by the rows 1,2,3,4,5,6,7 of the Pascal's triangle modulo 2 filled by zeros to obtain 8 coefficients. In (HODGSON, 1992) we have the following basic properties of the Pascal's triangle modulo 2:

1) Row $2^h - 1$ consists of 2^h ones: 111...111 (2^h 1's).

2) Row 2^h consists of two ones separated by $2^h - 1$ zeros: 100...001 (($2^h - 1$) 0's).

3) More generally, row $2^h + u$, where $0 \leq u < 2^h$, consists of two copies of the row u separated by $(2^h - 1 - u)$ zeros.

For $r = 4$ we already know that the rows 1,2,3 have an even number of 1's and, at least, two 1's. Observe that $r = h + 3$ and so $h = 2$. By the property 2) we have that the row 4 consists of two 1's separated by 3 zeros and, by the property 3), we have that the rows $4 + u$, where $1 \leq u \leq 3$, consist of 2 copies of the row u ($u = 1,2,3$) separated by $3 - u$ zeros.

Since the rows $u = 1,2,3$ have an even number of 1's and, at least, two 1's, by the property 3) the rows 5,6,7 have an even number of 1's and, at least, four 1's. So the rows 1,2,3,4,5,6,7 have an even number of 1's and, at least, two 1's (row 4).

Hence, by using these 3 properties, we are going to prove it by induction. Let $r \geq 3$, $r = h+3$, $k = 1,2,3,\ldots,n-1 = 2^{r-2} - 1$ and the rows $2^h + u$, where $0 \leq u \leq 2^h - 1$, that consist of two copies of the row u separated by $2^h - 1 - u$ zeros. Suppose that the rows $1,2,3,\ldots,2^h,2^h + 1,\ldots,2^{h+1} - 1$ have an even number of 1's and, at least, two 1's.

Now let's show, by induction, that this is valid for $r+1 = h+4 = (h+1)+3$. So, for $r+1$, we have the property 3) given by the rows $2^{h+1} + u$, where $0 \leq u \leq 2^{h+1} - 1$, that consist of two copies of the row u separated by $2^{h+1} - 1 - u$ zeros and we have the rows $1,2,3,\ldots,2^{h+1} - 1, 2^{h+1}, 2^{h+1} + 1,\ldots,2^{h+2} - 1$ that generate the code C_1 related to $r+1$.

But, by hypothesis of induction, we have that the rows $1,2,3,\ldots,2^h,2^h + 1,\ldots,2^{h+1} - 1$ have an even number of 1's and, at least, two 1's and since the rows $2^{h+1} + u$, where $0 \leq u \leq 2^{h+1} - 1$, consist of two copies of the row u separated by $2^{h+1} - 1 - u$ zeros, it follows that the rows $1,2,3,\ldots,2^{h+1} - 1, 2^{h+1}, 2^{h+1} + 1,\ldots,2^{h+2} - 1$ have an even number of 1's and, at least, two 1's (row 2^{h+1}).

Then we have proved, by induction, that d_k is even and $d_k \geq 2$. □

Since $\tau(\mathscr{J}^n) = \phi\mathbb{Z}[i]^n$, so the matrix $(M_{\mu'})^n$ generates the lattice $\phi\mathbb{Z}[i]^n$. But we know that the matrix $\phi I_{n\times n}$ also generates the lattice $\phi\mathbb{Z}[i]^n$, where $I_{n\times n}$ is the $n\times n$ identity matrix.

Therefore we can conclude that the matrices $(M_{\mu'})^n$ and $\phi I_{n\times n}$ are equivalent. Hence, using this fact, the following proposition gives us the extension by periodicity of the lattice partition chain for the positive positions, that is, $k \geq 0$:

Proposition 32. *For $k = n\alpha + j$, where $\alpha \in \mathbb{N}$ and $0 \leq j \leq n-1$, we have that $M_{\mu'(n\alpha+j)} = (M_{\mu'})^{k=(n\alpha+j)}$ is a generator matrix of the lattice $\phi^\alpha\Lambda_j$ seen as a $\mathbb{Z}[i]$-lattice, where Λ_j is the lattice found previously in this section, by the construction A, related to the position k compared to the $\mathbb{Z}[i]^n$-lattice.*

Proof. By previously, we have found the lattices Λ_j, where $0 \leq j \leq n-1$ and Λ_j is the lattice related to the position k, and we have that $M_{\mu' j} = (M_{\mu'})^j$ is a generator matrix of the lattice Λ_j. We know that the matrices $(M_{\mu'})^n$ and $\phi I_{n\times n}$ are equivalent.

For $k = n$, the matrix $(M_{\mu'})^n$ generates the lattice $\phi\mathbb{Z}[i]^n$; for $k = n + j$, we have $M_{\mu'(n+j)} = (M_{\mu'})^{(n+j)} = ((M_{\mu'})^n)(M_{\mu'})^j = \phi(M_{\mu'})^j$ as being a generator matrix of the lattice $\phi\Lambda_j$ and for $k = 2n + j$, we have $M_{\mu'(2n+j)} = (M_{\mu'})^{(2n+j)} = ((M_{\mu'})^{2n})(M_{\mu'})^j = \phi^2(M_{\mu'})^j = 2(M_{\mu'})^j$ as being a generator matrix of the lattice $2\Lambda_j$, since the matrices $(M_{\mu'})^n$ and $\phi I_{n\times n}$ are equivalent.

So let's suppose, by hypothesis of induction, that $(M_{\mu'})^{n\alpha+j}$, $\alpha \in \mathbb{N}$ and $0 \leq j \leq n-1$, is a generator matrix of the lattice $\phi^\alpha\Lambda_j$.

We will show, for $k = n(\alpha+1) + j$, that the lattice $\phi^{\alpha+1}\Lambda_j$ has a generator matrix as being the matrix $(M_{\mu'})^{(n(\alpha+1)+j)}$. In fact, $(M_{\mu'})^{n(\alpha+1)+j} = ((M_{\mu'})^n)((M_{\mu'})^{(n\alpha+j)})$, using the hypothesis of induction and the fact that $\phi I_{n\times n}$ and $(M_{\mu'})^n$ are equivalent matrices, we have $(M_{\mu'})^{n(\alpha+1)+j}$ as a generator matrix of the lattice $\phi^{\alpha+1}\Lambda_j$.

Therefore we showed that for $k = n\alpha + j$, $\alpha \in \mathbb{N}$ and $0 \leq j \leq n-1$, the matrix $(M_{\mu'})^{n\alpha+j}$ is a generator matrix of the lattice $\phi^\alpha\Lambda_j$.

But if α is even, we have $\alpha = 2\beta$, where $\beta \in \mathbb{N}$. Then $\phi^\alpha\Lambda_j = 2^{\alpha/2}\Lambda_j$, for $\alpha \neq 0$, and when $\alpha = 0$ we have the lattice Λ_j.

Now, if α is odd, we have $\alpha = 2\beta + 1$, where $\beta \in \mathbb{N}$, then $\phi^\alpha\Lambda_j = 2^{(\alpha-1)/2}\phi\Lambda_j$. □

And now the following proposition gives us the extension by periodicity of the lattice partition chain for the negative positions, that is, $k \leq -1$:

Proposition 33. *For all $k \in \mathbb{N}^*$, we have $\tau(\mathscr{J}^{-k}) = \tau(\mathscr{J}^k)^*$, where $\tau(\mathscr{J}^k)^*$ indicates the dual lattice of $\tau(\mathscr{J}^k)$.*

Proof. Let $\overrightarrow{x}$ and $\overrightarrow{y}$ be arbitrary elements of $\tau(\mathscr{J}^k)$ and $\tau(\mathscr{J}^{-k})$, respectively, where $k \in \mathbb{N}^*$. Therefore we have

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{\mathbb{L}/\mathbb{Q}(i)}(x \cdot y),$$

where $x \in \mathscr{J}^k$ and $y \in \mathscr{J}^{-k}$, then $x = (1+\beta)^k x_0$, with $x_0 \in O_{\mathbb{L}}$, and $y = (1+\beta)^{-k} y_0$, with $y_0 \in O_{\mathbb{L}}$.

It is easy to see that

$$Tr_{\mathbb{L}/\mathbb{Q}(i)}(x \cdot y) = \sum_{i=1}^{n} \tau_i(x \cdot y) = \sum_{i=1}^{n} \tau_i(x)\tau_i(y) = \sum_{i=1}^{n} \tau_i(x_0)\tau_i(y_0) = Tr_{\mathbb{L}/\mathbb{Q}(i)}(x_0 \cdot y_0).$$

We have that $Tr_{\mathbb{L}/\mathbb{Q}(i)}(x_0 \cdot y_0) \in \mathbb{Z} \subset \mathbb{Z}[i]$, where the Galois group of the field extension $[\mathbb{L}/\mathbb{Q}(i)]$ is given by $\{\tau_1, \tau_2, \ldots, \tau_n\} = \langle \tau' \rangle$, with $\tau_i : \mathbb{L} \to \mathbb{L}$, for $i = 1, 2, \ldots, n$, and $\tau' = \tau_i$, for some $i = 1, 2, \ldots, n$. So

$$\langle \overrightarrow{x}, \overrightarrow{y} \rangle = Tr_{\mathbb{L}/\mathbb{Q}(i)}(x \cdot y) \in \mathbb{Z}[i].$$

Then $\tau(\mathscr{J}^{-k}) \subset \tau(\mathscr{J}^k)^*$, for all $k \in \mathbb{N}^*$. We also have that

$$Vol[\tau(\mathscr{J}^k)^*] = \frac{1}{Vol[\tau(\mathscr{J}^k)]} = Vol[\tau(\mathscr{J}^{-k})]. \tag{57}$$

However the index $|\tau(\mathscr{J}^k)^*/\tau(\mathscr{J}^{-k})|$ is equal to 1 and so $\tau(\mathscr{J}^{-k}) = \tau(\mathscr{J}^k)^*$. □

So, in this section, we have constructed a nested lattice partition chain related to any dimension $n = 2^{r-2}$, with $r \geq 3$. Then, for the complex case, we have the generalization to obtain a nested lattice partition chain in order to quantize the channel coefficients.

6 THE REAL CASE FOR THE CONSTRUCTION OF NESTED LATTICES FROM IDEALS FOR CHANNEL APPROXIMATION

6.1 Introduction

By (NAZER; GASTPAR, 2011) we know that the *compute-and-forward* strategy enables relays to decode linear equations of the transmitted messages using the noisy linear combinations provided by the channel and we have an equivalent channel induced by the modulo-Λ transformation. In this "virtual" channel model each relay observes a $\mathbb{Z}[i]$-combination $\sum a_{ml}t_l$ of the lattice points corrupted by effective noise $z_{eq,m}$, that is,

$$y_m = \sum_{l=1}^{L} a_{ml}t_l + z_{eq,m}. \tag{58}$$

In this chapter, we will suppose that our interference channel is real-valued, specifically $a_{ml} \in \mathbb{R}$, and in order to realize interference alignment onto a lattice, we need to quantize the channel coefficients a_{ml}. We are going to describe a way to find a nested lattice partition chain, for any dimension $n = 2^{r-2}$, where $r \geq 3$, in order to quantize the channel coefficients. For that, we will make use of the maximal real subfield K of $L = \mathbb{Q}(\xi_{2^r})$, where $r \geq 3$, $\xi = \xi_{2^r}$ is the 2^r-th root of unity and $K = \mathbb{Q}(\theta)$, with $\theta = \xi + \xi^{-1}$.

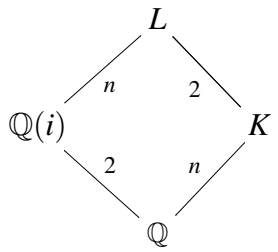
We also have that the coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself. Specifically, relay m only needs to know a_{ml}. Each transmitter only needs to know the desired message rate, not the realization of the channel.

6.2 Quantization of the Channel Gains

As described in section 6.1, suppose that our interference channel is real-valued, specifically $a_{ml} \in \mathbb{R}$. We suppose that all lattices used by the legitimate user and the interferers are one of a certain lattice partition chain and extended by periodicity. Now the idea we want to develop is that the effect of a channel gain on a given user is to shift the lattice used by the user either to the left, if its channel gain is smaller than 1, or to the right, if it is larger than 1. It is very important that the channel gain does not remove the lattice from the initial chain of nested lattices.

In this section we will consider n-dimensional real-valued vectors, where $n = 2^{r-2}$ and $r \geq 3$. Now we write, for a given user, how its codeword can be transformed so that we can perform the channel quantization. We will make use of the maximal real subfield K of $L = \mathbb{Q}(\xi_{2^r})$, where $r \geq 3$, $\xi = \xi_{2^r}$ is the 2^r-th root of unity and $K = \mathbb{Q}(\theta)$, with $\theta = \xi + \xi^{-1}$.

So we will consider the following Galois extensions, where $r \geq 3$:



(59)

Let $\xi = \xi_{2^r}$ be a 2^r-th root of unity, where $r \geq 3$. Let $L = \mathbb{Q}(\xi) = K(i)$ and $K = \mathbb{Q}(\theta)$ be the maximal real subfield of L, where $\theta = \xi + \xi^{-1}$. By the theorem 10 in (ANDRADE; ALVES; BERTOLDI, 2006), we have that $[L : \mathbb{Q}] = 2^{r-1}$, $[K : \mathbb{Q}] = 2^{r-2} = n$, $O_K = \mathbb{Z}[\theta]$ is the ring of integers of K and $\{1, \xi + \xi^{-1}, \ldots, \xi^{n-1} + \xi^{-(n-1)}\}$ is an integral basis of O_K.

As $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{r-1}$, where ϕ is the Euler function, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, then we have $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{r-2} = n$.

Let $Gal(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be the Galois group of K over $\mathbb{Q}$ ((ANDRADE; ALVES; BERTOLDI, 2006), pg. 6).

Let's find an ideal of norm equal to 2, that is, we will find an element of O_K with absolute algebraic norm equal to 2. In fact,

$$2 = N_{L/\mathbb{Q}}(1+\xi) = N_{K/\mathbb{Q}}(N_{L/K}(1+\xi)) =$$

$$= N_{K/\mathbb{Q}}(1+\xi^{-1}+\xi+1) = N_{K/\mathbb{Q}}(2+2cos(\pi/2^{(r-1)})).$$

Observe that $\xi + \xi^{-1} = \theta = 2cos(\pi/2^{(r-1)})$, then $N_{K/\mathbb{Q}}(2+\theta) = 2$. So

$$N_{K/\mathbb{Q}}(p) = 2, \text{ where } p = (2+\theta) \in O_K.$$

Therefore $\Im = \langle p \rangle = \langle 2+\theta \rangle = pO_K$ is a principal ideal of norm 2. By (ANDRADE; ALVES; BERTOLDI, 2006), pg. 3, we have that

$$R^T = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(\alpha_1) & \cdots & \sqrt{\sigma_1(\alpha)}\sigma_1(\alpha_n) \\ \sqrt{\sigma_2(\alpha)}\sigma_2(\alpha_1) & \cdots & \sqrt{\sigma_2(\alpha)}\sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sqrt{\sigma_n(\alpha)}\sigma_n(\alpha_1) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(\alpha_n) \end{pmatrix} \tag{60}$$

is a generator matrix of the lattice $\Lambda = \{x = M\lambda \mid \lambda \in \mathbb{Z}^n\}$, where $\alpha \in K$ is totally positive, that is, $\sigma_i(\alpha) > 0$, for all $i = 1, 2, \ldots, n$, and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of A over $\mathbb{Z}$, where $A \subseteq O_K$ is an ideal.

In this case we have that the Gram matrix $(R^T)^T R^T = RR^T$ coincides with the trace form $(Tr(\alpha\alpha_i\alpha_j))_{i,j=1}^n$, where T denotes the transposition.

We know that $\{1, \xi + \xi^{-1}, \ldots, \xi^{n-1} + \xi^{-(n-1)}\} = \{e_0, e_1, \ldots, e_{(n-1)}\}$ is an integral basis of O_K. Observe in (ANDRADE; ALVES; BERTOLDI, 2006), pg. 6, that T is a basis transformation matrix from $\{e_i\}_{i=0}^{n-1}$ to $\{f_i\}_{i=0}^{n-1}$, where $f_i = -\sum_{j=0}^{i} e_j$, for all $i = 0, 1, 2, \ldots, n-1$, and $T = T^T$. So $\{f_0, f_1, \ldots, f_{n-1}\}$ is another basis ($\mathbb{Z}$-basis) of O_K.

Finally the generator matrix of the rotated $\mathbb{Z}^n$-lattice is given by ((ANDRADE; ALVES; BERTOLDI, 2006), pg. 7)

$$R = \frac{1}{\sqrt{2^{r-1}}} TMA. \tag{61}$$

But in this work the columns of a matrix will generate the $\mathbb{Z}^n$-lattice, then $M_0 = R^T$ generates the rotated $\mathbb{Z}^n$-lattice Λ_0. So $\Lambda_0 = \{x = M_0\lambda \mid \lambda \in \mathbb{Z}^n\} \simeq \mathbb{Z}^n$ and $M_0 = \frac{1}{\sqrt{2^{r-1}}} AM^T T = \frac{1}{\sqrt{2^{r-1}}} AM'$ ($M' = M^T T$), where

$$M = \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}, \tag{62}$$

$$A = diag(\sqrt{\sigma_k(\alpha)})_{k=1}^n, \text{ where } \alpha = 2 - \theta, \text{ and} \tag{63}$$

$$T = \begin{pmatrix} -1 & -1 & -1 & \cdots & -1 \\ -1 & -1 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{64}$$

But $M' = M^T T$ can be directly calculated if we use the new basis $\{f_i\}_{i=0}^{n-1}$, that is,

$$M' = \begin{pmatrix} \sigma_1(f_0) & \cdots & \sigma_1(f_{n-1}) \\ \sigma_2(f_0) & \cdots & \sigma_2(f_{n-1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(f_0) & \cdots & \sigma_n(f_{n-1}) \end{pmatrix}. \tag{65}$$

Observe, by (ANDRADE; ALVES; BERTOLDI, 2006), that $RR^T = I$, where I is the identity matrix. Then

$$M_0^T M_0 = (R^T)^T R^T = RR^T = I.$$

At the receiver, we suppose that we apply M_0 to the received vector of (71) to get

$$\bar{y}_m = M_0 y_m = \sum_{l=1}^{L} a_{ml} M_0 t_l + M_0 z_{eq,m}. \tag{66}$$

As $z_{eq,m}$ is i.i.d. circularly symmetric complex Gaussian noise and M_0 is orthogonal, then the noise in (66) is also i.i.d. circularly symmetric complex Gaussian. Now let's take a look at the vectors of the form $a_{ml}M_0t_l$. For sake of simplicity of notations, we denote it by

$$\bar{x} = h \cdot M_0 \cdot x, \tag{67}$$

where $x = t_l$ is the lattice point transmitted by the considered user and $h = a_{ml}$ is the channel coefficient. We can rewrite it now as

$$\begin{pmatrix} h & 0 & \cdots & 0 \\ 0 & h & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h \end{pmatrix} \cdot U \cdot x = H \cdot U \cdot x. \tag{68}$$

As in the complex case, we have that $\Im^k$, $k \in \mathbb{Z}$, is an ideal of O_K generated by p^k, with $p = 2 + \theta$. So $\Im^k = p^k O_K$.

Analogously to the complex case, if $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis of O_K, then

$$\{p^k\alpha_1, p^k\alpha_2, \ldots, p^k\alpha_n\}$$

is a $\mathbb{Z}$-basis of $\Im^k = \langle p^k \rangle = p^k O_K$, since the set of invertible fractional ideals form an abelian group related to the product of ideals.

We know, by (ANDRADE; ALVES; BERTOLDI, 2006), that $\{f_0, f_1, \ldots, f_{n-1}\}$ is a $\mathbb{Z}$-basis of O_K used to find the rotated $\mathbb{Z}^n$-lattice Λ_0. So, by previously, it follows that $\{p^k f_0, p^k f_1, \ldots, p^k f_{n-1}\}$ is a $\mathbb{Z}$-basis of $\Im^k = p^k O_K$. Then the generator matrix M_k of the lattice $\Lambda_k = \{x = (M_k)\lambda \mid \lambda \in \mathbb{Z}^n\}$ is given by

$$M_k = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(p^k f_0) & \cdots & \sqrt{\sigma_1(\alpha)}\sigma_1(p^k f_{n-1}) \\ \sqrt{\sigma_2(\alpha)}\sigma_2(p^k f_0) & \cdots & \sqrt{\sigma_2(\alpha)}\sigma_2(p^k f_{n-1}) \\ \vdots & \ddots & \vdots \\ \sqrt{\sigma_n(\alpha)}\sigma_n(p^k f_0) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(p^k f_{n-1}) \end{pmatrix} =$$

$$= A \cdot \begin{pmatrix} \sigma_1(p^k) & 0 & \cdots & 0 \\ 0 & \sigma_2(p^k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(p^k) \end{pmatrix} \cdot M' = AA'M^T T, \tag{69}$$

where $A' = diag(\sigma_i(p^k))_{i=1}^n$.

As A and A' are diagonal matrices, we have $AA' = A'A$. Then $M_k = A'(AM^T T) = A'(AM')$.

So we can conclude, as in the complex case, that the matrix H can be approximated by

$$A' = \begin{pmatrix} \sigma_1(p^k) & 0 & \cdots & 0 \\ 0 & \sigma_2(p^k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(p^k) \end{pmatrix}. \tag{70}$$

In the appendix C, we have a program that gives us, for each $r \geq 3$ (each $n = 2^{r-2}$, where $r \geq 3$), a nested lattice partition chain, which is extended by periodicity so that it is a doubly infinite chain.

So, in this chapter, we have constructed a nested lattice partition chain related to any $r \geq 3$ (any $n = 2^{r-2}$, where $r \geq 3$). Then, for the real case, we have the generalization to obtain a nested lattice partition chain in order to quantize the channel coefficients.

7 ESTIMATION WITH MINIMUM MEAN SQUARE ERROR

7.1 Introduction

The requirements for new wireless communication systems are becoming more aggressive due to demand for transmission rates increasingly higher. Furthermore, the density of the communication systems is increasing, causing a strong presence of interference in wireless communication networks. Thus, the interference becomes increasingly a limiting factor of the performance of these systems. Therefore, a large amount of research has been made to mitigate the effects of the interference in these systems.

The Interference Alignment (IA) is a new scheme used in wireless communication networks, which allows a linear increase of the capacity with the increased number of users. Another line of research is the development of algorithms that, in addition to finding the solution of the alignment, also attempt to maximize the total capacity of the network (SCHMIDT et al., 2009; SHEN; MADSEN; VIDAL, 2008; PETERS; JUNIOR, 2011). One of these algorithms is based on the MMSE criterion.

In this chapter, one key step is the introduction of an error criterion that measures, in a probabilistic sense, the error between the desired quantity and our estimate of it. So we will focus on choosing our estimate to minimize the expected or mean value of the square of the error, referred to as a minimum mean-square-error (MMSE) criterion.

As we discussed in chapter 4, in (NAZER; GASTPAR, 2011) we have an equivalent channel induced by the modulo-Λ transformation. In this “virtual" channel model each relay observes a $\mathbb{Z}[i]$-combination $\sum a_{ml}t_l$ of the lattice points corrupted by effective noise $z_{eq,m}$, that is,

$$y_m = \sum_{l=1}^{L} a_{ml}t_l + z_{eq,m}. \tag{71}$$

We also have that the coding scheme only requires that each relay knows the channel coefficients from each transmitter to itself. Specifically, relay m only needs to know a_{ml}. Each transmitter only needs to know the desired message rate, not the realization of the channel.

In chapter 6, we supposed that our interference channel is real-valued, specifically $a_{ml} \in \mathbb{R}$, and in order to realize interference alignment onto a lattice, we quantized the channel coefficients a_{ml}.

Thus, in this chapter, for the case $a_{ml} \in \mathbb{R}$ and $n = 1$ or $n = 2^{r-2}$ ($r \geq 3$), we will minimize

the expected or mean value of the square of the error, referred to as a minimum mean-square-error (MMSE) criterion.

We can note that the following theory is analogous to the complex case. The following section presents the MMSE criterion for the 1-dimensional real case:

7.2 Estimation with Minimum Mean Square Error for the 1-Dimensional Real Case

This section presents the MMSE criterion for the 1-dimensional real case and it will be divided in two subsections. The first one will compute an expression for the mean-square-error (MSE) and, in the second one, we will obtain the MSE minimization.

7.2.1 Computing the mean-square-error (MSE)

In this section, we will compute for the 1-dimensional real case an expression for the mean-square-error (MSE). For the calculations, we will fix the receiver and denote it by R. So, in this case, we can write the received vector at R as the equation (71). For sake of simplicity of notations, we will denote the vectors y_m, $a_{ml}t_l$ and $z_{eq,m}$ by $\overrightarrow{y}$, $h_i\overrightarrow{x}_i$ and $\overrightarrow{z}$, respectively. Thus, equation (71) becomes

$$\overrightarrow{y} = \sum_{i=i}^{k} h_i \overrightarrow{x}_i + \overrightarrow{z}. \tag{72}$$

In the 1-dimensional real case suppose that h_i, $\overrightarrow{x}_i$ and $\overrightarrow{z}$ are real. Then the equation (72) becomes

$$y = \sum_{i=i}^{k} h_i x_i + z. \tag{73}$$

The Minimum Mean Square Error (MMSE) approach tries to find a coefficient β wich minimizes the criterion $E[\upsilon^2]$, where

$$E[\upsilon^2] = E\left[\sum_{i=1}^{k} (\beta h_i - a_i)^2 x_i^2 + \beta^2 z^2\right],$$

with $a_i \in \mathbb{Z}$, for $i = 1, \ldots, k$. In fact:

Let $a_i \in \mathbb{Z}$, where $i = 1, \ldots, k$. From equation (73) we have

$$\beta y = \sum_{i=1}^{k} \beta h_i x_i + \beta z = \sum_{i=1}^{k} a_i x_i + \sum_{i=1}^{k} (\beta h_i - a_i) x_i + \beta z,$$

where $\upsilon = \sum_{i=1}^{k}(\beta h_i - a_i)x_i + \beta z$ is the noise term. So

$$E[\upsilon^2] = E\left[\left(\sum_{i=1}^{k}(\beta h_i - a_i)x_i + \beta z\right)^2\right].$$

Since the Mean Square Area is equal to zero and the variables x_i and z, for $i = 1,\ldots,k$, are not correlated, we have

$$E[\upsilon^2] = E\left[\sum_{i=1}^{k}(\beta h_i - a_i)^2 x_i^2 + \beta^2 z^2\right] = \sum_{i=1}^{k}(\beta h_i - a_i)^2 E[x_i^2] + \beta^2 E[z^2].$$

Let $E[x_i^2] = p$, $E[z^2] = \sigma^2$ and $\rho = \frac{p}{\sigma^2}$, where ρ is the signal-to-noise ratio (SNR). Then

$$\frac{E[\upsilon^2]}{p} = \sum_{i=1}^{k}(\beta h_i - a_i)^2 + \beta^2\frac{1}{\rho} = \sum_{i=1}^{k}(\beta^2 h_i^2 + a_i^2 - 2\beta h_i a_i) + \beta^2\frac{1}{\rho} =$$

$$= \beta^2\left(\sum_{i=1}^{k} h_i^2 + \frac{1}{\rho}\right) - 2\beta\langle h,a\rangle + \| a \|^2 = \beta^2\left(\| h \|^2 + \frac{1}{\rho}\right) - 2\beta\langle h,a\rangle + \| a \|^2 .$$

So we have

$$\frac{E[\upsilon^2]}{p} = \beta^2\left(\| h \|^2 + \frac{1}{\rho}\right) - 2\beta\langle h,a\rangle + \| a \|^2 =$$

$$= \left(\| h \|^2 + \frac{1}{\rho}\right)\left[\beta^2 - \frac{2\beta\langle h,a\rangle}{\| h \|^2 + \frac{1}{\rho}} + \frac{\| a \|^2}{\| h \|^2 + \frac{1}{\rho}}\right] =$$

$$= \left(\| h \|^2 + \frac{1}{\rho}\right)\left[\left(\beta - \frac{\langle h,a\rangle}{\| h \|^2 + \frac{1}{\rho}}\right)^2 + \frac{\| a \|^2}{\| h \|^2 + \frac{1}{\rho}} - \frac{\langle h,a\rangle^2}{\left(\| h \|^2 + \frac{1}{\rho}\right)^2}\right].$$

Therefore $\beta = \frac{\langle h,a\rangle}{\|h\|^2 + \frac{1}{\rho}}$ is the coefficient wich minimizes the criterion $E[\upsilon^2]$. Then we have that the MSE is given by

$$p\left[\| a \|^2 - \frac{\langle h,a\rangle^2}{\| h \|^2 + \frac{1}{\rho}}\right] = p\left[\frac{1}{\| h \|^2 + \frac{1}{\rho}}\left(\| a \|^2\left(\| h \|^2 + \frac{1}{\rho}\right) - \langle h,a\rangle^2\right)\right].$$

To find the MMSE solution we have to minimize the following expression:

$$\| a \|^2\left(\| h \|^2 + \frac{1}{\rho}\right) - \langle h,a\rangle^2 . \tag{74}$$

So we have got an expression for the mean-square-error (MSE) and, minimizing the equation (74), we obtain the MMSE solution. Then the following section shows us how we can obtain the MMSE solution:

7.2.2 The MSE minimization

The goal of this section is to minimize the equation (74) to obtain the MMSE solution. Observe that the equation (74) is a quadratic form whose variables are a_i, with $i = 1, \ldots, k$.

So

$$F(a) = \| a \|^2 \left(\| h \|^2 + \frac{1}{\rho} \right) - \langle h, a \rangle^2 = a^T Q a = a^T M^T M a = b^T b,$$

where T denotes the transpose of a matrix, Q is the $k \times k$ gram matrix of the lattice Λ generated by the $k \times k$ matrix M and b is a lattice point, where $b = Ma$. We have that Q is a symmetric matrix and $F(a)$ is a positive definite quadratic form.

However we have to find $a = (a_1, a_2, \ldots, a_k) \in (\mathbb{Z}^k - \{0\})$ such that a is the vector that minimizes $F(a)$. So first we are going to find the matrix Q:

$$F(a) = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix} \cdot \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1k} \\ q_{21} & q_{22} & \cdots & q_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ q_{k1} & q_{k2} & \cdots & q_{kk} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} =$$

$$= \begin{pmatrix} \sum_{i=1}^k a_i q_{i1} & \sum_{i=1}^k a_i q_{i2} & \cdots & \sum_{i=1}^k a_i q_{ik} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} =$$

$$= \sum_{i=1}^k a_1 a_i q_{i1} + \sum_{i=1}^k a_2 a_i q_{i2} + \cdots + \sum_{i=1}^k a_k a_i q_{ik} =$$

$$= \sum_{i=1}^k \left(a_1 a_i q_{i1} + a_2 a_i q_{i2} + \cdots + a_k a_i q_{ik} \right).$$

Observe that $F(a)$ is also given by the equation (74), that is,

$$F(a) = \| a \|^2 \left(\| h \|^2 + \frac{1}{\rho} \right) - \langle h, a \rangle^2 = (I) + (II),$$

where $(I) = \| a \|^2 \left(\| h \|^2 + \frac{1}{\rho} \right)$ and $(II) = - \langle h, a \rangle^2$.

Then we have

$$(I) = \| a \|^2 \left(\| h \|^2 + \frac{1}{\rho} \right) =$$

$$= a_1^2 \left(\| h \|^2 + \frac{1}{\rho} \right) + a_2^2 \left(\| h \|^2 + \frac{1}{\rho} \right) + \cdots + a_k^2 \left(\| h \|^2 + \frac{1}{\rho} \right)$$

and

$$(II) = - \langle h, a \rangle^2 = -(h_1 a_1 + h_2 a_2 + \cdots + h_k a_k)^2 = -(h_1^2 a_1^2 + a_1 a_2 h_1 h_2 + a_1 a_3 h_1 h_3 + \cdots + a_1 a_k h_1 h_k + a_2 a_1 h_2 h_1 + a_2^2 h_2^2 + a_2 a_3 h_2 h_3 + a_2 a_4 h_2 h_4 + \cdots + a_2 a_k h_2 h_k + a_3 a_1 h_3 h_1 + a_3 a_2 h_3 h_2 + a_3^2 h_3^2 + a_3 a_4 h_3 h_4 + \cdots + a_3 a_k h_3 h_k + a_4 a_1 h_4 h_1 + a_4 a_2 h_4 h_2 + a_4 a_3 h_4 h_3 + a_4^2 h_4^2 + \cdots + a_4 a_k h_4 h_k + \cdots + a_k a_1 h_k h_1 + a_k a_2 h_k h_2 + a_k a_3 h_k h_3 + a_k a_4 h_k h_4 + \cdots + a_k^2 h_k^2).$$

Therefore since $F(a) = \| a \|^2 \left(\| h \|^2 + \frac{1}{\rho} \right) - \langle h, a \rangle^2 = a^T Q a$ we have that the symmetric matrix Q, where

$$Q = \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1k} \\ q_{21} & q_{22} & \cdots & q_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ q_{k1} & q_{k2} & \cdots & q_{kk} \end{pmatrix},$$

is given by: $q_{ij} = \left(\| h \|^2 + \frac{1}{\rho} \right) - h_i^2$, for $i = j$; $q_{ij} = -h_i h_j$, for $i < j$; and $q_{ij} = q_{ji}$, for $i > j$.

To find $a = (a_1, a_2, \ldots, a_k) \in (\mathbb{Z}^k - \{0\})$ such that a is the vector that minimizes $F(a)$, we have to find $b \in \Lambda$ such that b is the shortest lattice point, that is, the closest to the origin. So we have

$$min_{a \in (\mathbb{Z}^k - \{0\})} F(a) = min_{b \in \Lambda} \| b \|^2 .$$

We have $Q = M^T M$ and M can be decomposed as $M = V D_1 U^T$, where V and U are $k \times k$ orthogonal matrices and D_1 is a $k \times k$ diagonal matrix whose diagonal entries are the singular values of M.

By taking $J = U^T$ and $W = V^T$ and the fact that U and V are orthogonal matrices, we have that J and W are also $k \times k$ orthogonal matrices and $M = W^T D_1 J$. Then

$$Q = M^T M = (J^T D_1 W)(W^T D_1 J) = J^T D_1^2 J, \text{ since } W \text{ is an orthogonal matrix.}$$

So we have $Q = J^T D_1^2 J$, where J is an orthogonal matrix and D_1^2 is a $k \times k$ diagonal matrix whose diagonal entries are the eigenvalues of Q.

However $Q = J^T D_1^2 J = J^T D_1^T D_1 J = (D_1 J)^T (D_1 J)$, since D_1 is a diagonal matrix. Then we can take the matrix M as $M = D_1 J$, where J is an orthogonal matrix.

The columns of M form a basis for the lattice Λ. Through the QR (Gram-Schmidt) decomposition we have $M = OR$, where O is a $k \times k$ orthogonal matrix and R is a $k \times k$ upper triangular matrix. If the matrix M is non-singular this factorization is unique. So we have

$$min_{a \in (\mathbb{Z}^k - \{0\})} F(a) = min_{a \in (\mathbb{Z}^k - \{0\})} a^T Qa = min_{a \in (\mathbb{Z}^k - \{0\})} a^T M^T Ma =$$

$$= min_{a \in (\mathbb{Z}^k - \{0\})} a^T R^T Ra,$$

since O is an orthogonal matrix.

Then we use the Fincke-Pohst Algorithm, that is, given a constant $C > 0$, find all $x \in \mathbb{Z}^k$ such that $F(a) < C$. The algorithm runs in exponential time and works in many practical situations. It makes use of LLL as a subalgorithm.

The best way to determine with certainty the shortest non-zero vectors in the lattice is to let C be the norm of the shortest basis vector in a reduced basis (found using LLL) and then, by using the Fincke-Pohst Algorithm, we search for the shortest vectors in the lattice.

After finding these shortest vectors in the lattice, by testing each one, we can find the shortest one.

Thus, we described a way to find the MMSE solution. The following section presents the MMSE criterion for the n-dimensional real case, where $n = 2^{r-2}$ and $r \geq 3$:

7.3 Estimation with Minimum Mean Square Error for the n-Dimensional Real Case

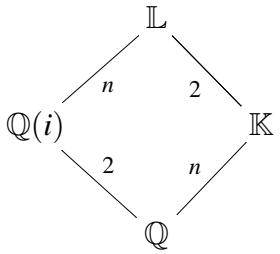
This section presents the MMSE criterion for the n-dimensional real case and it will be divided in two subsections. The first one will compute an expression for the mean-square-error (MSE) and, in the second one, we will obtain the MSE minimization.

In chapter 6, we supposed that our interference channel is real-valued, specifically $a_{ml} \in \mathbb{R}$, and in order to realize interference alignment onto a lattice, we quantized the channel coefficients a_{ml}.

Thus, in this section, for the case $a_{ml} \in \mathbb{R}$ and $n = 2^{r-2}$, where $r \geq 3$, we will minimize the expected or mean value of the square of the error, referred to as a minimum mean-square-error (MMSE) criterion.

7.3.1 Computing the mean-square-error (MSE)

In this section, we will compute for the n-dimensional real case an expression for the mean-square-error (MSE). So we will consider the following Galois extensions:



(75)

Let $\xi = \xi_{2^r}$ be a 2^r-th root of unity, where $r \geq 3$. Let $\mathbb{L} = \mathbb{Q}(\xi) = \mathbb{K}(i)$ and $\mathbb{K} = \mathbb{Q}(\theta)$ the maximal real subfield of $\mathbb{L}$, where $\theta = \xi + \xi^{-1}$. By theorem 10 ((ANDRADE; ALVES; BERTOLDI, 2006)) we have that $[\mathbb{L} : \mathbb{Q}] = 2^{r-1}$, $[\mathbb{K} : \mathbb{Q}] = 2^{r-2} = n$, $O_{\mathbb{K}} = \mathbb{Z}[\theta]$ is the ring of integers of $\mathbb{K}$ and $\{1, \xi + \xi^{-1}, \ldots, \xi^{n-1} + \xi^{-(n-1)}\}$ is an integral basis of $O_{\mathbb{K}}$.

As $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{r-1}$, where ϕ is the Euler function, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, then we have $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{r-2} = n$.

Let $Gal(\mathbb{K}/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be the Galois group of $\mathbb{K}$ over $\mathbb{Q}$ ((ANDRADE; ALVES; BERTOLDI, 2006), pg. 6), $\overrightarrow{x}_i = \Omega \overrightarrow{u}_i$ and $v_i \in O_{\mathbb{K}} = \mathbb{Z}[\theta]$, for $i = 1, \ldots, k$, where $\overrightarrow{u}_i \in \mathbb{Z}^n$ and $\Omega \in SO_n(\mathbb{R})$ is the canonical embedding.

As in section 7.2.1, for the calculations, we will fix the receiver and denote it by R. So, in this case, we can write the received vector at R as the equation

$$y_m = \sum_{l=1}^{L} a_{ml} I t_l + z_{eq,m}, \tag{76}$$

where I indicates the identity matrix.

For sake of simplicity of notations, we will denote y_m, $a_{ml} I t_l$ and $z_{eq,m}$ by $\overrightarrow{y}$, $h_i I \overrightarrow{x}_i$ and $\overrightarrow{z}$, respectively. Thus, equation (76) becomes

$$\overrightarrow{y} = \sum_{i=i}^{k} h_i I \overrightarrow{x}_i + \overrightarrow{z}, \tag{77}$$

where $h_i \in \mathbb{R}$ and the $n \times n$ matrix

$$\begin{pmatrix} h_i & 0 & \cdots & 0 \\ 0 & h_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_i \end{pmatrix}$$

is approximated by the $n \times n$ matrix V_i given by

$$\begin{pmatrix} \sigma_1(v_i) & 0 & \cdots & 0 \\ 0 & \sigma_2(v_i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(v_i) \end{pmatrix},$$

where $i = 1, \ldots, k$.

The Minimum Mean Square Error (MMSE) approach tries to find a $n \times n$ matrix B wich minimizes the criterion $E[\overrightarrow{v}^T \overrightarrow{v}]$, where

$$\overrightarrow{v} = \sum_{i=1}^{k} \left(h_i \left(\Omega^T B \Omega\right) - T_i\right) \overrightarrow{u_i} + \Omega^T B \overrightarrow{z},$$

$V_i\Omega = \Omega T_i$, for $i = 1, \ldots, k$, with $T_i \in \mathbb{M}_n(\mathbb{Z})$, and T denotes the transpose of a matrix. In fact:

From equation (77), we have

$$B\overrightarrow{y} = \sum_{i=1}^{k} B(h_i I)\overrightarrow{x}_i + B\overrightarrow{z} = \sum_{i=1}^{k} V_i \overrightarrow{x}_i + \sum_{i=1}^{k} (B(h_i I) - V_i)\overrightarrow{x}_i + B\overrightarrow{z},$$

where $V_i \overrightarrow{x}_i = V_i(\Omega \overrightarrow{u}_i) = \Omega(T_i \overrightarrow{u}_i)$, $T_i \in \mathbb{M}_n(\mathbb{Z})$ and $T_i \overrightarrow{u}_i = \overrightarrow{w}_i$. So

$$\sum_{i=1}^{k} V_i \overrightarrow{x}_i = \sum_{i=1}^{k} \Omega \overrightarrow{w}_i = \Omega \sum_{i=1}^{k} \overrightarrow{w}_i.$$

We also have that

$$\sum_{i=1}^{k} (B(h_i I) - V_i)\overrightarrow{x}_i = \sum_{i=1}^{k} ((\Omega\Omega^T)h_i B - V_i)\overrightarrow{x}_i = \sum_{i=1}^{k} ((\Omega\Omega^T)h_i B)\overrightarrow{x}_i - \sum_{i=1}^{k} V_i \overrightarrow{x}_i =$$

$$= \sum_{i=1}^{k} (\Omega\Omega^T)h_i B(\Omega\Omega^T)\overrightarrow{x}_i - \sum_{i=1}^{k} \Omega(T_i \overrightarrow{u}_i) = \sum_{i=1}^{k} (\Omega\Omega^T)h_i B\Omega \overrightarrow{u}_i - \sum_{i=1}^{k} \Omega(T_i \overrightarrow{u}_i) =$$

$$= \Omega \left(\sum_{i=1}^{k} (\Omega^T h_i B\Omega)\overrightarrow{u}_i \right) - \Omega \sum_{i=1}^{k} T_i \overrightarrow{u}_i = \Omega \sum_{i=1}^{k} (h_i(\Omega^T B\Omega) - T_i)\overrightarrow{u}_i$$

and $B\overrightarrow{z} = \Omega(\Omega^T B \overrightarrow{z})$.

Then we can conclude that

$$\overrightarrow{y}' = \Omega^T B \overrightarrow{y} = \sum_{i=1}^{k} T_i \overrightarrow{u}_i + \sum_{i=1}^{k} (h_i(\Omega^T B\Omega) - T_i)\overrightarrow{u}_i + \Omega^T B \overrightarrow{z},$$

where $\overrightarrow{v} = \sum_{i=1}^{k}(h_i(\Omega^T B\Omega) - T_i)\overrightarrow{u}_i + \Omega^T B\overrightarrow{z}$ is the noise term ($\overrightarrow{v}$ is a $n \times 1$ column vector). However

$$E[\overrightarrow{v}^T\overrightarrow{v}] = Tr(E[\overrightarrow{v}^T\overrightarrow{v}]) = E[Tr(\overrightarrow{v}^T\overrightarrow{v})] = E[Tr(\overrightarrow{v}\overrightarrow{v}^T)] = Tr(E[\overrightarrow{v}\overrightarrow{v}^T])$$

and

$$Tr(E[\overrightarrow{v}\overrightarrow{v}^T]) =$$

$$= Tr(E[(\sum_{i=1}^{k}(h_i(\Omega^T B\Omega) - T_i)\overrightarrow{u}_i + \Omega^T B\overrightarrow{z}) \cdot (\sum_{i=1}^{k}(h_i(\Omega^T B\Omega) - T_i)\overrightarrow{u}_i + \Omega^T B\overrightarrow{z})^T]).$$

Since the Mean Square Area is equal to zero and the variables $\overrightarrow{u}_i$ and $\overrightarrow{z}$, for $i = 1, \ldots, k$, are not correlated, we have

$$E[\overrightarrow{v}\overrightarrow{v}^T] = \sum_{i=1}^{k}(h_i(\Omega^T B\Omega) - T_i)E[\overrightarrow{u}_i\overrightarrow{u}_i^T](h_i(\Omega^T B^T\Omega) - T_i^T) +$$

$$+\Omega^T BE[\overrightarrow{z}\overrightarrow{z}^T]B^T\Omega.$$

Then we have

$$E[\overrightarrow{v}^T\overrightarrow{v}] = Tr(\sum_{i=1}^{k}(h_i(\Omega^T B\Omega) - T_i)E[\overrightarrow{u}_i\overrightarrow{u}_i^T](h_i(\Omega^T B^T\Omega) - T_i^T) +$$

$$+\Omega^T BE[\overrightarrow{z}\overrightarrow{z}^T]B^T\Omega).$$

Let $E[\overrightarrow{u}_i\overrightarrow{u}_i^T] = P$, for all $i = 1, \ldots, k$, $E[\overrightarrow{z}\overrightarrow{z}^T] = \sigma^2$ and $\rho = \frac{P}{\sigma^2}$, where ρ is the signal-to-noise ratio (SNR). Then

$$E[\overrightarrow{v}^T\overrightarrow{v}] = PTr(\sum_{i=1}^{k}(h_i(\Omega^T B\Omega) - T_i)(h_i(\Omega^T B^T\Omega) - T_i^T) +$$

$$+\frac{1}{\rho}\Omega^T BB^T\Omega) = PTr(\sum_{i=1}^{k}h_i^2(\Omega^T BB^T\Omega) -$$

$$-\sum_{i=1}^{k}h_i[(\Omega^T B\Omega)T_i^T + T_i(\Omega^T B^T\Omega)] +$$

$$+\sum_{i=1}^{k} T_i T_i^T + \frac{1}{\rho}\Omega^T BB^T\Omega).$$

Therefore we can conclude that

$$E[\overrightarrow{v}^T\overrightarrow{v}] = PTr((\|h\|^2+\frac{1}{\rho})\Omega^T BB^T\Omega -$$

$$-\sum_{i=1}^{k} h_i(\Omega^T B\Omega)T_i^T - \sum_{i=1}^{k} h_i T_i(\Omega^T B^T\Omega) + \sum_{i=1}^{k} T_i T_i^T).$$

Let $F=\Omega^T B\Omega$ ($F^T=\Omega^T B^T\Omega$) and $\gamma=(\|h\|^2+\frac{1}{\rho})$. So

$$E[\overrightarrow{v}^T\overrightarrow{v}] = P\gamma Tr(F\cdot F^T - \frac{1}{\gamma}F\sum_{i=1}^{k} h_i T_i^T -$$

$$-\frac{1}{\gamma}F^T\sum_{i=1}^{k} h_i T_i + \frac{1}{\gamma}\sum_{i=1}^{k} T_i T_i^T) = P\gamma Tr((F-\frac{1}{\gamma}\sum_{i=1}^{k} h_i T_i)(F-\frac{1}{\gamma}\sum_{i=1}^{k} h_i T_i)^T +$$

$$+\frac{1}{\gamma}\sum_{i=1}^{k} T_i T_i^T - \frac{1}{\gamma^2}(\sum_{i=1}^{k} h_i T_i)(\sum_{i=1}^{k} h_i T_i)^T).$$

Observe that $F=\frac{1}{\gamma}\sum_{i=1}^{k} h_i T_i$ minimizes the criterion $E[\overrightarrow{v}^T\overrightarrow{v}]$. Since $F=\Omega^T B\Omega$, it follows that

$$B\Omega = \frac{1}{\gamma}\Omega\sum_{i=1}^{k} h_i T_i \Leftrightarrow B = \frac{1}{\gamma}\Omega(\sum_{i=1}^{k} h_i T_i)\Omega^T = \frac{1}{\gamma}\sum_{i=1}^{k} h_i(\Omega T_i\Omega^T).$$

Then $B=\frac{1}{\gamma}\sum_{i=1}^{k} h_i(\Omega T_i\Omega^T)$ minimizes the criterion $E[\overrightarrow{v}^T\overrightarrow{v}]$ and we have that the MSE is given by

$$PTr(\sum_{i=1}^{k} T_i T_i^T - \frac{1}{\gamma}(\sum_{i=1}^{k} h_i T_i)(\sum_{i=1}^{k} h_i T_i)^T) =$$

$$= P(\sum_{i=1}^{k} Tr(T_i T_i^T) - \frac{1}{\gamma}\|\sum_{i=1}^{k} h_i T_i\|_F^2) = P(\sum_{i=1}^{k}\|T_i\|_F^2 - \frac{1}{\gamma}\|\sum_{i=1}^{k} h_i T_i\|_F^2), \tag{78}$$

with $\|A\|_F=\sqrt{Tr(AA^T)}$, where A is an $m\times n$ real matrix. This norm $\|\cdot\|_F$ is called *Frobenius norm*.

Since

$$\|T_i\|_F^2 = Tr(T_i T_i^T) = Tr(T_i T_i^T\Omega^T\Omega) = Tr(\Omega T_i T_i^T\Omega^T) =$$

$$= \sum_{j=1}^{n} \sigma_j(v_i)^2 = \sum_{j=1}^{n} \sigma_j(v_i^2) = Tr_{\mathbb{K}/\mathbb{Q}}(v_i^2)$$

and

$$\| \sum_{i=1}^{k} h_i T_i \|_F^2 = Tr((\sum_{i=1}^{k} h_i T_i)(\sum_{i=1}^{k} h_i T_i)^T) =$$

$$= Tr(\Omega(\sum_{i=1}^{k} h_i T_i)(\sum_{i=1}^{k} h_i T_i)^T \Omega^T) = Tr((\sum_{i=1}^{k} h_i \Omega T_i)(\sum_{i=1}^{k} h_i T_i^T \Omega^T)) =$$

$$= \sum_{i,j=1}^{k} h_i h_j Tr_{\mathbb{K}/\mathbb{Q}}(v_i v_j),$$

the MSE is given by

$$P(\sum_{i=1}^{k} Tr_{\mathbb{K}/\mathbb{Q}}(v_i^2) - \frac{1}{\gamma} \sum_{i,j=1}^{k} h_i h_j Tr_{\mathbb{K}/\mathbb{Q}}(v_i v_j)) =$$

$$= P\frac{1}{\gamma}(\gamma \sum_{i=1}^{k} Tr_{\mathbb{K}/\mathbb{Q}}(v_i^2) - \sum_{i,j=1}^{k} h_i h_j Tr_{\mathbb{K}/\mathbb{Q}}(v_i v_j)). \tag{79}$$

Thus, the following remark shows us, from equation (78), that we can obtain the MSE of the 1-dimensional real case:

Remark 7. *If we take $T_i = a_i \in \mathbb{Z}$, $\overrightarrow{u}_i$ and $\overrightarrow{z}$ 1-dimensional vectors and $h_i \in \mathbb{R}$, for $i = 1, \ldots, k$, by using the equation* (78)*, we will obtain the MSE of the 1-dimensional real case. In fact:*

Since

$$\sum_{i=1}^{k} \| T_i \|_F^2 = \sum_{i=1}^{k} \| a_i \|_F^2 = \sum_{i=1}^{k} Tr(a_i a_i^T) = \sum_{i=1}^{k} a_i^2 = \| a \|^2,$$

where $a = (a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k$, and

$$\| \sum_{i=1}^{k} h_i a_i \|_F^2 = Tr((h_1 a_1 + h_2 a_2 + \cdots + h_k a_k)(h_1 a_1 + h_2 a_2 + \cdots + h_k a_k)) =$$

$$= (h_1 a_1 + h_2 a_2 + \cdots + h_k a_k)^2 = \langle h, a \rangle^2,$$

where $h = (h_1, h_2, \ldots, h_k)$ and $a = (a_1, a_2, \ldots, a_k)$, we have

$$P(\sum_{i=1}^{k} \| T_i \|_F^2 - \frac{1}{\gamma} \| \sum_{i=1}^{k} h_i T_i \|_F^2) = P(\| a \|^2 - \frac{1}{\gamma} \langle h, a \rangle^2).$$

So we have the MSE of the 1-dimensional real case.

Therefore, we have got the equations (78) and (79) as expressions for the mean-square-error (MSE) and, minimizing one of these equations, we obtain the MMSE solution. Then the following section shows us how we can obtain the MMSE solution:

7.3.2 The MSE minimization

The goal of this section is to minimize the equation (79) to obtain the MMSE solution. As $v_i \in \mathbb{Z}[\theta]$, for $i = 1, \ldots, k$, then we have $v_i = a_i + b_i\theta$, where $a_i, b_i \in \mathbb{Z}$. So

$$\sum_{i=1}^{k} Tr_{\mathbb{K}/\mathbb{Q}}(v_i^2) = \sum_{i=1}^{k} Tr_{\mathbb{K}/\mathbb{Q}}(a_i^2 + 2a_i b_i \theta + b_i^2 \theta^2) = \sum_{i=1}^{k} (a_i^2 + b_i^2 \theta^2 +$$

$$+ a_i^2 + b_i^2 \sigma_2(\theta)^2 + a_i^2 + b_i^2 \sigma_3(\theta)^2 + \cdots + a_i^2 + b_i^2 \sigma_n(\theta)^2) =$$

$$= \sum_{i=1}^{k} (n a_i^2 + b_i^2(\theta^2 + \sigma_2(\theta)^2 + \cdots + \sigma_n(\theta)^2)) = \sum_{i=1}^{k} (n a_i^2 + \beta b_i^2),$$

since $Tr_{\mathbb{K}/\mathbb{Q}}(\theta) = \sum_{i=1}^{n} \sigma_i(\theta) = 0$ and we have $\beta = \theta^2 + \sigma_2(\theta)^2 + \cdots + \sigma_n(\theta)^2$ ($\beta \in \mathbb{R}$).

Now we are going to calculate $-\sum_{i,j=1}^{k} h_i h_j Tr_{\mathbb{K}/\mathbb{Q}}(v_i v_j)$, where $v_i = a_i + b_i\theta$ and $v_j = a_j + b_j\theta$, with $i, j = 1, \ldots, k$ and $a_i, b_i, a_j, b_j \in \mathbb{Z}$. However

$$Tr_{\mathbb{K}/\mathbb{Q}}(v_i v_j) = a_i a_j + a_i b_j \theta + a_j b_i \theta + b_i b_j \theta^2 + a_i a_j + a_i b_j \sigma_2(\theta) +$$

$$+ a_j b_i \sigma_2(\theta) + b_i b_j \sigma_2(\theta)^2 + a_i a_j + a_i b_j \sigma_3(\theta) + a_j b_i \sigma_3(\theta) + b_i b_j \sigma_3(\theta)^2 + \cdots +$$

$$+ a_i a_j + a_i b_j \sigma_n(\theta) + a_j b_i \sigma_n(\theta) + b_i b_j \sigma_n(\theta)^2 = n a_i a_j + b_i b_j (\theta^2 +$$

$$+ \sigma_2(\theta)^2 + \sigma_3(\theta)^2 + \cdots + \sigma_n(\theta)^2) = n a_i a_j + \beta b_i b_j,$$

since $Tr_{\mathbb{K}/\mathbb{Q}}(\theta) = \sum_{i=1}^{n} \sigma_i(\theta) = 0$ and we have $\beta = \theta^2 + \sigma_2(\theta)^2 + \cdots + \sigma_n(\theta)^2$. Therefore we

have

$$-\sum_{i,j=1}^{k} h_i h_j Tr_{\mathbb{K}/\mathbb{Q}}(v_i v_j) = -\sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j).$$

Then, from the equation (79), it follows that the MSE is given by

$$P\frac{1}{\gamma}(\gamma\sum_{i=1}^{k}(na_i^2+\beta b_i^2) - \sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j)).$$

To find the MMSE solution we have to minimize the following expression:

$$\gamma\sum_{i=1}^{k}(na_i^2+\beta b_i^2) - \sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j). \tag{80}$$

Observe that the equation (80) is a quadratic form whose variables are α_i, with $i = 1,\ldots,2k$, where $\alpha_{2j} = b_j$ and $\alpha_{2j-1} = a_j$, for $j = 1,\ldots,k$.

So

$$F(\alpha) = \gamma\sum_{i=1}^{k}(na_i^2+\beta b_i^2) - \sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j) = \alpha^T Q \alpha = \alpha^T M^T M \alpha = b^T b,$$

where T denotes the transpose of a matrix, Q is the $2k \times 2k$ gram matrix of the lattice Λ generated by the $2k \times 2k$ matrix M and b is a lattice point, where $b = M\alpha$. We have that Q is a symmetric matrix and $F(\alpha)$ is a positive definite quadratic form.

However we have to find $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2k}) \in (\mathbb{Z}^{2k} - \{0\})$ such that α is the vector that minimizes $F(\alpha)$. So first we are going to find the matrix Q:

$$F(\alpha) = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{2k} \end{pmatrix} \cdot \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1(2k)} \\ q_{21} & q_{22} & \cdots & q_{2(2k)} \\ q_{31} & q_{32} & \cdots & q_{3(2k)} \\ q_{41} & q_{42} & \cdots & q_{4(2k)} \\ \vdots & \vdots & \ddots & \vdots \\ q_{(2k)1} & q_{(2k)2} & \cdots & q_{(2k)(2k)} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2k} \end{pmatrix} =$$

$$= \begin{pmatrix} \sum_{i=1}^{2k}\alpha_i q_{i1} & \sum_{i=1}^{2k}\alpha_i q_{i2} & \sum_{i=1}^{2k}\alpha_i q_{i3} & \cdots & \sum_{i=1}^{2k}\alpha_i q_{i(2k)} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \vdots \\ \alpha_{2k} \end{pmatrix} =$$

$$= \sum_{i=1}^{2k} \alpha_1 \alpha_i q_{i1} + \sum_{i=1}^{2k} \alpha_2 \alpha_i q_{i2} + \sum_{i=1}^{2k} \alpha_3 \alpha_i q_{i3} + \cdots + \sum_{i=1}^{2k} \alpha_{2k} \alpha_i q_{i(2k)} =$$

$$= \sum_{i=1}^{2k} \left(\alpha_1 \alpha_i q_{i1} + \alpha_2 \alpha_i q_{i2} + \alpha_3 \alpha_i q_{i3} + \cdots + \alpha_{2k} \alpha_i q_{i(2k)} \right).$$

Observe that $F(\alpha)$ is also given by the equation (80), that is,

$$F(\alpha) = \gamma \sum_{i=1}^{k} (na_i^2 + \beta b_i^2) - \sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j) = (I) + (II),$$

where $(I) = \gamma \sum_{i=1}^{k} (na_i^2 + \beta b_i^2)$ and $(II) = -\sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j)$.

Then we have

$$(I) = (\gamma n) a_1^2 + (\gamma \beta) b_1^2 + (\gamma n) a_2^2 + (\gamma \beta) b_2^2 + \cdots + (\gamma n) a_k^2 + (\gamma \beta) b_k^2$$

and

$(II) = -(h_1^2(na_1^2 + \beta b_1^2) + h_1 h_2(na_1 a_2 + \beta b_1 b_2) + h_1 h_3(na_1 a_3 + \beta b_1 b_3) + h_1 h_4(na_1 a_4 + \beta b_1 b_4) + \cdots + h_1 h_{k-1}(na_1 a_{k-1} + \beta b_1 b_{k-1}) + h_1 h_k(na_1 a_k + \beta b_1 b_k) + h_2 h_1(na_2 a_1 + \beta b_2 b_1) + h_2^2(na_2^2 + \beta b_2^2) + h_2 h_3(na_2 a_3 + \beta b_2 b_3) + h_2 h_4(na_2 a_4 + \beta b_2 b_4) + \cdots + h_2 h_{k-1}(na_2 a_{k-1} + \beta b_2 b_{k-1}) + h_2 h_k(na_2 a_k + \beta b_2 b_k) + h_3 h_1(na_3 a_1 + \beta b_3 b_1) + h_3 h_2(na_3 a_2 + \beta b_3 b_2) + h_3^2(na_3^2 + \beta b_3^2) + h_3 h_4(na_3 a_4 + \beta b_3 b_4) + \cdots + h_3 h_{k-1}(na_3 a_{k-1} + \beta b_3 b_{k-1}) + h_3 h_k(na_3 a_k + \beta b_3 b_k) + h_4 h_1(na_4 a_1 + \beta b_4 b_1) + h_4 h_2(na_4 a_2 + \beta b_4 b_2) + h_4 h_3(na_4 a_3 + \beta b_4 b_3) + h_4^2(na_4^2 + \beta b_4^2) + \cdots + h_4 h_{k-1}(na_4 a_{k-1} + \beta b_4 b_{k-1}) + h_4 h_k(na_4 a_k + \beta b_4 b_k) + \cdots + h_{k-1} h_1(na_{k-1} a_1 + \beta b_{k-1} b_1) + h_{k-1} h_2(na_{k-1} a_2 + \beta b_{k-1} b_2) + h_{k-1} h_3(na_{k-1} a_3 + \beta b_{k-1} b_3) + h_{k-1} h_4(na_{k-1} a_4 + \beta b_{k-1} b_4) + \cdots + h_{k-1}^2(na_{k-1}^2 + \beta b_{k-1}^2) + h_{k-1} h_k(na_{k-1} a_k + \beta b_{k-1} b_k) + h_k h_1(na_k a_1 + \beta b_k b_1) + h_k h_2(na_k a_2 + \beta b_k b_2) + h_k h_3(na_k a_3 + \beta b_k b_3) + h_k h_4(na_k a_4 + \beta b_k b_4) + \cdots + h_k h_{k-1}(na_k a_{k-1} + \beta b_k b_{k-1}) + h_k^2(na_k^2 + \beta b_k^2))$.

Therefore, since $F(\alpha) = \gamma \sum_{i=1}^{k} (na_i^2 + \beta b_i^2) - \sum_{i,j=1}^{k} h_i h_j (na_i a_j + \beta b_i b_j) = \alpha^T Q \alpha$, we have that the symmetric matrix Q, where

$$Q = \begin{pmatrix} q_{11} & q_{12} & q_{13} & q_{14} & \cdots & q_{1(2k)} \\ q_{21} & q_{22} & q_{23} & q_{24} & \cdots & q_{2(2k)} \\ q_{31} & q_{32} & q_{33} & q_{34} & \cdots & q_{3(2k)} \\ q_{41} & q_{42} & q_{43} & q_{44} & \cdots & q_{4(2k)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{(2k)1} & q_{(2k)2} & q_{(2k)3} & q_{(2k)4} & \cdots & q_{(2k)(2k)} \end{pmatrix},$$

is given by: let $i = 1, \ldots, k$, then

$$q_{(2i-1)(2j-1)} = n(\gamma - h_j^2), \text{ for } j = i;$$

$$q_{(2i-1)(2j)} = 0, \text{ for } j = 1, \ldots, k;$$

$$q_{(2i-1)(2j-1)} = -nh_i h_j, \text{ for } j = 1, \ldots, k \text{ and } j \neq i;$$

and

$$q_{(2i)(2j)} = \beta(\gamma - h_i^2), \text{ for } j = i;$$

$$q_{(2i)(2j-1)} = 0, \text{ for } j = 1, \ldots, k;$$

$$q_{(2i)(2j)} = -\beta h_i h_j, \text{ for } j = 1, \ldots, k \text{ and } j \neq i.$$

To find $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2k}) \in (\mathbb{Z}^{2k} - \{0\})$ such that α is the vector that minimizes $F(\alpha)$, we have to find $b \in \Lambda$ such that b is the shortest lattice point, that is, the closest to the origin. So we have

$$min_{\alpha \in (\mathbb{Z}^{2k} - \{0\})} F(\alpha) = min_{b \in \Lambda} \parallel b \parallel^2 .$$

Then as in the 1-dimensional real case we have $Q = M^T M$ and M can be decomposed as $M = VD_1U^T$, where V and U are $2k \times 2k$ orthogonal matrices and D_1 is a $2k \times 2k$ diagonal matrix whose diagonal entries are the singular values of M.

By taking $J = U^T$ and $W = V^T$ and the fact that U and V are orthogonal matrices, we have that J and W are also $2k \times 2k$ orthogonal matrices and $M = W^T D_1 J$. Then

$$Q = M^T M = (J^T D_1 W)(W^T D_1 J) = J^T D_1^2 J, \text{ since } W \text{ is an orthogonal matrix.}$$

So we have $Q = J^T D_1^2 J$, where J is an orthogonal matrix and D_1^2 is a $2k \times 2k$ diagonal matrix whose diagonal entries are the eigenvalues of Q.

However $Q = J^T D_1^2 J = J^T D_1^T D_1 J = (D_1 J)^T (D_1 J)$, since D_1 is a diagonal matrix. Then we can take the matrix M as $M = D_1 J$, where J is an orthogonal matrix.

The columns of M form a basis for the lattice Λ. Through the QR (Gram-Schmidt) decomposition we have $M = OR$, where O is a $2k \times 2k$ orthogonal matrix and R is a $2k \times 2k$ upper

triangular matrix. If the matrix M is non-singular this factorization is unique. So we have

$$min_{\alpha\in(\mathbb{Z}^{2k}-\{0\})}F(\alpha) = min_{\alpha\in(\mathbb{Z}^{2k}-\{0\})}\alpha^T Q\alpha = min_{\alpha\in(\mathbb{Z}^{2k}-\{0\})}\alpha^T M^T M\alpha =$$

$$= min_{\alpha\in(\mathbb{Z}^{2k}-\{0\})}\alpha^T R^T R\alpha,$$

since O is an orthogonal matrix.

Then we use the Fincke-Pohst Algorithm, that is, given a constant $C > 0$, find all $x \in \mathbb{Z}^{2k}$ such that $F(\alpha) < C$. The algorithm runs in exponential time and works in many practical situations. It makes use of LLL as a subalgorithm.

The best way to determine with certainty the shortest non-zero vectors in the lattice is to let C be the norm of the shortest basis vector in a reduced basis (found using LLL) and then, by using the Fincke-Pohst Algorithm, we search for the shortest vectors in the lattice.

After finding these shortest vectors in the lattice, by testing each one, we can find the shortest one.

Thus, we described a way to find the MMSE solution for the n-dimensional real case, where $n = 2^{r-2}$ and $r \geq 3$.

We can observe that the theory described for the real case related to the MMSE criterion is analogous to the n-dimensional complex case, where $n = 2^{r-2}$ and $r \geq 3$.

Furthermore, since the second order moments are the same, we have to obtain the normalization of $E[\overrightarrow{v}^T\overrightarrow{v}]$, that is, we have to multiply $E[\overrightarrow{v}^T\overrightarrow{v}]$ by $\frac{1}{n}$, since we have n coordinates. So we have $\frac{1}{n}E[\overrightarrow{v}^T\overrightarrow{v}]$ and it follows that

$$\frac{1}{n}E[\overrightarrow{v}^T\overrightarrow{v}] \longrightarrow 0, \text{ when } n \longrightarrow \infty.$$

Then, after such a normalization, we have that the MMSE solution goes to zero, when n goes to the infinity. So, in a probabilistic sense, the error between the desired quantity and our estimate of it goes to zero, when n goes to the infinity.

8 CONSTRUCTION A ASSOCIATED TO CYCLIC CODES OF NESTED LATTICES VIA BINARY CYCLOTOMIC FIELDS AND THE CONSTRUCTION OF DENSE LATTICES VIA CYCLOTOMIC FIELDS

8.1 Introduction

In this chapter, we present the construction of nested lattices from ideals via binary cyclotomic fields. We show the construction A of these nested lattices and, in this case, the linear codes associated to this construction are cyclic codes. So nested lattices from ideals via binary cyclotomic fields can also be obtained from the construction A, whose the associated codes, in this case, are cyclic codes.

We have seen, in this work, that the generalization to obtain infinite nested lattice partition chains shows us the construction A of the corresponding lattices of each infinite nested lattice partition chain. These lattices are not dense, because their minimum squared distances $d^2_{min}(\Lambda)$ are equal to 2.

As the Hermite constant is given by $\gamma(\Lambda) = d^2_{min}(\Lambda)/V(\Lambda)^{2/n}$, where n is the dimension of the lattice Λ, and the respective minimum squared distances are always the same (equal to 2), we just need to consider the lattices with the smallest volume, which are corresponding to D_n, for each dimension n. All the other ones are less dense than D_n, since their mininum squared distances are equal and their volumes are bigger.

Here we are going to show that the dense lattices D_4 and E_8 can be constructed from ideals via the cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{24})$, respectively.

8.2 Construction A Associated to Cyclic Codes of Nested Lattices from Ideals via Binary Cyclotomic Fields

This section presents the construction of nested lattices from ideals via binary cyclotomic fields. We show the construction A of these nested lattices and, in this case, the linear codes associated to this construction are cyclic codes. However, nested lattices from ideals via binary cyclotomic fields can also be obtained from the construction A, whose the associated codes, in this case, are cyclic codes.

Therefore, as in section 5.2, we will consider the following Galois extensions, where $r \geq 3$:

$$\begin{array}{c} L = \mathbb{Q}(\xi_{2^r}) \\ \Big| \, 2^{(r-2)} \\ \mathbb{Q}(i) \\ \Big| \, 2 \\ \mathbb{Q} \end{array} \tag{81}$$

As $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{(r-1)}$, where ϕ is the Euler function, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, then we have $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$. We have that the Galois groups of $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)]$ and $[\mathbb{Q}(i) : \mathbb{Q}]$ are given by

$$Gal(\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)) = \{\sigma_1 = id : \mathbb{Q}(\xi_{2^r}) \to \mathbb{Q}(\xi_{2^r}), \sigma_2, \sigma_3, \ldots, \sigma_{2^{(r-2)}}\} \text{ and}$$

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma_1 = id : \mathbb{Q}(i) \to \mathbb{Q}(i) \text{ and } \sigma_2 : \mathbb{Q}(i) \to \mathbb{Q}(i), \text{ where } \sigma_2(i) = -i\},$$

respectively.

By (OGGIER, 2005), we have $\mathbb{Q}(\xi_{2^r}) = \mathbb{Q}(\xi_{2^r} + \xi_{2^r}^{-1})\mathbb{Q}(i)$. From proposition 2, it follows that $O_L = \mathbb{Z}[\xi_{2^r}]$, the ring of integers of L, is a free $\mathbb{Z}[i]$-module of rank $2^{(r-2)}$ and

$$\{1, \xi_{2^r}, \xi_{2^r}^2, \ldots, \xi_{2^r}^{(2^{(r-2)}-1)}\}$$

is a $\mathbb{Z}[i]$-basis.

Therefore, by the proposition 5, we have that $\sigma(O_L)$ is isomorphic to the $\mathbb{Z}[i]^{2^{(r-2)}}$-lattice.

Now observe that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = (1+i)(1-i) = 2$ and $(1+i)^2 = 2i$. As i is a unit in $\mathbb{Q}(i)$, taking as ideals, we have $2\mathbb{Z}[i] = (2) = (2i) = (1+i)^2$ in $\mathbb{Z}[i]$, so 2 is totally ramified in $\mathbb{Q}(i)$ ($2\mathbb{Z}[i] = (2) = (I')^2$, where $I' = (1+i)$).

As $-i$ is also a unit in $\mathbb{Q}(i)$, we have $(1+i) = ((-i)(1+i)) = (1-i)$. Therefore $(2) = I^2$, where $I = (1-i)$.

Also we can show, by induction over r, that $N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1+\xi_{2^r}) = N_{\mathbb{Q}(\xi_{2^r})/\mathbb{Q}(i)}(1-\xi_{2^r}) = 1-i$. Therefore 2 is totally ramified in $\mathbb{Q}(\xi_{2^r})$ and $2\mathbb{Z}[\xi_{2^r}] = (2) = \mathfrak{I}^{2^{(r-1)}}$, where $\mathfrak{I} = (1+\xi_{2^r})$.

So we have that $\mathfrak{I}$ is the ideal in $O_L = \mathbb{Z}[\xi_{2^r}]$ generated by $\mu = 1+\xi_{2^r}$. By the proposition 4, we have that the ideal $\mathfrak{I}^k$ is generated by μ^k, for all $k \geq 2$. Observe that, for $k = 0$, we have $\mathfrak{I}^0 = O_L = \mathbb{Z}[\xi_{2^r}]$.

The next theorem will give us, for each $r \geq 3$ and $n = 2^{r-2}$, the construction of nested lattices from ideals via the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$:

Theorem 13. *For each $r \geq 3$ and $n = 2^{r-2}$, we have the construction of nested lattices from ideals via the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$. These lattices are obtained from the construction A, whose the associated codes, in this case, are the cyclic codes generated by $(1+x)^s$, where $0 < s = n-k \leq n$ and k is the dimension of the cyclic code.*

Proof. Let $\xi = \xi_{2^r}$. We have $\xi^n = i$, $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$ and $i \equiv 1$ (modulo $(1+i)$), since $i = i(1+i)+1$.

Let $v \in O_L \simeq \mathbb{Z}[i]^n$, then $v = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$, where $a_k \in \mathbb{Z}[i]$, with $k = 0,1,\ldots,n-1$, and $\xi^n = i$.

Since $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$ and $a_k \in \mathbb{Z}[i]$, we have $a_k = (1+i)b_k + c_k$, where $b_k \in \mathbb{Z}[i]$ and c_k=0 or 1. Then

$$v = ((1+i)b_0 + c_0) + ((1+i)b_1 + c_1)\xi + \cdots + ((1+i)b_{n-1} + c_{n-1})\xi^{n-1} =$$

$$= [(1+i)b_0 + (1+i)b_1\xi + \cdots + (1+i)b_{n-1}\xi^{n-1}] + [c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}] =$$

$$= (1+i)(b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1}) + (c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}).$$

Let $w = (1+i)(b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1})$, so $w \in (1+i)O_L \subset O_L$, where $(1+i)O_L \simeq (1+i)\mathbb{Z}[i]^n$, and

$$v = w + (c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}), \text{ where } c_k \in \mathbb{F}_2 = \{0,1\}.$$

Observe that σ is an isomorphism between O_L and the $\mathbb{Z}[i]^n$-lattice and $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$. However,

$$v - w = c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}, \text{ where } c_k \in \mathbb{F}_2 = \{0,1\}.$$

We have $\xi^n = i \equiv 1$ (modulo $(1+i)$), so $\xi^n = 1$ over the field $\mathbb{F}_2 = \{0,1\}$. Let $x = \xi$, then $x^n = 1$ over $\mathbb{F}_2$ and it follows that

$$v(x) - w(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \text{ (modulo } x^n - 1).$$

Since $n-1 < n$, we can conclude that

$$[v(x) - w(x)] = \{c_0 + c_1x + \cdots + c_{n-1}x^{n-1}, \text{ where } c_k \in \mathbb{F}_2 = \{0,1\}\} \simeq \mathbb{F}_2^n.$$

Since $v \in O_L$ is an arbitrary element, it follows that $\mathbb{Z}[i]^n = (1+i)\mathbb{Z}[i]^n + (n,n,1)_{\mathbb{F}_2}$, where $C_0 = (n,n,1)_{\mathbb{F}_2}$ is the universal code.

Now observe that $\Im = (1+\xi) = \{(1+\xi)(a_0+a_1\xi+\cdots+a_{n-1}\xi^{n-1}),$ where $a_k \in \mathbb{Z}[i],\ k = 0,1,\ldots,n-1,$ and $\xi^n = i$ over $\mathbb{Q}(i)\}$.

Let $u \in \Im$, then $u = (1+\xi)(a_0+a_1\xi+\cdots+a_{n-1}\xi^{n-1})$, where $a_k \in \mathbb{Z}[i]$, with $k = 0,1,\ldots,n-1$, and $\xi^n = i \equiv 1$ (modulo $(1+i)$).

Since $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$ and $a_k \in \mathbb{Z}[i]$, we have $a_k = (1+i)b_k + c_k$, where $b_k \in \mathbb{Z}[i]$ and c_k=0 or 1. Therefore,

$$u = (1+\xi)[((1+i)b_0+c_0)+((1+i)b_1+c_1)\xi+\cdots+((1+i)b_{n-1}+c_{n-1})\xi^{n-1})] =$$

$$= (1+\xi)[(1+i)b_0+(1+i)b_1\xi+\cdots+(1+i)b_{n-1}\xi^{n-1}]+$$

$$+(1+\xi)[c_0+c_1\xi+\cdots+c_{n-1}\xi^{n-1}] =$$

$$= (1+\xi)(1+i)(b_0+b_1\xi+\cdots+b_{n-1}\xi^{n-1})+(1+\xi)(c_0+c_1\xi+\cdots+c_{n-1}\xi^{n-1}) =$$

$$= (1+i)(1+\xi)(b_0+b_1\xi+\cdots+b_{n-1}\xi^{n-1})+(1+\xi)(c_0+c_1\xi+\cdots+c_{n-1}\xi^{n-1}).$$

Let $w_1 = (1+i)(1+\xi)(b_0+b_1\xi+\cdots+b_{n-1}\xi^{n-1})$. Since $\xi^n = i$ and $b_k \in \mathbb{Z}[i]$, we have $w_1 \in (1+i)O_L \subset O_L$, where $(1+i)O_L \simeq (1+i)\mathbb{Z}[i]^n$, and

$$u = w_1 + (1+\xi)(c_0+c_1\xi+\cdots+c_{n-1}\xi^{n-1}),\ \text{where } c_k \in \mathbb{F}_2 = \{0,1\}.$$

Observe that σ is an isomorphism between O_L and the $\mathbb{Z}[i]^n$-lattice and $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$. However,

$$u - w_1 = (1+\xi)(c_0+c_1\xi+\cdots+c_{n-1}\xi^{n-1}),\ \text{where } c_k \in \mathbb{F}_2 = \{0,1\}.$$

We have $\xi^n = i \equiv 1$ (modulo $(1+i)$), so $\xi^n = 1$ over the field $\mathbb{F}_2 = \{0,1\}$. Let $x = \xi$, then $x^n = 1$ over $\mathbb{F}_2$ and it follows that

$$u(x) - w_1(x) = (1+x)(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) \text{ (modulo } x^n-1).$$

So we can conclude that

$$[u(x) - w_1(x)] = \{(1+x)(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) \text{ (modulo } x^n-1);$$

$$c_k \in \mathbb{F}_2\} = (1+x),$$

which is the parity check cyclic code that corresponds to the ideal in $\frac{\mathbb{F}_2[x]}{(x^n-1)}$ generated by $(1+x)$.

However, we have $u \in \Im = (1+\xi)$ an arbitrary element and, after the quotient, we have the identification with the ideal in $\frac{\mathbb{F}_2[x]}{(x^n-1)}$ generated by $(1+x)$. Then it follows that $\sigma(\Im) = (1+i)\mathbb{Z}[i]^n + C_1$, where C_1 is the parity check cyclic code, which has dimension $n-1$.

Let $0 < s \leq n = 2^{r-2}$, $u_s \in \Im^s$ and $\Im^s = ((1+\xi)^s) = \{(1+\xi)^s(a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1})$, where $a_k \in \mathbb{Z}[i]$, $k = 0,1,\ldots,n-1$, and $\xi^n = i$ over $\mathbb{Q}(i)\}$.

Analogously to the case $s = 1$, we have $u_s = (1+\xi)^s(a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1})$, where $a_k \in \mathbb{Z}[i]$, with $k = 0,1,\ldots,n-1$, and $\xi^n = i \equiv 1$ (modulo $(1+i)$).

Since $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$ and $a_k \in \mathbb{Z}[i]$, we have $a_k = (1+i)b_k + c_k$, where $b_k \in \mathbb{Z}[i]$ and c_k=0 or 1. Therefore,

$$u_s = (1+\xi)^s[((1+i)b_0 + c_0) + ((1+i)b_1 + c_1)\xi + \cdots + ((1+i)b_{n-1} + c_{n-1})\xi^{n-1}] =$$

$$= (1+\xi)^s[(1+i)b_0 + (1+i)b_1\xi + \cdots + (1+i)b_{n-1}\xi^{n-1}] +$$

$$+ (1+\xi)^s[c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}] =$$

$$= (1+\xi)^s(1+i)(b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1}) + (1+\xi)^s(c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}) =$$

$$= (1+i)(1+\xi)^s(b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1}) +$$

$$+ (1+\xi)^s(c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}).$$

Let $w_s = (1+i)(1+\xi)^s(b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1})$. Since $\xi^n = i$ and $b_k \in \mathbb{Z}[i]$, we have $w_s \in (1+i)O_L \subset O_L$, where $(1+i)O_L \simeq (1+i)\mathbb{Z}[i]^n$, and

$$u_s = w_s + (1+\xi)^s(c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}), \text{ where } c_k \in \mathbb{F}_2 = \{0,1\}.$$

Observe that σ is an isomorphism between O_L and the $\mathbb{Z}[i]^n$-lattice and $\frac{\mathbb{Z}[i]}{(1+i)\mathbb{Z}[i]} \simeq \mathbb{F}_2 = \{0,1\}$. However,

$$u_s - w_s = (1+\xi)^s(c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}), \text{ where } c_k \in \mathbb{F}_2 = \{0,1\}.$$

We have $\xi^n = i \equiv 1$ (modulo $(1+i)$), so $\xi^n = 1$ over the field $\mathbb{F}_2 = \{0,1\}$. Let $x = \xi$, then

$x^n = 1$ over $\mathbb{F}_2$ and it follows that

$$u_s(x) - w_s(x) = (1+x)^s(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) \text{ (modulo } x^n - 1).$$

So we can conclude that

$$[u_s(x) - w_s(x)] = \{(1+x)^s(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) \text{ (modulo } x^n - 1);$$

$$c_k \in \mathbb{F}_2\} = ((1+x)^s),$$

which corresponds to the ideal in $\frac{\mathbb{F}_2[x]}{(x^n-1)}$ generated by $(1+x)^s$, where $0 < s \leq n$.

However, we have $u_s \in \Im^s = ((1+\xi)^s)$ an arbitrary element and, after the quotient, we have the identification with the ideal in $\frac{\mathbb{F}_2[x]}{(x^n-1)}$ generated by $(1+x)^s$. Then it follows that $\sigma(\Im^s) = (1+i)\mathbb{Z}[i]^n + C_s$, where C_s is the binary cyclic code with generator polynomial $(1+x)^s$, which has dimension $n-s$.

When $s = n$, we have $\sigma(\Im^n) = (1+i)\mathbb{Z}[i]^n + C_n$, where C_n is the binary cyclic code with generator polynomial $(1+x)^n$.

But $(1+x)^n = x^n + 1$, since $n = 2^{r-2}$, and $x^n + 1$ is equivalent to $x^n - 1$. So the binary cyclic code C_n is the cyclic code which only contains the null codeword, since the binary polynomial $x^n - 1$ generates the cyclic code which only contains the null codeword. □

However, the previous theorem gives us, for each $r \geq 3$ and $n = 2^{r-2}$, the construction of nested lattices from ideals via the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$. Such lattices are obtained from the construction A, whose the associated codes, in this case, are the binary cyclic codes generated by $(1+x)^s$, where $0 < s = n - k \leq n$ and k is the dimension of the cyclic code.

8.3 Construction of the Dense Lattices D_4 and E_8 from Ideals via Cyclotomic Fields

In this work, the generalization to obtain infinite nested lattice partition chains shows us the construction A of the corresponding lattices of each infinite nested lattice partition chain. We have that these lattices are not dense, because their minimum squared distances $d^2_{min}(\Lambda)$ are equal to 2.

In this section, we are going to show that the dense lattices D_4 and E_8 can be constructed from ideals via the cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{24})$, respectively.

So the following section shows us the construction of the dense lattice D_4 from an ideal via the binary cyclotomic field $\mathbb{Q}(\xi_8)$:

8.3.1 Construction of the dense lattice D_4

The goal of this section is to show that the dense lattice D_4 can be obtained from an ideal via the binary cyclotomic field $\mathbb{Q}(\xi_8)$. However, as in section 4.3.1, we will consider the following Galois extensions:

$$\begin{array}{c} L=\mathbb{Q}(\xi_8) \\ \Big| 2 \\ \mathbb{Q}(i) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{82}$$

As $[\mathbb{Q}(\xi_8):\mathbb{Q}]=\phi(8)=4$, where ϕ is the Euler function, and $[\mathbb{Q}(i):\mathbb{Q}]=2$, then we have $[\mathbb{Q}(\xi_8):\mathbb{Q}(i)]=2$. We have that the Galois groups of $[\mathbb{Q}(\xi_8):\mathbb{Q}(i)]$ and $[\mathbb{Q}(i):\mathbb{Q}]$ are given by

$$Gal(\mathbb{Q}(\xi_8)/\mathbb{Q}(i))=\{\sigma_1=id:\mathbb{Q}(\xi_8)\to\mathbb{Q}(\xi_8) \text{ and } \sigma_2:\mathbb{Q}(\xi_8)\to\mathbb{Q}(\xi_8);\ \sigma_2(\xi_8)=-\xi_8\} \text{ and}$$

$$Gal(\mathbb{Q}(i)/\mathbb{Q})=\{\sigma_1=id:\mathbb{Q}(i)\to\mathbb{Q}(i) \text{ and } \sigma_2:\mathbb{Q}(i)\to\mathbb{Q}(i);\ \sigma_2(i)=-i\},$$

respectively, where *id* is the identity map.

By (OGGIER, 2005), we have $\mathbb{Q}(\xi_8)=\mathbb{Q}(\xi_8+\xi_8^{-1})\mathbb{Q}(i)=\mathbb{Q}(\sqrt{2})\mathbb{Q}(i)$. From proposition 2, it follows that $O_L=\mathbb{Z}[\xi_8]$, the ring of integers of L, is a free $\mathbb{Z}[i]$-module of rank 2 and $\{1,\xi_8\}$ is a $\mathbb{Z}[i]$-basis.

Since $\{1,\xi_8\}$ is a $\mathbb{Z}[i]$-basis of O_L, so the matrix

$$M_0=\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\xi_8) & \sigma_2(\xi_8) \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ \xi_8 & -\xi_8 \end{pmatrix}$$

is the generator matrix of the complex algebraic lattice $\sigma(O_L)$.

Observe that M_0 and $M=M_0^T$ have the same properties. If we take $M_0'=\frac{1}{\sqrt{2}}M_0$, we have $(M_0')(M_0')^H$ equal to the identity matrix, where $(M_0')^H$ denotes the transpose conjugate of M_0'. So $M_0'=\frac{1}{\sqrt{2}}M_0$ is a unitary matrix and using the same argument as before we have that $U=\frac{1}{\sqrt{2}}M_0^T$ is also a unitary matrix.

Therefore, by the proposition 5, $\sigma(O_L)$ is isomorphic to the $\mathbb{Z}[i]^2$-lattice.

Now observe that $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i)=(1+i)(1-i)=2$ and $(1+i)^2=2i$. As i is a unit in $\mathbb{Q}(i)$, taking as ideals, we have $2\mathbb{Z}[i]=(2)=(2i)=(1+i)^2$ in $\mathbb{Z}[i]$, so 2 is totally ramified in $\mathbb{Q}(i)$ ($2\mathbb{Z}[i]=(2)=(I')^2$, where $I'=(1+i)$).

As $-i$ is also a unit in $\mathbb{Q}(i)$, we have $(1+i) = ((-i)(1+i)) = (1-i)$. Therefore $(2) = I^2$, where $I = (1-i)$.

We also have that

$$1-i = (1+\xi_8)(1-\xi_8) = N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1+\xi_8) = N_{\mathbb{Q}(\xi_8)/\mathbb{Q}(i)}(1-\xi_8).$$

Then we can conclude that 2 is totally ramified in $\mathbb{Q}(\xi_8)$ and $2\mathbb{Z}[\xi_8] = (2) = \mathfrak{I}^4$, where $\mathfrak{I} = (1+\xi_8)$ is the ideal in $O_L = \mathbb{Z}[\xi_8]$ generated by $\mu = 1+\xi_8$.

We can show that $\{\mu, \mu\xi_8\}$ is a $\mathbb{Z}[i]$-basis of $\mathfrak{I} = \mu\mathbb{Z}[\xi_8] = \mu O_L$, where $\{1, \xi_8\}$ is a $\mathbb{Z}[i]$-basis of O_L.

Then, by the proposition 12, we have that the generator matrix of the complex algebraic lattice $\sigma(\mu O_L)$ is given by (note that the transposed matrix has the same properties)

$$M_1 = \begin{pmatrix} \mu & \mu\xi_8 \\ \sigma(\mu) & \sigma(\mu)\sigma(\xi_8) \end{pmatrix} = \begin{pmatrix} \mu & 0 \\ 0 & \sigma(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \xi_8 \\ 1 & -\xi_8 \end{pmatrix} \cdot M_\mu.$$

It is easy to see that M_μ is given by

$$\begin{pmatrix} 1 & i \\ 1 & 1 \end{pmatrix},$$

where M_μ is a generator matrix of the lattice D_4 seen as a $\mathbb{Z}[i]$-lattice; in fact, the matrix M_μ with real entries is given by

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

and we can note that in each column of M_μ the sum of the coefficients is even, therefore the lattice Λ_1 generated by M_μ is a sublattice of D_4. Moreover, we have that $Vol(\Lambda_1) = 2 = Det(M_\mu) = Vol(D_4)$, then the index $|D_4/\Lambda_1|$ is equal to 1 and so $\Lambda_1 = D_4$.

With these properties, we have that M_μ is a generator matrix of D_4 seen as a $\mathbb{Z}[i]$-lattice.

This means that, if μ generates the ideal μO_L, then the matrix M_μ is a generator matrix of the lattice D_4.

So, in this section, we have just showed that the dense lattice D_4 can be obtained from an ideal via the binary cyclotomic field $\mathbb{Q}(\xi_8)$.

Now, to achieve the goal of this chapter, the following section provides us the construction of the dense lattice E_8 from an ideal via the cyclotomic field $\mathbb{Q}(\xi_{24})$.

8.3.2 Construction of the dense lattice E_8

In this section, we are going to show that the dense lattice E_8 can be obtained from an ideal via the cyclotomic field $\mathbb{Q}(\xi_{24})$. So we will consider the following Galois extensions:

$$\begin{array}{c} L=\mathbb{Q}(\xi_{24}) \\ \Big| 4 \\ \mathbb{Q}(\omega) \\ \Big| 2 \\ \mathbb{Q} \end{array} \tag{83}$$

Let $\xi_3=\omega=e^{\frac{2\pi i}{3}}=\frac{-1+\sqrt{3}i}{2}$ and $\xi=\xi_{24}=e^{\frac{2\pi i}{24}}$ be the third root of unity and the 24-th root of unity, respectively. We can notice that $\omega^2+\omega+1=0$ and $\omega^2=-\xi_{24}^4$, then we have $\xi_{24}^4+\omega^2=0$. Observe that x^2+x+1 and $x^4+\omega^2$ are monic and irreducible polynomials over $\mathbb{Q}$ and $\mathbb{Q}(\omega)$, respectively. As $[\mathbb{Q}(\xi_{24}):\mathbb{Q}]=\phi(24)=8$, where ϕ is the Euler function, and $[\mathbb{Q}(\omega):\mathbb{Q}]=2$, then we have $[\mathbb{Q}(\xi_{24}):\mathbb{Q}(\omega)]=4=n$.

Since $\{1,\xi,\ldots,\xi^7\}$ is an integral basis of $O_L=\mathbb{Z}[\xi_{24}]=\mathbb{Z}[\xi]$, the ring of integers of L, and $\xi_{24}=-\omega^2$, it follows that $O_L=\mathbb{Z}[\xi]$ is a free $\mathbb{Z}[\omega]$-module of rank 4 and

$$\{1,\xi,\xi^2,\xi^3\}$$

is a $\mathbb{Z}[\omega]$-basis of O_L.

Let $2+\omega=\sqrt{-3}=i\sqrt{3}\in\mathbb{Z}[\omega]$, where $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}(\omega)$. Now observe that $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(2+\omega)=(2+\omega)(2+\omega^2)=4+2\omega^2+2\omega+\omega^3=2(\omega^2+\omega)+5=-2+5=3$, since $\omega^2+\omega+1=0$, and $(2+w)^2=-3\omega^2=3(-\omega^2)$. So 3 is totally ramified in $\mathbb{Q}(\omega)$.

However, we have that 3 is totally ramified in $\mathbb{Q}(\xi_{24})=\mathbb{Q}(\xi)$ and $3\mathbb{Z}[\xi_{24}]=(3)=\mathfrak{I}^8$, where $\mathfrak{I}=((1+\omega)\xi+\omega\xi^2+\omega\xi^3)$. Then we have that $\mathfrak{I}$ is the ideal in $O_L=\mathbb{Z}[\xi]$ generated by $\mu=(1+\omega)\xi+\omega\xi^2+\omega\xi^3$.

Observe that $\xi\in\mathbb{Z}[\xi]$ and $\mu=\xi((1+\omega)+\omega\xi+\omega\xi^2)$. Since ξ is a unity in $\mathbb{Z}[\xi]$, it follows that the ideal $\mathfrak{I}$ is also generated by $\mu'=(1+\omega)+\omega\xi+\omega\xi^2$. So $\mathfrak{I}=((1+\omega)+\omega\xi+\omega\xi^2)=(\mu')$.

The next theorem will show us that the dense lattice E_8 can be obtained from the ideal $\Im = ((1+\omega)+\omega\xi+\omega\xi^2)$ via the cyclotomic field $\mathbb{Q}(\xi_{24})$:

Theorem 14. *The dense lattice E_8 can be obtained from the ideal $\Im = ((1+\omega)+\omega\xi+\omega\xi^2)$ in $\mathbb{Z}[\xi_{24}]$, the ring of integers of $\mathbb{Q}(\xi_{24})$, via the cyclotomic field $\mathbb{Q}(\xi_{24})$. The lattice E_8 is obtained from the construction A, whose the associated code, in this case, is the negacyclic code generated by $(-1+x+x^2)$ and called Tetracode.*

Proof. Let $\xi = \xi_{24}$. We have $\xi^4 = -\omega^2$, $\frac{\mathbb{Z}[\omega]}{(2+\omega)\mathbb{Z}[\omega]} \simeq \mathbb{F}_3 = \{0,1,-1\}$ and $\omega^2 \equiv 1$ (modulo $(2+\omega)$), since $\omega^2 = -(1+\omega) \equiv 1$ (modulo $(2+\omega)$).

Let $v \in O_L$, then $v = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3$, where $a_k \in \mathbb{Z}[\omega]$, with $k = 0,1,2,3$, and $\xi^4 = -\omega^2$.

Since $\frac{\mathbb{Z}[\omega]}{(2+\omega)\mathbb{Z}[\omega]} \simeq \mathbb{F}_3 = \{0,1,-1\}$ and $a_k \in \mathbb{Z}[\omega]$, we have $a_k = (2+\omega)b_k + c_k$, where $b_k \in \mathbb{Z}[\omega]$ and c_k=0,1 or -1. Then

$$v = ((2+\omega)b_0 + c_0) + ((2+\omega)b_1 + c_1)\xi + ((2+\omega)b_2 + c_2)\xi^2 + ((2+\omega)b_3 + c_3)\xi^3 =$$

$$= [(2+\omega)b_0 + (2+\omega)b_1\xi + (2+\omega)b_2\xi^2 + (2+\omega)b_3\xi^3] + [c_0 + c_1\xi + c_2\xi^2 + c_3\xi^3] =$$

$$= (2+\omega)(b_0 + b_1\xi + b_2\xi^2 + b_3\xi^3) + (c_0 + c_1\xi + c_2\xi^2 + c_3\xi^3).$$

Let $w = (2+\omega)(b_0 + b_1\xi + b_2\xi^2 + b_3\xi^3)$, so $w \in (2+\omega)O_L \subset O_L$ and

$$v = w + (c_0 + c_1\xi + c_2\xi^2 + c_3\xi^3), \text{ where } c_k \in \mathbb{F}_3 = \{0,1,-1\}.$$

However,

$$v - w = c_0 + c_1\xi + c_2\xi^2 + c_3\xi^3, \text{ where } c_k \in \mathbb{F}_3 = \{0,1,-1\}.$$

We have $\xi^4 = -\omega^2 \equiv (-1)$ (modulo $(2+\omega)$), so $\xi^4 = -1$ over the field $\mathbb{F}_3 = \{0,1,-1\}$. Let $x = \xi$, then $x^4 = -1$ over $\mathbb{F}_3$ and it follows that

$$v(x) - w(x) = c_0 + c_1x + c_2x^2 + c_3x^3 \text{ (modulo } x^4 - 1).$$

Since $3 < 4$, we can conclude that

$$[v(x) - w(x)] = \{c_0 + c_1x + c_2x^2 + c_3x^3, \text{ where } c_k \in \mathbb{F}_3 = \{0,1,-1\}\} \simeq \mathbb{F}_3^4.$$

Using the fact that $v \in O_L$ is an arbitrary element, it follows that $\frac{O_L}{(2+\omega)O_L} \simeq \mathbb{F}_3^4$. But since

$\frac{\mathbb{Z}[\omega]}{(2+\omega)\mathbb{Z}[\omega]} \simeq \mathbb{F}_3$, we have $\mathbb{Z}[\omega]^4 = (2+\omega)\mathbb{Z}[\omega]^4 + (4,4,1)_{\mathbb{F}_3}$, where $C_0 = (4,4,1)_{\mathbb{F}_3}$ is the universal code. Therefore $O_L \simeq \mathbb{Z}[\omega]^4$.

Now observe that $\Im = ((1+\omega)+\omega\xi+\omega\xi^2) = \{((1+\omega)+\omega\xi+\omega\xi^2)(a_0+a_1\xi+a_2\xi^2+a_3\xi^3),$ where $a_k \in \mathbb{Z}[\omega],\ k=0,1,2,3,$ and $\xi^4 = -\omega^2$ over $\mathbb{Q}(\omega)\}$.

Let $u \in \Im$, then $u = \mu'(a_0+a_1\xi+a_2\xi^2+a_3\xi^3)$, where $a_k \in \mathbb{Z}[\omega]$, with $k=0,1,2,3$, and $\xi^4 = -\omega^2 \equiv (-1)$ (modulo $(2+\omega)$).

Since $\frac{\mathbb{Z}[\omega]}{(2+\omega)\mathbb{Z}[\omega]} \simeq \mathbb{F}_3 = \{0,1,-1\}$ and $a_k \in \mathbb{Z}[\omega]$, we have $a_k = (2+\omega)b_k + c_k$, where $b_k \in \mathbb{Z}[\omega]$ and c_k=0,1 or -1. Therefore,

$$u = \mu'[((2+\omega)b_0+c_0)+((2+\omega)b_1+c_1)\xi+((2+\omega)b_2+c_2)\xi^2+((2+\omega)b_3+c_3)\xi^3)] =$$

$$= \mu'[(2+\omega)b_0+(2+\omega)b_1\xi+(2+\omega)b_2\xi^2+(2+\omega)b_3\xi^3] + \mu'[c_0+c_1\xi+c_2\xi^2+c_3\xi^3] =$$

$$= \mu'(2+\omega)(b_0+b_1\xi+b_2\xi^2+b_3\xi^3) + \mu'(c_0+c_1\xi+c_2\xi^2+c_3\xi^3) =$$

$$= (2+\omega)\mu'(b_0+b_1\xi+b_2\xi^2+b_3\xi^3) + \mu'(c_0+c_1\xi+c_2\xi^2+c_3\xi^3).$$

Let $w_1 = (2+\omega)\mu'(b_0+b_1\xi+b_2\xi^2+b_3\xi^3)$. Since $\xi^4 = -\omega^2$ and $b_k \in \mathbb{Z}[\omega]$, we have $w_1 \in (2+\omega)O_L \subset O_L$, where $(2+\omega)O_L \simeq (2+\omega)\mathbb{Z}[\omega]^4$, and

$$u = w_1 + \mu'(c_0+c_1\xi+c_2\xi^2+c_3\xi^3), \text{ where } c_k \in \mathbb{F}_3 = \{0,1,-1\}.$$

Observe that $\frac{\mathbb{Z}[\omega]}{(2+\omega)\mathbb{Z}[\omega]} \simeq \mathbb{F}_3 = \{0,1,-1\}$ and let σ be an isomorphism between O_L and the $\mathbb{Z}[\omega]^4$-lattice. However,

$$u - w_1 = ((1+\omega)+\omega\xi+\omega\xi^2)(c_0+c_1\xi+c_2\xi^2+c_3\xi^3),$$

where $c_k \in \mathbb{F}_3 = \{0,1,-1\}$.

As $((1+\omega)+\omega\xi+\omega\xi^2) \in O_L$, then we have

$$((1+\omega)+\omega\xi+\omega\xi^2) \equiv (-1+\xi+\xi^2) \text{ (modulo } (2+\omega)),$$

since $(1+\omega) \equiv -1$ (modulo $(2+\omega)$) and $\omega \equiv 1$ (modulo $(2+\omega)$).

We have $\xi^4 = -\omega^2 \equiv (-1)$ (modulo $(2+\omega)$), so $\xi^4 = (-1)$ over the field $\mathbb{F}_3 = \{0,1,-1\}$. Let $x = \xi$, then $x^4 = (-1)$ $(x^4+1=0)$ over $\mathbb{F}_3$ and it follows that

$$u(x) - w_1(x) = (x^2+x-1)(c_0+c_1x+c_2\xi^2+c_3x^3) \text{ (modulo } x^4+1).$$

So we can conclude that

$$[u(x)-w_1(x)] = \{(x^2+x-1)(c_0+c_1x+c_2x^2+c_3x^3) \text{ (modulo } x^4+1);$$

$$c_k \in \mathbb{F}_3\} = (x^2+x-1),$$

which corresponds to the ideal in $\frac{\mathbb{F}_3[x]}{(x^4+1)}$ generated by (x^2+x-1).

However, we have $u \in \Im = (\mu')$ an arbitrary element and, after the quotient, we have the identification with the ideal in $\frac{\mathbb{F}_3[x]}{(x^4+1)}$ generated by (x^2+x-1). Then it follows that $\sigma(\Im) = (2+\omega)\mathbb{Z}[\omega]^4 + C_1$, where C_1 is the negacyclic code called *Tetracode*, which has dimension 2 and generator polynomial x^2+x-1. The Tetracode C_1 is given by

$$C_1 = \{(0,0,0,0);(0,-1,1,1);(0,1,-1,-1);(1,-1,-1,0);$$

$$(-1,1,1,0);(1,1,0,1);(1,0,1,-1);(-1,-1,0,-1);(-1,0,-1,1)\}$$

and its respective generator matrix is given by

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

Therefore, by (CONWAY; SLOANE, 1999), page 200, we have

$$\sigma(\Im) = (2+\omega)\mathbb{Z}[\omega]^4 + C_1 = (2+\omega)\mathbb{Z}[\omega]^4 + (4,2,3)_{\mathbb{F}_3} = E_8.$$

So we have that $\Lambda_4 = \mathbb{Z}[\omega]^4/\Lambda_3/\Lambda_2 = E_8/\Lambda_1/\Lambda_0 = (2+\omega)\mathbb{Z}[\omega]^4$ is a lattice partition chain, where each partition has order equal to 3 and the codes related to each lattice Λ_j, $j = 0,1,2,3,4$, have dimension equal to j.

However, we can conclude that the lattice E_8 can be obtained from an ideal via the cyclotomic field $\mathbb{Q}(\xi_{24})$. □

Also, in this section, we can conclude that the dense lattices D_4 and E_8 can be constructed from ideals via the cyclotomic fields $\mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\xi_{24})$, respectively.

9 CONCLUSION AND FUTURE WORK

In this work, we extended the procedure of the construction of perfect codes from cyclic division algebras over $\mathbb{Q}(\zeta_3)$ for the family of dimension n, where n is any even degree such that 3 does not divide n.

For that, we observed that Elia et al. (ELIA; SETHURAMAN; KUMAR, 2007) generalized the procedure of the construction of perfect codes and showed their existence for any dimension when the considered codes are subsets of cyclic division algebras over the number field $\mathbb{Q}(i)$. Furthermore, the authors proposed a construction of perfect codes from cyclic division algebras over the number field $\mathbb{Q}(\zeta_3)$ only for the dimension $n = 2^s n_1$, with $s \in \{0,1\}$ and n_1 is odd. For doing such a generalization, we have the concept of perfect space-time codes that was introduced in (OGGIER et al., 2006).

We can see that the main difference between the works (OGGIER et al., 2006; ELIA; SETHURAMAN; KUMAR, 2007) is that (OGGIER et al., 2006) only chooses the non-norm element γ to be a root of unity in $\mathscr{O}_K$, where $\mathscr{O}_K$ is the ring of integers of the number field K, while (ELIA; SETHURAMAN; KUMAR, 2007) uses elements with denominators. If one fixes the constraint that γ is indeed a root of unity, then the codes cannot exist in other dimensions than $2,3,4,6$, as shown by (BERHUY; OGGIER, 2009).

From the arithmetic procedure proposed in (ANDRADE; CARVALHO, 2011) for the construction of $\mathbb{Z}^n$-rotated lattices from cyclic extensions of $\mathbb{Q}$ with even positive degree n, the new class of perfect space-time codes obtained keeps the same properties as the codes proposed by Elia *et.al* (ELIA; SETHURAMAN; KUMAR, 2007). However, in this case, the good shaping associated to the lattices is given by the $\mathscr{A}_2^n$-rotated lattices.

Also in this work, we developed a new methodology to quantize the channel coefficients in order to realize interference alignment onto a lattice. Our channel model is the same from the compute-and-forward strategy (NAZER; GASTPAR, 2011).

In this new methodology, we have described a way to find an infinite nested lattice partition chain for any dimension $n = 2^{r-2}$, where $r \geq 3$, and we made use of the binary cyclotomic field $\mathbb{Q}(\xi_{2^r})$, with $r \geq 3$, $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}] = \phi(2^r) = 2^{(r-1)}$, where ϕ is the Euler function, and $[\mathbb{Q}(\xi_{2^r}) : \mathbb{Q}(i)] = 2^{(r-2)} = n$. So we developed, for the complex case, the generalization to obtain such infinite nested lattice partition chains. We also developed a methodology for the real case.

And by using the MMSE criterion, we showed, in a probabilistic sense, that the error be-

tween the desired quantity and our estimate of it goes to zero, when n goes to the infinity. So we have a good channel approximation.

The generalization to obtain these infinite nested lattice partition chains shows us the construction A of the corresponding lattices of each infinite nested lattice partition chain. These lattices are not dense because their minimum squared distances $d^2_{min}(\Lambda)$ are equal to 2.

As the Hermite constant is given by $\gamma(\Lambda) = d^2_{min}(\Lambda)/V(\Lambda)^{2/n}$, where n is the dimension of the lattice Λ, and the respective minimum squared distances are always the same (equal to 2), we just need to consider the lattices with the smallest volume, which are corresponding to D_n, for each dimension n. All the other ones are less dense than D_n, since their mininum squared distances are equal and their volumes are bigger.

The error probability is related to the Hermite constant (CONWAY; SLOANE, 1999), that is, as the Hermite constant increases, the error probability decreases. So, for further work, we want to obtain the distributed computation, that is, the non-linearity for the compute-and-forward strategy and, at the same time, we want to achieve the AWGN channel capacity. For that, the goal is to find finite number fields that give us right commutative orders, i.e., by using the Minkowski embedding we want to associate such commutative orders with the lattices in (EREZ; ZAMIR, 2004), where we can obtain the AWGN channel capacity. Since orders are rings, we have the multiplication operation and, by using the Minkowski embedding, we can associate the multiplication of two elements that belong to the commutative order with an element of the lattice. So we can perform the non-linearity for the compute-and-forward strategy.

Also, we can apply this new methodology in communication interference (JAFARIAN; VISHWANATH, 2012). The compute-and-forward strategy (NAZER; GASTPAR, 2011) and the communication interference are related to the communications engineering.

Another possible application is related to the computer science, it might be possible to apply the theory developed in this work in homomorphic encryption schemes.

This new methodology is original and can contributes greatly to the area, that is, it also can be very useful in future developments.

REFERENCE

ALBERT, A. A. *Structure of algebras*. 2. ed. Providence: American Mathematical Society Colloquium Publications, 1961. 210 p.

ANDRADE, A. A.; CARVALHO, E. D. Cyclic construction of rotated lattices with full diversity. *Journal of Advanced Research in Applied Mathematics-JARAM*, Irvine, PAS-3, n. 3, p. 82–92, Jun. 2011.

ANDRADE, A. A. de; ALVES, C.; BERTOLDI, T. C. Rotated lattices via the cyclotomic field $\mathbb{Q}(\xi_{2^r})$. *International Journal of Applied Mathematics*, Hong Kong, PAS-19, n. 3, p. 321–331, Aug. 2006.

BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the rayleigh fading channel. *IEEE Trans. Inform. Theory*, New York, PAS-50, n. 4, p. 702–714, Mar. 2004.

BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. Algebraic lattice constellations: bounds on performance. *IEEE Trans. Inform. Theory*, New York, PAS-52, n. 1, p. 319–327, Jan. 2006.

BELFIORE, J.-C.; REKAYA, G.; VITERBO, E. The golden code: a 2×2 full rate space-time code with non vanishing determinants. *IEEE Trans. Inform. Theory*, New York, PAS-51, n. 4, p. 1432–1436, Apr. 2005.

BERHUY, G.; OGGIER, F. On the existence of perfect space-time codes. *IEEE Trans. Inform. Theory*, New York, PAS-55, n. 5, p. 2078–2082, May 2009.

BOUTROS, J.; VITERBO, E. Signal space diversity: a power - and bandwidth-efficient diversity technique for the rayleigh fading channel. *IEEE Trans. Inform. Theory*, New York, PAS-44, n. 4, p. 1453–1467, Jul. 1998.

CONWAY, J. H.; SLOANE, N. J. A. *Sphere packings, lattices and groups*. 3. ed. New York: Springer-Verlag, 1999. 703 p.

DAYAL, P.; VARANASI, M. K. An optimal two transmit antennas space-time code and its stacked extensions. In: SIGNALS, SYSTEMS AND COMPUTERS, CONFERENCE RECORDS, 37.,2003. *Asilomar Conference*. [S.l.: s.n.], 2003. v. 1, p. 987–991.

ELIA, P.; SETHURAMAN, B. A.; KUMAR, P. V. Perfect space-time codes for any number of antennas. *IEEE Trans. Inform. Theory*, New York, PAS-53, n. 11, p. 3853–3868, Nov. 2007.

ENDLER, O. *Teoria dos números algébricos*. 2. ed. Rio de Janeiro: IMPA, 2006. 199 p.

EREZ, U.; ZAMIR, R. Achieving $\frac{1}{2}$log(1+snr) on the awgn channel with lattice encoding and decoding. *IEEE Trans. Inform. Theory*, New York, PAS-50, n. 10, p. 2293–2314, Oct. 2004.

ESMONDE, J.; MURTY, M. R. *Problems in algebraic number theory*. 2. ed. New York: Springer-Verlag, 2005. 352 p.

FORNEY, G. D. Coset codes-part i: Introduction and geometrical classification. *IEEE Trans. Inform. Theory*, New York, PAS-34, n. 5, p. 1123–1151, Sep. 1988.

FOSCHINI, G. J. Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas. *Bell Labs Technical Journal*, New York, PAS-1, n. 2, p. 41–59, Oct. 1996.

HASSIBI, B.; HOCHWALD, B. High-rate codes that are linear in space and time. *IEEE Trans. Inform. Theory*, New York, PAS-48, n. 7, p. 1804–1824, Jul. 2002.

HODGSON, B. R. On some number sequences related to the parity of binomial coefficients. *Université Laval, Québec G1K 7P4, Canada*, Québec, PAS-30, n. 1, p. 35–47, Feb. 1992.

HOLLANTI, C.; LAHTONEN, J.; RANTO, K.; VEHKALAHTI, R. On the densest mimo lattices from cyclic division algebras. *IEEE Trans. Inform. Theory*, New Jersey, PAS-55, n. 8, p. 3751–3780, Aug. 2009.

JAFARIAN, A.; VISHWANATH, S. Achievable rates for k-user gaussian interference channels. *IEEE Trans. Inform. Theory*, New York, v. 58, n. 7, p. 4367–4380, Jul. 2012.

JESUS, C. H. S. de. *Discriminante dos subcorpos de corpos ciclotômicos de condutores potência de um primo ímpar* . 2007. 128 f. Tese (Doutorado) — Centro de Ciências Exatas e da Natureza, Universidade Federal da Paraíba, Paraíba, 2007.

KIRAN, T.; RAJAN, B. S. Stbc-schemes with nonvanishing determinant for certain number of transmit antennas. *IEEE Trans. Inform. Theory*, New York, PAS-51, n. 8, p. 2984–2992, Aug. 2005.

MARCUS, D. A. *Number fields*. New York: Springer-Verlag, 1977. 279 p.

NAZER, B.; GASTPAR, M. Compute-and-forward: harnessing interference through structured codes. *IEEE Trans. Inform. Theory*, New York, PAS-57, n. 10, p. 6463–6486, Oct. 2011.

OGGIER, F. *Algebraic methods for channel coding*. 2005. 125 f. Tese (Doutorado) — École Polytechnique Fédérale de Lausanne, Lausanne, 2005.

OGGIER, F.; REKAYA, G.; BELFIORE, J.-C.; VITERBO, E. Perfect space-time block codes. *IEEE Trans. Inform. Theory*, New York, PAS-52, n. 9, p. 3885–3902, Sep. 2006.

OGGIER, F.; SOLE, P.; BELFIORE, J. C. Lattice codes for the wiretap gaussian channel: construction and analysis. *IEEE Trans. Inform. Theory*, 2011.

PETERS, S. W.; JUNIOR, W. H. Cooperative algorithms for mimo interference channels. *IEEE Transactions on Vehicular Technology*, New York, PAS-60, n. 1, p. 206–218, Jan. 2011.

SAMUEL, P. *Algebraic theory of numbers*. 2. ed. New York: Dover Publications, 2008. 109 p.

SCHMIDT, D. A.; SHI, C.; BERRY, R. A.; HONIG, M. L.; UTSCHICK, W. Minimum mean squared error interference alignment. In: SIGNALS, SYSTEMS AND COMPUTERS,

CONFERENCE RECORDS, 43.,2009. *Asilomar Conference*. [S.l.: s.n.], 2009. p. 1106–1110. ISBN 978-1-4244-5825-7.

SETHURAMAN, B.; RAJAN, B.; SHASHIDHAR, V. Full-diversity, high-rate, space-time block codes from division algebras. *IEEE Trans. Inform. Theory*, New York, PAS-49, n. 10, p. 2596–2616, Oct. 2003.

SHEN, M.; MADSEN, A. H. st; VIDAL, J. An improved interference alignment scheme for frequency selective channels. In: *ISIT 2008*. [S.l.: s.n.], 2008. p. 559–563. ISBN 978-1-4244-2257-9.

STEWART, I.; TALL, D. *Algebraic number theory and Fermat's last theorem*. 3. ed. Natick: A K Peters, 2002. 309 p.

TELATAR, I. E. Capacity of multi-antenna gaussian channels. *European Transactions on Telecommunications*, New Jersey, PAS-10, n. 6, p. 585–596, Nov./ Dec. 1999.

TRINCA, C. C.; CARVALHO, E. D.; FILHO, J. V.; ANDRADE, A. A. On the construction of perfect codes from hex signal constellations. *Journal of the Franklin Institute*, Philadelphia, PAS-349, n. 10, p. 3060–3077, Dec. 2012.

WASHINGTON, L. C. *Introduction to cyclotomic fields*. 2. ed. New York: Springer-Verlag, 1997. 487 p.

ZAMIR, R. Lattices are everywhere. In: ANNUAL WORKSHOP ON INFORMATION THEORY AND ITS APPLICATIONS, 4.,2009. *Proceedings of the 4th ITA*. [S.l.: s.n.], ITA, 2009. p. 392–421. ISBN 978-1-4244-3990-4.

APPENDIX A - FINDING A UNIT-MAGNITUDE ELEMENT γ

In this appendix we present a non-norm element γ in $F = \mathbb{Q}(\xi_3)$. By Theorem 11, it is equivalent to find a prime ideal in $\mathbb{Z}[\xi_3]$, whose inertial degree f in K/F is $f = [K:F] = n$. For our propose, we use the next theorem:

Theorem 15. *(Dirichlet's theorem) Let a, m be integers such that $1 \leq a \leq m$ and $gcd(a,m) = 1$. Then the arithmetic progression $\{a, a+m, a+2m, \cdots, a+km, \cdots\}$ contains infinitely many primes.*

Let $n = 3^s n_2$, where $n_2 > 0$ is an even number not multiple of 4. By Theorem 15, there is the smallest odd prime $p \neq 3$ such that $n_2 | (p-1)$. Such a prime is guaranteed to exist when we apply the theorem 15 to the progression $1, 1+n_2, \ldots, 1+kn_2, \ldots$.

The cyclic group $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ contains an element $a \in \mathbb{Z}_p^*$ whose order equals $(p-1)$. Now our goal is to find a prime q such that

$$q \equiv 7 (mod\ 3^{s+1}) \text{ and } q \equiv a (mod\ p).$$

Therefore $q = k3^{s+1} + 7$. Note that $q \equiv 1 (mod\ 3)$. Since $(3^{s+1}, p) = 1$, by the Chinese Remainder Theorem, it follows that there exists an integer b such that

$$q \equiv 7 (mod\ 3^{s+1}) \quad \text{and} \quad b \equiv a (mod\ p).$$

Note that there is an integer b that is relatively prime to $3^{s+1}p$. Now we consider the arithmetic progression

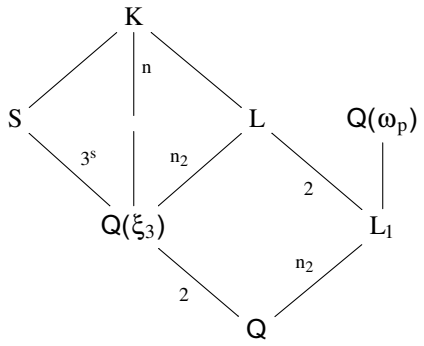
$$b + l\ (3^{s+1}p),\ \textit{where } l = 0, 1, 2, \ldots \tag{84}$$

By Theorem 15, this arithmetic progression is guaranteed to contain a prime q having the desired properties. Now we show that this leads to the construction of a cyclic division algebra.

Let L_1 be a subfield of $\mathbb{Q}(\omega_p)$, where $\omega_p = e^{\frac{2\pi i}{p}}$ and L_1 is a cyclic extension of $\mathbb{Q}$ of degree n_2.

Let L be the compositum of L_1 and $\mathbb{Q}(\xi_3)$, and let K be the compositum of the fields L and $S = \mathbb{Q}(\xi_3)(\theta)$, where $\theta = e^{\frac{2\pi i}{3^{s+1}}}$.

Figure 1 - Constructing a cyclic extension of $\mathbb{Q}(\xi_3)$ of degree $n = 3^s n_2$. The integers shown indicate the degree of the corresponding extension.



Fonte: Oggier (2005)

Figure 1 shows the tower of fields used in the construction of a cyclic extension of $\mathbb{Q}(\xi_3)$ of degree $n = 3^s n_2$. The integers shown indicate the degree of the corresponding extension.

Note that K is cyclic over $\mathbb{Q}(\xi_3)$, since it is a compositum of the cyclic extension $\mathbb{Q}(\xi_3)(\theta)/\mathbb{Q}(\xi_3)$ of degree 3^s and the cyclic extension $L/\mathbb{Q}(\xi_3)$ of degree n_2 (note that 3^s and n_2 are relatively prime).

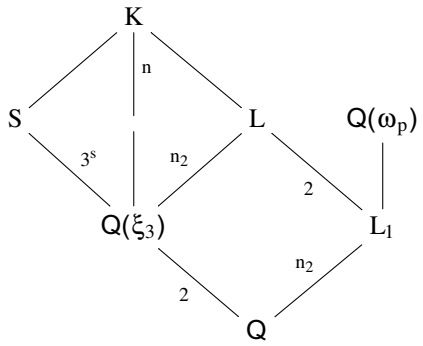
Next consider the decomposition of the prime ideal (q) in the extension $K/\mathbb{Q}$. Since q has order $(p-1)$ in $\mathbb{Z}_p$, it follows that q remains inert in $\mathbb{Q}(\omega_p)/\mathbb{Q}$. Since $q \equiv 7 \ (mod\ 3^{s+1})$ and 7 has order 3^s in $\mathbb{Z}_{3^{s+1}}$, it follows that in the extension $K/\mathbb{Q}$ q splits completely in $\mathbb{Q}(\xi_3)/\mathbb{Q}$, where $q = 1 \ (mod\ 3)$, but remains inert thereafter.

Let q split in $\mathbb{Q}(\xi_3)/\mathbb{Q}$ according to

$$q = \pi_1 \bar{\pi}_1,$$

where $\pi_1 = a + b\xi_3$ and $\bar{\pi}_1 = a + b\xi_3^2$. Now by using the fact that in the field tower $[E : K : F]$ of field extensions $f_{E/F} = f_{E/K} f_{K/F}$, $g_{E/F} = g_{E/K} g_{K/F}$ and $[E : F] = f_{E/F} g_{E/F}$, it follows that π_1 remains inert in the extension $K/\mathbb{Q}(\xi_3)$.

Figure 2 - Constructing a cyclic extension of $\mathbb{Q}(\xi_3)$ of degree $n = 3^s n_2$. The integers shown indicate the inertial degrees associated with the decomposition of either the prime ideal $q\mathbb{Z}$ or of one of its factors, over the corresponding extension.



Fonte: Elia, Sethuraman e Kumar (2007)

Figure 2 shows the tower of fields used in the construction of a cyclic extension of $\mathbb{Q}(\xi_3)$ of degree $n = 3^s n_2$. The integers shown indicate the inertial degrees associated with the decomposition of either the prime ideal $q\mathbb{Z}$ or of one of its factors, over the corresponding extension.

Now to find a non-norm element of unit magnitude, we note that since the units of $\mathbb{Z}[\xi_3]$ belong to the set $\{\pm 1, \pm\xi_3, \pm\xi_3^2\}$, the associates of $\pi = a + b\xi_3$ belong to the set

$$\{a+b\xi_3, -a-b\xi_3, \xi_3 a+b\xi_3^2, -\xi_3 a-b\xi_3^2, b+a\xi_3^2, -b-a\xi_3^2\}.$$

Since $ab \neq 0$ and $a \neq \pm b$, we have that $a + b\xi_3^2$ does not belong to the set of associates of $a + b\xi_3$. Our goal is to show that the element given by $\gamma = \frac{\pi_1}{\bar{\pi}_1}$ is a non-norm element, i.e, that the smallest exponent k for which γ^k is the norm of an element in $K^* = K - \{0\}$, is n. This is the case since if $\gamma^k = N_{K/F}(l)$, for some $l \in K^*$, then

$$\pi_1^k = (\bar{\pi}_1)^k \prod_{\alpha=0}^{n-1} \sigma^\alpha(l), \tag{85}$$

where σ is the generator of the cyclic Galois group of K/F. For $l = \frac{a}{b}$, where $a, b \in \mathscr{O}_K$, we have, in terms of ideals of $\mathscr{O}_K$,

$$(\pi_1)^k \prod_{\alpha=0}^{n-1} (\sigma^\alpha(b)) = (\bar{\pi}_1)^k \prod_{\alpha=0}^{n-1} (\sigma^\alpha(a)). \tag{86}$$

Since the primes π_1 and $\bar{\pi}_1$ are relatively prime, it follows that π_1 must divide $\sigma^\alpha(a)$, for some α. But since $\sigma(\pi_1) = \pi_1$, we have that if (π_1) divides $(\sigma^\alpha(x))$, for some α and $x \in \mathscr{O}_K$, then it must divide $(\sigma^\alpha(x))$, $\forall\ \alpha$. This in turn implies that the power of (π_1) in the prime decomposition of $(\pi_1)^k \prod_{\alpha=0}^{n-1} (\sigma^\alpha(b))$ is $k \ mod\ n$ whereas the power of (π_1) in the prime decomposition of $(\bar{\pi}_1)^k \prod_{\alpha=0}^{n-1} (\sigma^\alpha(a))$ is a multiple of n and it follows that γ is a non-norm

element. Equivalently k must be a multiple of n.

APPENDIX B - CONSTRUCTION OF $\mathscr{A}_2^N$ LATTICES

Boutros and Viterbo (BOUTROS; VITERBO, 1998) constructed a family of orthogonal matrices M isomorphic to the $\mathbb{Z}[i]^n$-rotated lattice (cubic form) from the cyclotomic number field $K = F(\theta)$, where $F = \mathbb{Q}(i)$, $\theta = e^{\frac{2\pi i}{N}}$ is an N-th root of unity, $N = 2^{s_1}3^{s_2}$, for some $s_1, s_2 = 0, 1, 2, \ldots$, and $n = \Phi(N)$, where Φ is the Euler function. K is an algebraic extension of $\mathbb{Q}(i)$ of degree $\frac{\Phi(N)}{2}$. We recall that this is a totally complex field with signature $(r_1 = 0, r_2 = n/2)$ and minimal polynomial

$$\mu_\theta(x) = \prod_{(k,N)=1} (x - \theta^k),$$

where (k,N) is the greatest common divisor of k and N. The minimal polynomial over $\mathbb{Z}[i]$ is denoted by $m(x)$ and defined later in this appendix.

We will show, with the same procedure of the construction of orthogonal matrices M (cubic form) proposed in (BOUTROS; VITERBO, 1998), that it is possible to construct a family of orthogonal matrices isomorphic to the $\mathbb{Z}[\xi_3]^n$-rotated lattice.

Notice that if we take the cyclotomic number field K given by $K = F(\theta)$, where $\theta = e^{\frac{2\pi\xi_3}{N}}$, we will find a family of orthogonal matrices isomorphic to the $\mathbb{Z}[\xi_3]^n$-rotated lattice. K is an algebraic extension of $F = \mathbb{Q}(\xi_3)$ of degree $\frac{\Phi(N)}{2}$.

So let us denote

$$\theta_1 = \theta, \theta_2, \ldots, \theta_{n/2}$$

the complex roots of $\mu_\theta(x)$, which define the $n/2$ distinct field $\mathbb{Q}$-homomorphisms

$$\sigma_1(\theta) = \theta_1, \ \sigma_2(\theta) = \theta_2, \ldots, \sigma_{n/2}(\theta) = \theta_{n/2}.$$

To construct a complex lattice Λ of dimension $n/2$ we apply the canonical embedding to the ring of integers $\mathscr{O}_K = \mathbb{Z}[\xi_3](\theta)$ generated by $\{1, \theta, \theta^2, \ldots, \theta^{n/2-1}\}$. Its generator matrix is given by

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_{n/2} \\ \vdots & \vdots & & \vdots \\ \theta_1^{n/2-1} & \theta_2^{n/2-1} & \cdots & \theta_{n/2}^{n/2-1} \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \cdots \\ v_{\frac{n}{2}} \end{pmatrix}, \tag{87}$$

where the complex lattice basis vectors $v_i, i = 1, 2, \ldots, n/2$, correspond to the rows of M.

We are interested in selecting the roots θ_i, $i = 1, 2, \ldots, n/2$, or equivalently, we want to find the minimal polynomial $\mu_\theta(x)$ so that M becomes an orthogonal matrix, i.e, a generator matrix

for the complex integer lattice in dimension $n/2$. The orthogonality among the complex vectors implies the orthogonality among the corresponding real vectors. The complex inner product of any two rows

$$v_{p+1} = (\theta_1^p, \theta_2^p, \ldots, \theta_{n/2}^p)$$

and

$$v_{q+1} = (\theta_1^q, \theta_2^q, \ldots, \theta_{n/2}^q),\ p,q = 0,1,\ldots,n/2-1,$$

of M must satisfy

$$\left\langle v_{p+1}, v_{q+1} \right\rangle = \sum_{k=1}^{n/2} (\theta_k)^p (\bar{\theta}_k)^q = 1,\ if\ p = q,\ and$$

$$\left\langle v_{p+1}, v_{q+1} \right\rangle = \sum_{k=1}^{n/2} (\theta_k)^p (\bar{\theta}_k)^q = 0,\ if\ p \neq q.$$

For $p > q$, it follows that

$$\left\langle v_{p+1}, v_{q+1} \right\rangle = \sum_{k=1}^{n/2} (\theta_k \bar{\theta}_k)^q (\theta_k)^{p-q} = \sum_{k=1}^{n/2} \|\theta_k\|^q (\theta_k)^{p-q} = 0 \tag{88}$$

and since the complex roots θ_i are placed on the unit circle $\|\theta_k\| = 1$,

$$\left\langle v_{p+1}, v_{q+1} \right\rangle = \sum_{k=1}^{n/2} (\theta_k)^m = S_m = 0,\ \mathrm{m} = 1,2,\ldots,n/2-1. \tag{89}$$

In other words, the first $n/2-1$ power symmetric functions S_m of the roots of $\mu_\theta(x)$ are null. The polynomial $\mu_\theta(x)$, which we want to determine, can be factored into $m(x)\overline{m}(x)$, where we assume that θ_i, $i = 1,2,\ldots,n/2$, are the roots of the polynomial $m(x)$ of degree $n/2$ over the ring $\mathscr{O}_F$, while $\overline{m}(x)$ takes on the complex conjugates roots.

Applying Newton's identities we easily observe that

$$m(x) = (x-\theta_1)\cdots(x-\theta_{n/2}) = x^{n/2} + P \text{ and } \overline{m}(x) = x^{n/2} + \overline{P} \tag{90}$$

so that

$$\mu_\theta(x) = x^n + (P+\overline{P})x^{n/2} + 1. \tag{91}$$

Now that we have the general form of the minimal polynomial we still need to determine which of the n roots of unity must be chosen to apply the canonical embedding.

Let $\theta_k = e^{i\phi_k}$, $k = 1,\ldots,n/2$, be the unknown roots of $m(x)$ which we want to determine. P is the product of the $n/2$ roots laying on the unity circle

$$P = e^{i\psi},\ \text{-}\pi \leq \psi < \pi. \tag{92}$$

In (BOUTROS; VITERBO, 1998) it is shown that if $\mu_\theta(x)$ has integer coefficients, so

$$P+\overline{P} = e^{i\psi} + e^{-i\psi} = 2cos\psi \in \mathbb{Z}, \tag{93}$$

which implies $\psi = \pm\pi/3, \pm\pi/2, \pm 2\pi/3$.

Boutros and Viterbo (BOUTROS; VITERBO, 1998) have shown that the possible values for the roots of $m(x)$ are valid for the cases $N = 2n$ and $N = 3n$. Then the values of ψ are $-\pi/2$ and $-2\pi/3$, and these values correspond to the polynomials of the type $x^n + \varepsilon x^{n/2} + 1$, where $\varepsilon = 0$ and $\varepsilon = 1$, respectively.

However we want $\mu_\theta(x) = x^n + (P+\overline{P})x^{n/2} + 1 \in \mathbb{Z}$, so the admissible values of ψ are $\pm\pi/2$ and $\pm 2\pi/3$.

Notice that if $\psi = \pm\pi/2$, by Equation (92), we obtain $P = e^{\pm i\frac{\pi}{2}} \in \mathbb{Z}[i]$. Therefore, as consequence of Equation(90), we conclude that the minimal polynomial $m(x) = x^{n/2} + P \in \mathbb{Z}[i]$. On the other hand, if $\psi = \pm 2\pi/3$, by Equation (92), we obtain $P = e^{\pm i\frac{2\pi}{3}} \in \mathbb{Z}[\xi_3]$. Therefore, as consequence of Equation (90), we conclude that the minimal polynomial $m(x) = x^{n/2} + P \in \mathbb{Z}[\xi_3]$. Thus there exist $\mathbb{Z}[i]^{n/2}$ and $\mathscr{A}_2^{n/2}$-rotated lattices for the dimensions $n = 2^{s_1}$, for $s_1 = 1, 2, \ldots$, and $n = 2^{s_1}3^{s_2}$, for $s_1 = 0, 1, 2, \ldots$ and $s_2 = 1, 2, \ldots$, respectively. For our purpose in this work we only have interest in the case $n = 2^{s_1}3^{s_2}$, for $s_1 = 1$ and $s_2 = 1, 2, \ldots$.

APPENDIX C - PROGRAM FOR CALCULATING THE GENERATOR AND GRAM MATRICES OF THE LATTICES ASSOCIATED TO THE REAL NESTED LATTICE PARTITION CHAINS

This program, made by using KASH program, presents the generator and Gram matrices of the lattices in each nested lattice partition chain. We can observe that each nested lattice partition chain is extended by periodicity and such a periodicity is equal to $n = 2^{r-2}$. The program is given as it follows:

```
r:=4;
w:=16;
m:=2^r;
n:=2^(r-2);
zeta:=Exp(2*PI*I/m);
theta:=zeta+zeta^(-1);
alpha:=2-theta;
p:=2+theta;
uw:=p^w;

sigmaw:=[];
sigma:=[];
L:=[1..n*n];
l:=List(L,x->0);
M:=Matrix(R,n,n,l);
GR:=Matrix(Z,n,n,l);
MI:=Matrix(Z,n,n,l);
T:=Matrix(Z,n,n,l);
Aw:=Matrix(R,n,n,l);
N:=Matrix(Z,n,n,l);
A:=Matrix(R,n,n,l);
NL:=Matrix(Z,n,n,l);
S:=Matrix(Z,n,n,l);

    # compute sqrt(alpha_k);

    for k in [1..n] do
```

```
sigma[k]:=Sqrt(2-2*Cos((2*PI*(2*k-1))/m));

od;

♯ compute uw_j;

for j in [1..n] do

sigmaw[j]:=(2+2∗Cos((2∗PI∗(2∗j-1))/m))^w;

od;

♯ compute A;

diag:=MatrixAlgebra(R,n);
A:=DiagonalMatrix(diag,sigma);

♯ compute Aw;

diag:=MatrixAlgebra(R,n);
Aw:=DiagonalMatrix(diag,sigmaw);

♯ compute M;

for j in [1..n] do

SetEntry(M,1,j,1);

od;

for i in [1..(n-1)] do

for j in [1..n] do

SetEntry(M,(i+1),j,2*Cos(((2*PI)/m)*i*(2*j-1)));

od;

od;

MT:=Transpose(M);
```

```
♯ compute T;
for j in [1..n] do
for i in [1..(n-(j-1))] do
SetEntry(T,i,j,-1);
od;
od;

Mw:=M∗A∗Aw;
MwT:=Transpose(Mw);

P:=M*A;
Pinv:=P^(-1);
Mu:=P*Aw*Pinv;
MuT:=Transpose(Mu);

♯ compute MI;
for i in [1..n] do
for j in [1..n] do
SetEntry(MI,i,j,Round(Mu[i][j]));
od;
od;

MIT:=Transpose(MI);
gu:=MI*MIT;
gul:=LLLGram(gu);
```

```
♯ compute N=guR;
for i in [1..n] do
for j in [1..n] do
SetEntry(N,i,j,Round(gu[i][j]));
od;
od;

NL:=LLLGram(N);

♯ compute S;
for i in [1..n] do
for j in [1..n] do
SetEntry(S,i,j,Round(gul[i][j]));
od;
od;
```

We can observe that the matrix NL is equal to the matrix S.